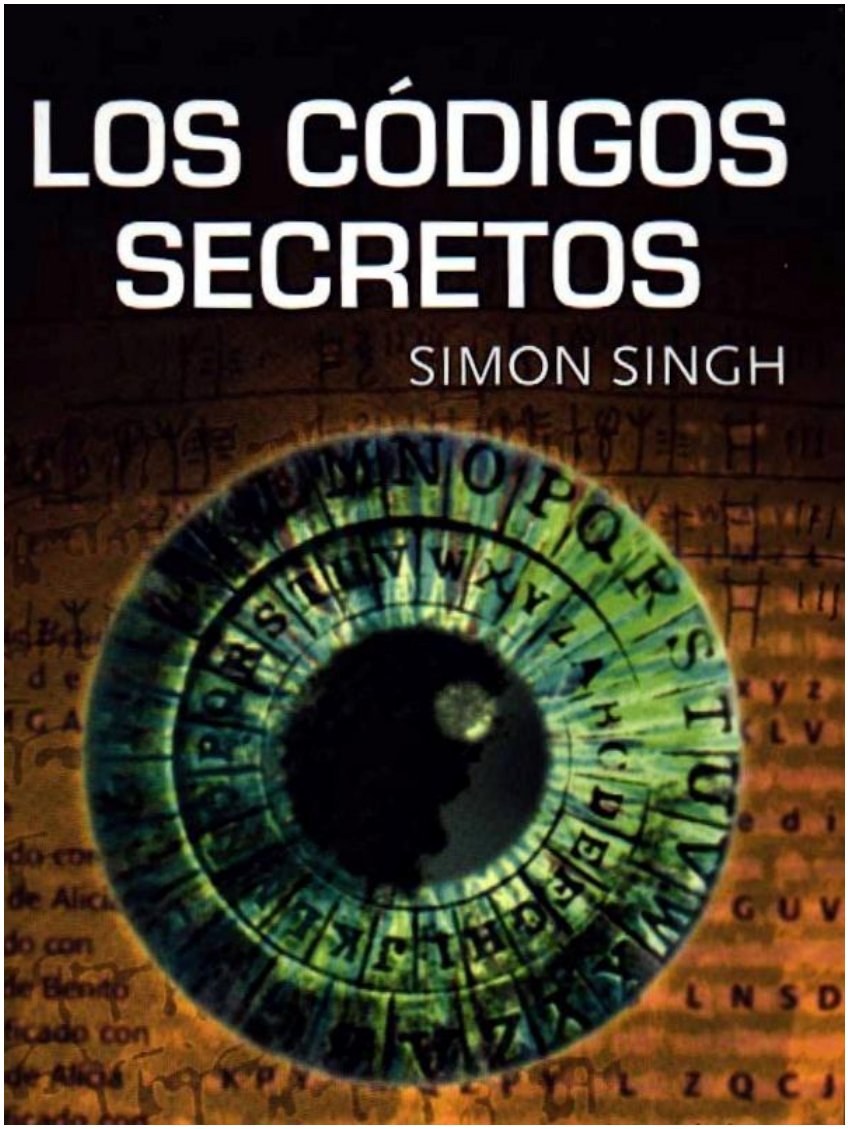

LOS CÓDIGOS SECRETOS
SIMON SINGH

Presentación

Desde las campañas militares de Julio César a las actuales compras por Internet, el ser humano se ha visto en la necesidad de cifrar sus mensajes para evitar que éstos, en caso de ser interceptados, puedan ser leídos. La criptografía se ha erigido en la herramienta primordial para tal fin. Pero su imparable desarrollo se ha visto condicionado por los avances logrados por su reverso: el criptoanálisis, la ciencia cuyo objetivo se centra en descifrar códigos.

Simon Singh relata en Los códigos secretos los progresos de una y otra ciencia a través de las historias de amantes y militares, conspiradores y buscadores de tesoros, sin pasar por alto a famosos escritores de novelas de misterio, hasta llegar, finalmente, a la inquietante realidad emergente en nuestros días: una nueva sociedad intercomunicada hasta un punto inimaginable pero, al mismo tiempo, más vulnerable que nunca a un control total y demoledor.

La vieja pugna entre creadores de cifras y descifradores sigue viva, latente y encarnizada; sin embargo, su área de acción ya no se circunscribe a las altas esferas del poder. El campo de batalla se ha ampliado a todos los ámbitos de la sociedad civil, al cotidiano mundo del ciudadano de a pie.

A mi madre y a mi padre,
Sawaran Kaur y Mehnga Singh

El deseo de descubrir secretos está profundamente arraigado en la naturaleza humana. Incluso la mente menos curiosa se excita ante la promesa de acceder a conocimientos ocultos para otras personas. Algunos tienen la suerte de encontrar un trabajo que consiste en solucionar misterios, pero la mayoría de nosotros tenemos que contentarnos con sublimar ese deseo resolviendo misterios artificiales creados para nuestro entretenimiento. Las historias de detectives o los crucigramas satisfacen las necesidades de la mayoría; el desciframiento de códigos secretos puede ser la tarea de unos pocos.

El desciframiento del Lineal B
John Chadwick

Índice

Introducción

Durante miles de años, los reyes, reinas y generales han dependido de la comunicación eficiente para gobernar sus países y ordenar a sus ejércitos. Al mismo tiempo, todos ellos han sido conscientes de las consecuencias que se producirían si sus mensajes cayeran en las manos equivocadas, revelando valiosos secretos a naciones rivales y divulgando información vital a las fuerzas contrarias. Fue la amenaza de que el enemigo interceptara los mensajes lo que motivó el desarrollo de códigos y cifras: técnicas para disfrazar un mensaje de forma que sólo pueda leerlo el receptor a quien va dirigido.

El deseo de mantener secretos, ha provocado que las naciones hayan puesto en funcionamiento departamentos encargados de crear códigos, sobre los que recae la responsabilidad de la seguridad de las comunicaciones mediante la invención y la puesta en práctica de los mejores códigos posibles. Al mismo tiempo, los descifradores de códigos enemigos han tratado de desentrañar estos códigos y robar secretos. Los descifradores de códigos son alquimistas lingüísticos, una tribu mística que trata de hacer aparecer palabras inteligibles de símbolos sin sentido. La historia de los códigos y las cifras es la historia de siglos de batalla entre los creadores de códigos y los descifradores, una carrera de armamentos intelectuales que ha tenido un impacto enorme en el curso de la Historia.

Al escribir *Los códigos secretos,* me he guiado por dos objetivos principales. El primero es trazar la evolución de los códigos. Evolución es un término completamente apropiado, ya que el desarrollo de los códigos puede ser considerado como una lucha evolutiva. Un código se enfrenta constantemente al ataque de los descifradores. Cuando éstos han producido una nueva arma que revela la debilidad de un código, éste deja de ser útil. O se extingue o evoluciona en un código nuevo, más fuerte. A su vez, este nuevo código prospera sólo hasta que los descifradores identifican su punto débil, y así sucesivamente. Esta situación es análoga a la de, por ejemplo, una cepa de bacterias infecciosas. Las bacterias viven, se desarrollan y sobreviven hasta que los médicos descubren un antibiótico que descubre una debilidad en ellas y las mata. Las bacterias se ven forzadas a evolucionar y mostrarse más listas que el antibiótico, y, si lo consiguen, prosperarán

una vez más y se restablecerán. Las bacterias se ven forzadas continuamente a evolucionar para sobrevivir al ataque violento de nuevos antibióticos.

La batalla constante entre los creadores de códigos y los descifradores ha inspirado toda una serie de notables avances científicos. Los creadores de códigos se han esforzado continuamente por construir códigos cada vez más fuertes para defender las comunicaciones, mientras que los descifradores han inventado constantemente métodos más poderosos para atacarlos. En sus esfuerzos por destruir y preservar secretos, ambos bandos se han servido de una amplia

gama de disciplinas y tecnologías, de las matemáticas a la lingüística, de la teoría de la información a la teoría cuántica. En contrapartida, los creadores de códigos y los descifradores han enriquecido estas materias, y su trabajo ha acelerado el desarrollo tecnológico, especialmente en el caso de los ordenadores modernos.

La Historia está llena de códigos. Ellos han decidido el desenlace de batallas y han llevado a la muerte a reyes y reinas. Por ello, he podido servirme de historias de intriga política y de relatos de vida y muerte para ilustrar los principales puntos decisivos del desarrollo evolutivo de los códigos.

La historia de los códigos es tan desmesuradamente rica que me he visto forzado a excluir muchas historias fascinantes, lo que significa, a su vez, que mi estudio no es definitivo. Si usted desea descubrir más cosas acerca de su historia favorita o de su descifrador favorito, yo le remitiría a la lista de lecturas adicionales, que debería ayudar a aquellos lectores que quieran estudiar el tema con más detalle.

Una vez tratada la evolución de los códigos y su impacto en la Historia, el segundo objetivo del libro es demostrar por qué el tema es en nuestros días más relevante que nunca. Según la información se va convirtiendo en una mercancía cada vez más valiosa, y según la revolución de las comunicaciones cambia la sociedad, el proceso de cifrar mensajes, conocido como codificación, desempeñará un papel cada vez más importante en la vida cotidiana. Hoy en día, nuestras llamadas de teléfono pasan por satélites y nuestro correo electrónico pasa por varios ordenadores, y ambas formas de comunicación pueden ser interceptadas con facilidad, poniendo en peligro de esta forma nuestra privacidad. Similarmente, como cada vez más negocios se llevan a cabo a través de Internet, hay que crear salvaguardias para proteger a las empresas y a sus clientes. La codificación es la única manera de

proteger nuestra privacidad y garantizar el éxito del mercado digital. El arte de la comunicación secreta, también conocido como criptografía, suministrará las cerraduras y las llaves de la Era de la Información.

Sin embargo, la creciente demanda pública de criptografía está en conflicto con las necesidades de la aplicación de la ley y la seguridad nacional. Durante décadas, la policía y los servicios de inteligencia han intervenido teléfonos para acumular evidencia contra terroristas y consorcios del crimen organizado, pero el reciente desarrollo de códigos ultraseguros amenaza con socavar la utilidad de las intervenciones del teléfono. En los umbrales del siglo XXI, los libertarios sociales están insistiendo en la necesidad del uso general de la criptografía para proteger la privacidad del individuo. También insisten en ello las empresas, que requieren una criptografía fuerte para garantizar la seguridad de las transacciones en el mundo del comercio por Internet el cual está experimentando un crecimiento rapidísimo. Al mismo tiempo, las fuerzas de la ley y el orden están presionando a los gobiernos para que restrinjan el uso de la criptografía. La cuestión es: ¿qué valoramos más, nuestra privacidad o una fuerza policial eficaz? ¿O existe una solución intermedia?

Aunque la criptografía tiene ahora un gran impacto en las actividades civiles, hay que señalar que la criptografía militar sigue siendo un tema importante. Se ha dicho que la primera guerra mundial fue la guerra de los químicos, por que se utilizó por vez primera el gas mostaza y el cloro, y que la segunda guerra mundial fue la guerra de los físicos, porque se hizo explotar la bomba atómica. De forma similar, se ha alegado que la tercera guerra mundial sería la guerra de los matemáticos, porque los matemáticos controlarán la siguiente gran arma de guerra: la información. Los matemáticos han sido los responsables del desarrollo de los códigos que se utilizan actualmente para proteger la información militar. No es de extrañar, por tanto, que los matemáticos estén también en la vanguardia de la batalla para descifrar estos códigos.

Al describir la evolución de los códigos y su impacto en la Historia, me he permitido un pequeño rodeo. El capítulo 5 describe el desciframiento de varias escrituras antiguas, incluidos el Lineal B y los jeroglíficos egipcios. Técnicamente, la criptografía se ocupa de las comunicaciones que están diseñadas deliberadamente para mantener secretos frente a un enemigo, mientras que las escrituras de las

civilizaciones antiguas no estaban pensadas con la intención de ser indescifrables: lo que sucede simplemente es que hemos perdido la habilidad de interpretarlas. Sin embargo, la destreza requerida para desvelar el significado de los textos arqueológicos está estrechamente emparentada con el arte del desciframiento de códigos. Desde que leí *El desciframiento del Lineal* B, la descripción de John Chadwick de cómo se desenmarañó un antiguo texto mediterráneo, me he sentido impresionado por los excelentes logros intelectuales de los hombres y las mujeres que han sido capaces de descifrar las escrituras de nuestros antepasados, permitiéndonos de esta forma leer acerca de sus civilizaciones, sus religiones y su vida cotidiana.

Dirigiéndome a los puristas, debería disculparme por el título de este libro. *Los códigos secretos* no sólo se ocupa de los códigos. La palabra «código» alude a un tipo muy particular de comunicación secreta, que ha ido cayendo en desuso a lo largo de los siglos. En un código, una palabra o una frase es reemplazada por una palabra, un número o un símbolo. Por ejemplo, los agentes secretos tienen nombres codificados, palabras que se utilizan en vez de sus verdaderos nombres para enmascarar su identidad. De manera similar, la frase Atacad al amanecer podría sustituirse por la contraseña Júpiter, y se podría enviar esta palabra a un comandante en el campo de batalla para desconcertar al enemigo. Si el cuartel general y el comandante se han puesto de acuerdo previamente con respecto a este código, el significado de Júpiter estará claro para el receptor a quien va dirigido, pero no significará nada para el enemigo que lo intercepte. La alternativa al código es la cifra, una técnica que funciona a un nivel más básico, reemplazando letras en vez de palabras enteras. Por ejemplo, cada letra de una frase podría reemplazarse por la siguiente letra del alfabeto, de manera que A fuera reemplazada por B, B por C, y así sucesivamente. Atacad al amanecer se convierte así en Bubdbe bm bnbñfdfs. Las cifras desempeñan un papel esencial en la criptografía, por lo que este libro debería llamarse realmente *Los códigos secretos y las cifras.* Sin embargo, he renunciado a la exactitud en favor de la elegancia.

Según ha ido surgiendo la necesidad, he definido los diversos términos técnicos utilizados en el campo de la criptografía. Aunque generalmente me he ajustado a estas definiciones, habrá ocasiones en las que utilice un término que quizá no sea

técnicamente exacto, pero que me parece más familiar para los que no son especialistas. Por ejemplo, al describir a una persona que trata de descifrar una cifra, a menudo he utilizado el término *descifrador de códigos*, en vez del más exacto *descifrador de cifras.* Sólo lo he hecho cuando el significado de la palabra es obvio debido al contexto. En la mayoría de los casos, sin embargo, la jerga de la criptografía es bastante transparente: por ejemplo, *texto llano* es el mensaje antes de la codificación, y *texto cifrado* es el mensaje después de la misma.

Antes de concluir esta introducción, debo mencionar un problema al que se enfrenta cualquier autor que aborda el tema de la criptografía: la ciencia del secreto es en gran medida una ciencia secreta. Muchos de los héroes que aparecen en este libro nunca obtuvieron el reconocimiento por su trabajo mientras vivían, porque su contribución no podía reconocerse públicamente mientras lo que habían inventado aún tenía valor diplomático o militar. Al documentarme e investigar para escribir este libro, tuve la oportunidad de hablar con expertos del GCHQ (Government Communications Headquarters, Sede Central de Comunicaciones del Gobierno británico), que me revelaron detalles de investigaciones extraordinarias realizadas en la década de los setenta y que acababan de dejar de ser clasificadas como secretas. Como resultado de haber salido de esa clasificación, tres de los mejores criptógrafos del mundo pueden recibir ahora el crédito que merecen. Sin embargo, esta reciente revelación sólo ha servido para recordarme que están sucediendo muchísimas más cosas, de las que ni yo ni ningún otro autor es consciente. Organizaciones como el GCHQ y la NSA norteamericana (National Security Agency, Agencia para la Seguridad Nacional) continúan realizando investigaciones secretas en el campo de la criptografía, lo que significa que sus avances permanecen secretos y que los individuos que los producen continúan anónimos.

A pesar de los problemas del secreto gubernamental y de la investigación secreta, he dedicado el último capítulo de este libro a la especulación sobre el futuro de los códigos y las cifras. En el fondo, este capítulo es un intento de ver si podemos predecir quién ganará la lucha evolutiva entre el creador de cifras y el descifrador. ¿Lograrán alguna vez los creadores de códigos diseñar uno verdaderamente indescifrable y triunfar en su búsqueda del secreto absoluto? ¿O construirán los descifradores una máquina capaz de descifrar cualquier mensaje? Teniendo en

cuenta que algunas de las mejores mentes trabajan en laboratorios secretos y que reciben la mayor parte de los fondos destinados a la investigación, está claro que algunas de mis afirmaciones en el capítulo final pueden resultar inexactas. Por ejemplo, digo que los ordenadores cuánticos — máquinas potencialmente capaces de descifrar todas las cifras actuales— están en un estado muy primitivo, pero es posible que alguien ya haya construido uno. Las únicas personas que se encuentran en posición de señalar mis errores son precisamente las que no pueden tomarse la libertad de revelarlos.

Capítulo 1

La cifra de María Estuardo, reina de Escocia

Contenido:

La mañana del miércoles 15 de octubre de 1586, la reina María Estuardo entró en la abarrotada sala de justicia del castillo de Fotheringhay. Los años de encarcelamiento y el reumatismo habían hecho sentir su huella, pero ella permanecía digna, tranquila e indiscutiblemente regia. Ayudada por su médico, fue pasando ante los jueces, funcionarios y espectadores, y se aproximó al trono que había a mitad de camino de la larga y estrecha sala. María había creído que el trono era un gesto de respeto hacia ella, pero se equivocaba. El trono simbolizaba a la ausente reina Isabel, su enemiga y acusadora. Con delicadeza, María fue separada del trono y guiada hacia el otro extremo de la habitación, al asiento de los acusados, una silla de terciopelo carmesí.

Se juzgaba a María, reina de Escocia, por traición. Había sido acusada de conspirar para asesinar a la reina Isabel para hacerse con la corona inglesa. *Sir* Francis Walsingham, el secretario principal de Isabel, ya había arrestado a los demás conspiradores, logrando que confesaran, y los había ejecutado. Ahora planeaba demostrar que María estaba en el centro de la conspiración y que, por tanto, era igualmente culpable e igualmente merecedora de la muerte.

Walsingham sabía que antes de poder ejecutar a María tendría que convencer a la reina Isabel de su culpabilidad. Aunque Isabel odiaba a María, tenía varias razones para mostrarse reacia a verla condenada a muerte. En primer lugar, María era una reina escocesa y muchos cuestionaban si un tribunal inglés tenía autoridad para ejecutar a un cabeza de Estado extranjero. En segundo lugar, ejecutar a María

podría establecer un precedente incómodo —si al Estado le está permitido matar a una reina, entonces quizá los rebeldes podrían tener menos reservas a la hora de matar a otra reina, concretamente a Isabel—. En tercer lugar, Isabel y María eran primas, y su lazo de sangre hacía que Isabel se sintiera mucho más impresionable con respecto a ordenar su ejecución. En resumidas cuentas, Isabel sólo aprobaría la ejecución de María si Walsingham podía probar más allá de cualquier vestigio de duda que ésta había tomado parte en la conspiración para asesinarla.

Los conspiradores eran un grupo de jóvenes nobles católicos ingleses decididos a eliminar a Isabel, una protestante, y sustituirla por María, católica como ellos. Era evidente para el tribunal que María era la cabecilla simbólica de los conspiradores, pero no estaba claro que ella hubiese dado su aprobación a la conspiración. En realidad, María había autorizado la trama. El desafío para Walsingham era demostrar una conexión palpable entre María y los conspiradores.

Figura 1. María Estuardo, reina de Escocia.

En la mañana de su juicio, María estaba sola sentada en el banquillo, vestida de triste terciopelo negro. En los casos de traición, al acusado no se le permitía tener abogado ni tampoco podía llamar a testigos. A María ni siquiera se le permitió que

sus secretarios la ayudaran a preparar su caso. Sin embargo, su situación no era desesperada, porque había tenido cuidado de asegurarse que toda su correspondencia con los conspiradores se hubiera escrito en cifra. La cifra convertía sus palabras en una serie de símbolos sin sentido, y María creía que, incluso si Walsingham había capturado las cartas, no podría tener ni idea del significado de las palabras que contenían. Si su contenido era un misterio, entonces las cartas no podrían ser utilizadas como prueba contra ella.

Sin embargo, todo ello dependía de la suposición de que la cifra no había sido descifrada.

Desgraciadamente para María, Walsingham no era tan sólo secretario principal, también era jefe del espionaje de Inglaterra. Había interceptado las cartas de María a los conspiradores y sabía exactamente quién sería capaz de descifrarlas. Thomas Phelippes era el experto más eminente de la nación en descifrar cifras, y durante años había estado descifrando los mensajes de los que conspiraban contra la reina Isabel, proporcionando de esta forma la evidencia necesaria para condenarlos. Si podía descifrar las cartas incriminatorias entre María y los conspiradores, entonces la muerte de ésta sería inevitable. Por otra parte, si la cifra de María era lo suficientemente fuerte para ocultar sus secretos, entonces existía una posibilidad de que pudiera sobrevivir. No por vez primera, una vida dependía de la solidez de una cifra.

1. La evolución de la escritura secreta

Algunos de los testimonios más antiguos de escritura secreta se remontan a Heródoto, «el padre de la Historia», según el filósofo y estadista romano Cicerón. En *Las Historias*, Heródoto hizo una crónica de los conflictos entre Grecia y Persia en el siglo V a. C., que él consideró como un enfrentamiento entre la libertad y la esclavitud, entre los estados independientes griegos y los persas opresores. Según Heródoto, fue el arte de la escritura secreta lo que salvó a Grecia de ser ocupada por Jerjes, el Rey de Reyes, el despótico líder de los persas.

El prolongado enfrentamiento entre Grecia y Persia alcanzó una crisis poco después de que Jerjes comenzara a construir una ciudad en Persépolis, la nueva capital para su reino. Llegaron tributos y regalos de todo el imperio y de los estados vecinos,

con las notables excepciones de Atenas y Esparta. Decidido a vengar esta insolencia, Jerjes comenzó a movilizar una fuerza, declarando que «extenderemos el imperio de Persia de tal manera que sus límites serán el propio cielo de Dios, de forma que el sol no brillará en ninguna tierra más allá de los límites de lo que es nuestro». Pasó los cinco años siguientes reuniendo en secreto la mayor fuerza de lucha de la Historia, y entonces, en el año 480 a. C., estuvo listo para lanzar un ataque sorpresa.

Sin embargo, la proliferación militar persa había sido presenciada por Demarato, un griego que había sido expulsado de su patria y que vivía en la ciudad persa de Susa. A pesar de estar exiliado, aún sentía cierta lealtad hacia Grecia, y decidió enviar un mensaje para advertir a los espartanos del plan de invasión de Jerjes. El desafío consistía en cómo enviar el mensaje sin que fuera interceptado por los guardas persas. Heródoto escribió:

> *Como el peligro de que lo descubrieran era muy grande, sólo había una manera en que podía contribuir a que pasara el mensaje: retirar la cera de un par de tablillas de madera, escribir en la madera lo que Jerjes planeaba hacer y luego volver a cubrir el mensaje con cera. De esta forma, las tablillas, al estar aparentemente en blanco, no ocasionarían problemas con los guardas del camino. Cuando el mensaje llegó a su destino, nadie fue capaz de adivinar el secreto, hasta que, según tengo entendido, la hija de Cleomenes, Gorgo, que era la esposa de Leónidas, lo vaticinó y les dijo a los demás que si quitaban la cera encontrarían algo escrito debajo, en la madera. Se hizo así; el mensaje quedó revelado y fue leído, y después fue comunicado a los demás griegos.*

Como resultado de esta advertencia, los hasta entonces indefensos griegos comenzaron a armarse. Los beneficios de las minas de plata pertenecientes al Estado, que normalmente se distribuían entre los ciudadanos, fueron ahora transferidos a la Marina para la construcción de doscientas naves de guerra.

Jerjes había perdido el vital elemento de la sorpresa y, el 23 de septiembre del año 480 a. C., cuando la flota persa se aproximó a la bahía de Salamina, cerca de

Atenas, los griegos estaban preparados. Aunque Jerjes creía que había atrapado a la marina griega, los griegos estaban incitando deliberadamente a las naves persas para que entraran en la bahía. Los griegos sabían que sus naves, más pequeñas y menores en número, serían destruidas en el mar abierto, pero se dieron cuenta que entre los confines de la bahía podrían superar estratégicamente a los persas. Cuando el viento cambió de dirección, los persas fueron llevados por el viento al interior de la bahía, forzados a un enfrentamiento en los términos de los griegos. La princesa persa Artemisa quedó rodeada por tres lados y trató de volver hacia el mar abierto, consiguiendo tan sólo chocar con una de sus propias naves. Entonces cundió el pánico, más naves persas chocaron entre sí y los griegos lanzaron un sangriento ataque. En menos de un día, las formidables fuerzas de Persia habían sido humilladas.

La estrategia de Demarato para la comunicación secreta se basaba simplemente en la ocultación del mensaje. Heródoto narró también otro incidente en el que la ocultación fue suficiente para conseguir el paso seguro de un mensaje. Él hizo la crónica de la historia de Histaiaeo, que quería alentar a Aristágoras de Mileto para que se rebelara contra el rey de Persia. Para transmitir sus instrucciones de forma segura, Histaiaeo afeitó la cabeza de su mensajero, escribió el mensaje en su cuero cabelludo y luego esperó a que le volviera a crecer el pelo. Evidentemente, aquél era un período de la Historia que toleraba una cierta falta de urgencia. El mensajero, que aparentemente no llevaba nada conflictivo, pudo viajar sin ser molestado. Al llegar a su destino, se afeitó la cabeza y se la mostró al receptor a quien iba destinado el mensaje.

La comunicación secreta lograda mediante la ocultación de la existencia de un mensaje se conoce como *esteganografía*, derivado de las palabras griegas *siéganos*, que significa «encubierto», y *grafo*, que significa «escribir». En los dos mil años que han transcurrido desde Heródoto, diversas formas de esteganografía han sido utilizadas por todo el mundo. Por ejemplo, en la China antigua se escribían mensajes sobre seda fina, que luego era aplastada hasta formar una pelotita diminuta que se recubría de cera. Entonces, el mensajero se tragaba la bola de cera. En el siglo XV, el científico italiano Giovanni Porta describió cómo esconder un mensaje dentro de un huevo cocido haciendo una tinta con una mezcla de una onza

de alumbre y una pinta de vinagre, y luego escribiendo en la cáscara. La solución penetra la cáscara porosa y deja un mensaje en la superficie de la albúmina del huevo duro, que sólo se puede leer si se pela el huevo. La esteganografía incluye también la práctica de escribir con tinta invisible. Ya en el siglo I, Plinio el Viejo explicó cómo la «leche» de la planta *Thithymallus* podía usarse como tinta invisible. Aunque se vuelve transparente al secarse, al calentarla suavemente se chamusca y se pone marrón. Muchos fluidos orgánicos se comportan de manera similar, porque son ricos en carbono y se chamuscan fácilmente. De hecho, es sabido que los espías modernos a los que se les ha acabado su tinta invisible habitual improvisan utilizando su propia orina.

La longevidad de la esteganografía corrobora que ofrece sin duda un nivel de seguridad, pero padece de una debilidad fundamental. Si registran al mensajero y descubren el mensaje, el contenido de la comunicación secreta se revela en el acto. La interceptación del mensaje compromete inmediatamente toda la seguridad. Un guarda concienzudo podría registrar rutinariamente a cualquier persona que cruce una frontera, y raspar cualquier tablilla cubierta de cera, calentar cualquier hoja de papel en blanco, pelar huevos cocidos, afeitar la cabeza de alguien, y así sucesivamente, e inevitablemente se producirían ocasiones en las que el mensaje quedaría revelado.

Por eso, paralelamente al desarrollo de la esteganografía, se produjo la evolución de la *criptografía,* término derivado de la palabra griega *kryptos,* que significa «escondido». El objetivo de la criptografía no es ocultar la existencia de un mensaje, sino más bien ocultar su significado, un proceso que se conoce como *codificación.* Para hacer que el mensaje sea ininteligible se codifica siguiendo un protocolo específico, sobre el cual se han puesto de acuerdo de antemano el emisor y el receptor a quien va dirigido. De esta forma, dicho receptor puede invertir el protocolo codificador y hacer que el mensaje sea comprensible. La ventaja de la criptografía es que si el enemigo intercepta un mensaje cifrado, éste es ilegible. Sin conocer el protocolo codificador, al enemigo le resultaría difícil, cuando no imposible, recrear el mensaje original a partir del texto cifrado.

Aunque la criptografía y la esteganografía son independientes, es posible codificar y ocultar un mismo mensaje para aumentar al máximo la seguridad. Por ejemplo, el

micropunto es una forma de esteganografía que se hizo popular durante la segunda guerra mundial. Agentes alemanes en Latinoamérica reducían fotográficamente una página de texto a un punto de menos de 1 milímetro de diámetro y luego escondían este micropunto sobre un punto y aparte de una carta aparentemente inocua. La primera vez que el FBI descubrió un micropunto fue en 1941, siguiendo un soplo que decía que los norteamericanos debían buscar en la superficie de una carta un brillo diminuto, indicativo de un minúsculo film Después de eso, los norteamericanos pudieron leer el contenido de la mayoría de micropuntos interceptados, excepto cuando los agentes alemanes habían tomado la precaución extra de codificar su mensaje antes de reducirlo. En tales casos de criptografía combinada con esteganografía, a veces los norteamericanos pudieron interceptar y bloquear las comunicaciones, pero no lograron averiguar nueva información sobre la actividad del espionaje alemán. De las dos ramas de la comunicación secreta, la criptografía es la más poderosa a causa de su habilidad para evitar que la información caiga en manos enemigas.

A su vez, la criptografía misma puede ser dividida en dos ramas, conocidas como *trasposición y sustitución.* En la trasposición, las letras del mensaje simplemente se colocan de otra manera, generando así un anagrama. Para mensajes muy cortos, como los de una sola palabra, este método es relativamente inseguro porque sólo hay un número limitado de maneras de combinar un puñado de letras. Por ejemplo, tres letras sólo pueden ser combinadas de seis maneras diferentes, por ejemplo, ron, rno, orn, onr, nro, ñor. Sin embargo, según el número de letras va incrementándose, el número de posibles combinaciones se dispara rápidamente, haciendo imposible volver al mensaje original a no ser que se conozca el proceso codificador exacto. Por ejemplo, considérese esta breve frase. Contiene solamente 35 letras, y, sin embargo, existen más de

50.000.000.000.000.000.000.000.000.00

de combinaciones distintas entre ellas. Si una persona pudiera revisar una combinación por segundo, y si todas las personas del mundo trabajaran día y noche, aún se necesitarían más de mil veces los siglos de vida del universo para

revisar todas las combinaciones.

Una trasposición de letras realizada al azar parece ofrecer un nivel muy alto de seguridad, porque a un interceptor enemigo le resultaría muy poco práctico descodificar incluso una breve frase. Pero hay un inconveniente. La trasposición genera eficazmente un anagrama increíblemente difícil, y si las letras se mezclan al azar, sin pies ni cabeza, la descodificación del anagrama es tan imposible para el recipiente a quien va dirigido como para un interceptor enemigo. Para que la trasposición sea efectiva, la combinación de letras necesita seguir un sistema sencillo, que haya sido acordado previamente por el emisor y el receptor, pero que se mantenga secreto frente al enemigo. Por ejemplo, los niños en la escuela a veces envían mensajes utilizando la trasposición de «riel», en la que el mensaje se escribe alternando las letras en dos líneas separadas. A continuación, la secuencia de letras de la línea inferior se añade al final de la secuencia de la línea superior, creándose así el mensaje cifrado final. Por ejemplo:

TU SECRETO ES TU PRISIONERO; SI LO SUELTAS, TÚ ERES SU PRISIONERO

⇓

TSCEOSURSOEOIOULATEESPIINR

UERTETPMNRSLSETSURSURSOEO

⇓

TSCEOSURSOEOIOULATEESPIINRUERTETPIINRSLSETSURSURSOEO

El receptor puede recuperar el mensaje simplemente invirtiendo el proceso. Hay varias otras formas de trasposición sistemática, incluida la cifra de riel de tres líneas, en la que primero se escribe el mensaje en tres líneas separadas en vez de dos. Como alternativa, se podría cambiar cada par de letras, de forma que la primera y la segunda cambien de lugar, así como la tercera y la cuarta, y así sucesivamente.

Otra forma de trasposición es la producida en el primer aparato criptográfico militar de la Historia, el *escitalo* espartano, que se remonta al siglo V a. C. El escitalo es una vara de madera sobre la que se enrosca una tira de cuero o de pergamino, tal como se muestra en la Figura 2. El emisor escribe el mensaje a lo largo de la

longitud del escitalo y luego desenrosca la tira, que ahora parece llevar una lista de letras sin sentido. El mensaje ha sido codificado. El mensajero llevaba la tira de cuero y, en un nuevo giro esteganográfico, a veces la llevaba de cinturón, con las letras ocultas en la parte interna. Para recuperar el mensaje, el receptor simplemente enrosca la tira de cuero en torno a un escitalo del mismo diámetro que el usado por el emisor. En el año 404 a. C. se presentó ante Lisandro de Esparta un mensajero, maltrecho y ensangrentado, uno de los cinco únicos supervivientes del arduo viaje desde Persia. El mensajero le dio su cinturón, y Lisandro lo enrolló en su escitalo, enterándose así de que Farnabazo de Persia planeaba atacarlo. Gracias al escitalo, Lisandro se preparó para afrontar ese ataque y lo repelió.

Figura 2. Cuando se desenrosca del escitalo (vara de madera) del emisor, la tira de cuero parece llevar una lista de letras al azar S, T, S, F... Sólo al volver a enroscar la tira alrededor de otro escitalo con el diámetro correcto reaparecerá el mensaje.

La alternativa a la trasposición es la sustitución. Una de las descripciones más antiguas de codificación por sustitución aparece en el *Kamasutra,* un texto escrito en el siglo IV por el erudito brahmín Vatsyayana, pero que se basa en manuscritos que se remontan al siglo IV a. C. El *Kamasutra* recomienda que las mujeres deberían estudiar 64 artes, como cocinar, saber vestirse, dar masajes y preparar perfumes. La lista incluye también algunas artes menos obvias, como la prestidigitación, el ajedrez, la encuadernación de libros y la carpintería. El número 45 de la lista es *mlecchita-vikalpa,* el arte de la escritura secreta, preconizado para ayudar a las mujeres a ocultar los detalles de sus relaciones amorosas. Una de las

técnicas recomendadas es emparejar al azar las letras del alfabeto y luego sustituir cada letra del mensaje original por su pareja. Si aplicamos este principio al alfabeto romano podríamos emparejar las letras de esta manera:

A	D	H	I	K	M	O	R	S	U	W	Y	Z
↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕
V	X	B	G	J	C	Q	L	N	E	F	P	T

Entonces, en vez de encontrémonos a medianoche, el emisor escribiría

USMQSZLUCQSQN V CUXGVSQMBU.

Esta forma de escritura secreta se conoce como cifra de sustitución porque cada letra del texto llano se sustituye por una letra diferente, funcionando así de manera complementaria a la cifra por trasposición. En la trasposición, cada letra mantiene su identidad pero cambia su posición, mientras que en la sustitución, cada letra cambia su identidad pero mantiene su posición El primer uso documentado de una cifra de sustitución con propósitos militares aparece en *La guerra de las Galias*, de Julio César. César describe cómo envió un mensaje a Cicerón, que se encontraba sitiado y a punto de rendirse. La sustitución reemplazó las letras romanas por letras griegas, haciendo que el mensaje resultara ininteligible para el enemigo. César describió la dramática entrega del mensaje:

> *Se dieron instrucciones al mensajero para que si no pudiese acercarse, arrojara una lanza, con la carta sujeta a la correa, al atrincheramiento del campamento. Temiendo el peligro, el galo arrojó la lanza, tal como se le había dicho. Por casualidad, la lanza se clavó en la torre, y durante dos días nuestras tropas no la vieron; al tercer día fue divisada por un soldado, que la bajó y la llevó a Cicerón. Después de leerla detalladamente, éste la narró en un desfile de las tropas, proporcionando a todos la mayor de las alegrías.*

César utilizó la escritura secreta tan frecuentemente que Valerio Probo escribió un tratado entero acerca de sus cifras, que desgraciadamente no ha sobrevivido. Sin embargo, gracias a la obra de Suetonio *Vidas de los Césares LVI*, escrita en el siglo segundo de nuestra era, tenemos una descripción detallada de uno de los tipos de cifra de sustitución utilizado por César. El emperador sencillamente sustituía cada letra del mensaje con la letra que está tres lugares más adelante en el alfabeto. Los criptógrafos a menudo piensan en términos de *alfabeto llano*, el alfabeto que se usa para escribir el mensaje original, y *alfabeto cifrado,* las letras que sustituyen a las del alfabeto llano. Cuando el alfabeto llano se coloca sobre el alfabeto cifrado, tal como se muestra en la Figura 3, queda claro que el alfabeto cifrado ha sido movido tres lugares, por lo que esta forma de sustitución a menudo es llamada la *cifra de cambio del César*, o simplemente, la cifra del César. Una cifra es el nombre que se da a cualquier forma de sustitución criptográfica en la que cada letra es reemplazada por otra letra o símbolo.

Aunque Suetonio sólo menciona un cambio del César de tres lugares, es evidente que al utilizar cualquier cambio de entre 1 y 25 lugares es posible generar 25 cifras distintas. De hecho, si no nos limitamos a cambiar

ordenadamente el alfabeto y permitimos que el alfabeto cifrado sea cualquier combinación del alfabeto llano, podemos generar un número aún mayor de cifras distintas. Hay más de 400.000.000.000.000.000.000.000.000 combinaciones posibles y, por tanto, de cifras diferentes.

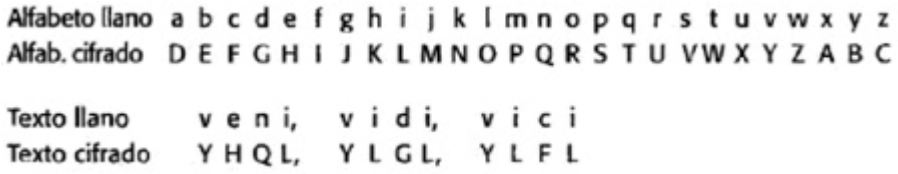


Figura 3. La cifra del César aplicada a un mensaje corto. La cifra del César se basa en un alfabeto cifrado que se ha movido un cierto número de lugares (en este caso, tres) con respecto al alfabeto llano. La convención en la criptografía es escribir el alfabeto llano en letras minúsculas, y el alfabeto cifrado en mayúsculas. De manera similar, el mensaje original, el texto llano, se escribe en minúsculas y el texto cifrado, en mayúsculas.

Cada una de las cifras puede ser considerada en términos de un método de codificación general, conocido como el *algoritmo*, y una *clave*, que especifica los detalles exactos de una codificación particular. En este caso, el algoritmo conlleva sustituir cada letra del alfabeto llano por una letra proveniente de un alfabeto cifrado, y el alfabeto cifrado puede consistir en cualquier combinación del alfabeto llano. La clave define el alfabeto cifrado exacto que hay que usar para una codificación particular. La relación entre el algoritmo y la clave queda ilustrada en la Figura 4.

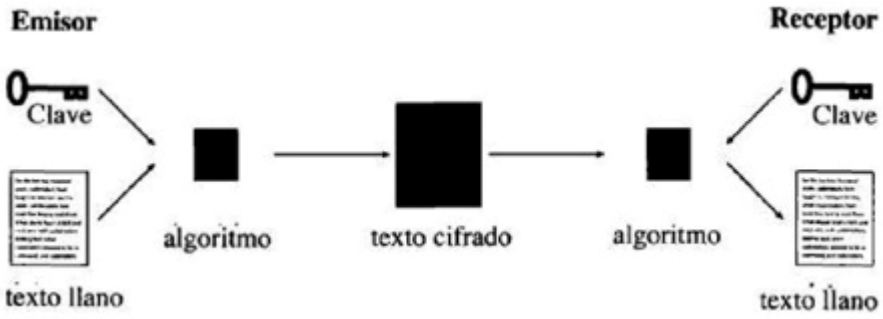


Figura 4. Para codificar un mensaje de texto llano, el emisor lo pasa por un algoritmo de codificación. El algoritmo es un sistema general de codificación y necesita ser especificado exactamente seleccionando una clave. Al aplicar la clave y el algoritmo juntos a un texto llano se genera el mensaje codificado, o texto cifrado. Puede que el texto cifrado sea interceptado por un enemigo mientras está siendo transmitido al receptor, pero el enemigo no podría descifrar el mensaje. Sin embargo, el receptor, que conoce tanto la clave como el algoritmo utilizados por el emisor, puede reconvertir el texto cifrado en el mensaje en texto llano.

Un enemigo que estudie un mensaje codificado interceptado puede tener una fuerte sospecha de la existencia del algoritmo, pero quizá no conozca la clave exacta. Por ejemplo, puede muy bien sospechar que cada letra del texto llano ha sido reemplazada por una letra diferente según un alfabeto cifrado particular, pero es improbable que sepa qué alfabeto cifrado ha sido utilizado. Si el alfabeto cifrado, la clave, se mantiene como secreto bien guardado entre el emisor y el receptor, el enemigo no podrá descifrar el mensaje interceptado. La importancia de la clave, a diferencia del algoritmo, es un principio estable de la criptografía. Fue expuesto

definitivamente en 1883 por el lingüista holandés Augusto Kerckhoffs von Nieuwenhof en su libro *La Cryptographie militaire:* el «Principio de Kerckhoffs: La seguridad de un cripto-sistema no debe depender de mantener secreto el cripto-algoritmo. La seguridad depende sólo de mantener secreta la clave».

Además de mantener secreta la clave, un sistema de cifra seguro debe tener también una amplia gama de claves potenciales. Por ejemplo, si el emisor utiliza la cifra de cambio del César para cifrar un mensaje, la codificación es relativamente débil, porque sólo hay 25 claves potenciales. Desde el punto de vista del enemigo, si éste intercepta el mensaje y sospecha que el algoritmo utilizado es el cambio del César, entonces sólo tiene que revisar las 25 posibilidades. Sin embargo, si el emisor utiliza el algoritmo de sustitución más general, que permite que el alfabeto cifrado sea cualquier combinación del alfabeto llano, entonces hay

400.000.000.000.000.000.000.000.000

claves posibles entre las que elegir. Una de ellas es la que se muestra en la Figura 5. Desde el punto de vista del enemigo, si el mensaje es interceptado y se conoce el algoritmo, queda aún la horrenda tarea de revisar todas las claves posibles. Si un agente enemigo fuera capaz de revisar una de las 400.000.000.000.000.000.000.000.000 claves posibles por segundo le llevaría aproximadamente un billón de veces los siglos de vida del universo revisar todas ellas y descifrar el mensaje.

Figura 5. Un ejemplo del algoritmo de sustitución general, en el que cada letra del texto llano se sustituye por otra letra según una clave. La clave se define mediante el alfabeto cifrado, que puede ser cualquier combinación del alfabeto llano.

La ventaja de este tipo de cifra radica en que es fácil de poner en práctica, a la vez que ofrece un alto nivel de seguridad. Para el emisor es fácil definir la clave, que

consiste meramente en determinar el orden de las 26 letras en el alfabeto cifrado elegido, y, sin embargo, al enemigo le será prácticamente imposible revisar todas las claves posibles por el denominado «ataque por la fuerza bruta». La simplicidad de la clave es importante, porque el emisor y el receptor tienen que compartir el conocimiento de la clave, y cuanto más simple sea ésta, menor será la posibilidad de un malentendido.

De hecho, es posible una clave aún más simple si el emisor está dispuesto a aceptar una ligera reducción del número de claves potenciales. En vez de combinar al azar el alfabeto llano para conseguir el alfabeto cifrado, el emisor elige una *palabra clave* o una *frase clave.* Por ejemplo, para utilizar JULIUS CAESAR como frase clave hay que comenzar por quitar los espacios y las letras repetidas (JULISCAER), y luego usar esto como el principio del alfabeto cifrado. El resto del alfabeto cifrado es simplemente el resto de las letras del alfabeto, en su orden correcto, comenzando donde acaba la frase clave. De esta forma, el alfabeto cifrado sería así:

Alfabeto llano	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Alfab. cifrado	J	U	L	I	S	C	A	E	R	T	V	W	X	Y	Z	B	D	F	G	H	K	M	N	O	P	Q

La ventaja de confeccionar un alfabeto cifrado de esta manera radica en que es fácil memorizar la palabra o la frase clave, y con ello el alfabeto cifrado. Esto es importante, porque si el emisor tiene que guardar el alfabeto en un trozo de papel, el enemigo puede capturar el papel, descubrir la clave y leer cualquier comunicación que haya sido codificada con ella. Sin embargo, si la clave puede ser aprendida de memoria, es menos probable que caiga en manos enemigas. Evidentemente, el número de alfabetos cifrados generados por frases clave es menor que el número de alfabetos cifrados generados sin restricción, pero el número sigue siendo inmenso, y al enemigo le resultaría prácticamente imposible descifrar un mensaje probando todas las frases clave posibles.

Esta simplicidad y fortaleza hicieron que la cifra de sustitución dominara el arte de la escritura secreta a lo largo del primer milenio de nuestra era. Los creadores de códigos habían desarrollado un sistema para garantizar la comunicación segura, de manera que no era necesario ningún nuevo avance: sin

necesidad, no era necesaria ninguna nueva invención. La responsabilidad había recaído sobre los descifradores de códigos, que trataban de descifrar la cifra de sustitución. ¿Había alguna manera de que un enemigo interceptor desenmarañase un mensaje codificado? Muchos estudiosos antiguos consideraban que la cifra de sustitución era indescifrable, gracias al gigantesco número de claves posibles, y durante siglos esto parecía ser verdad. Sin embargo, los descifradores encontraron finalmente un atajo en el proceso de examinar exhaustivamente todas las claves. En vez de tardar billones de años en descifrar una cifra, el atajo podía revelar el mensaje en cuestión de minutos. El gran paso adelante sucedió en Oriente y requirió una brillante combinación de lingüística, estadística y devoción religiosa.

2. Los criptoanalistas árabes

Cuando tenía alrededor de cuarenta años, Mahoma empezó a visitar regularmente una cueva solitaria en el monte Hira, en las afueras de La Meca. Se trataba de un paraje de retiro, un lugar para la oración, la meditación y la contemplación. Fue durante un período de profunda reflexión, hacia el año 610 de nuestra era, cuando fue visitado por el arcángel Gabriel, que proclamó que Mahoma iba a ser el mensajero de Dios. Ésta fue la primera de una serie de revelaciones que continuaron hasta la muerte de Mahoma, ocurrida unos veinte años después. Las revelaciones fueron anotadas por varios escribientes durante la vida del Profeta, pero sólo como fragmentos, y quedó para Abú Bakr, el primer califa del islam, la tarea de reunir todos ellos en un solo texto. La labor la continuó Umar, el segundo califa, y su hija Hafsa, y fue finalmente completada por Utmán, el tercer califa. Cada revelación se convirtió en uno de los 114 capítulos del Corán.

El califa en el poder era el responsable de continuar la labor del Profeta, defendiendo sus enseñanzas y difundiendo sus palabras. Entre el nombramiento de Abú Bakr en el año 632 y la muerte del cuarto califa, Alí, en el año 661, el islam se extendió hasta que la mitad del mundo conocido estuvo bajo el dominio musulmán. Luego, en el año 750, tras un siglo de consolidación, el comienzo del califato (o dinastía) abasí anunció la edad dorada de la civilización islámica. Las artes y las ciencias florecieron en igual medida. Los artesanos islámicos nos legaron pinturas magníficas, elaboradas tallas y los textiles más minuciosos de la Historia, mientras

que el legado de los científicos islámicos resulta evidente en la gran cantidad de palabras árabes que aparecen en el léxico de la ciencia moderna, tales como *álgebra, alcalino o cénit.*

La riqueza de la cultura islámica fue en gran medida el resultado de una sociedad rica y pacífica. Los califas abastes estaban menos interesados en la conquista que sus predecesores, y en vez de ello, dirigieron sus esfuerzos a establecer una sociedad organizada y próspera. Los impuestos bajos fomentaron el crecimiento de los negocios, así como del comercio y la industria, mientras que las leyes estrictas redujeron la corrupción y protegieron a los ciudadanos. Todo ello se apoyaba en un eficaz sistema de gobierno, y a su vez, los gobernantes se apoyaban en la comunicación segura, lograda mediante el uso de la codificación. Además de cifrar los delicados asuntos de estado, está documentado que los funcionarios protegían los archivos de los impuestos, demostrando un uso general y rutinario de la criptografía. Aún más evidencia de ello nos llega de muchos manuales administrativos, tales como el *Adab al- Kuttab* («El Manual de los Secretarios»), del siglo X, que incluye secciones dedicadas a la criptografía.

Los gobernantes y funcionarios utilizaban generalmente un alfabeto cifrado que era simplemente una variación del orden del alfabeto llano, tal como lo describí antes, pero también usaban alfabetos cifrados que contenían otros tipos de símbolos. Por ejemplo, la a del alfabeto llano podía ser reemplazada por # en el alfabeto cifrado, la b podía ser reemplazada por +, y así sucesivamente. La *cifra de sustitución monoalfabética* es el nombre general que se da a cualquier cifra de sustitución en la que el alfabeto cifrado consiste en letras o en símbolos, o en una mezcla de ambos. Todas las cifras de sustitución que hemos visto hasta ahora pertenecen a esta categoría general.

Si los árabes se hubieran limitado a familiarizarse con el uso de la cifra de sustitución monoalfabética no merecerían una mención muy significativa en ninguna historia de la criptografía. Sin embargo, además de utilizar cifras, los eruditos árabes también eran capaces de destruirlas. De hecho, fueron ellos quienes inventaron el *criptoanálisis*, la ciencia de descifrar un mensaje sin conocer la clave. Mientras el criptógrafo desarrolla nuevos métodos de escritura secreta, es el criptoanalista el que se esfuerza por encontrar debilidades en estos métodos, para

penetrar en los mensajes secretos. Los criptoanalistas árabes lograron encontrar un método para descifrar la cifra de sustitución monoalfabética, la cual había permanecido invulnerable durante muchos siglos.

El criptoanálisis no podía ser inventado hasta que una civilización hubiese alcanzado un nivel suficientemente sofisticado de erudición en varias disciplinas, incluidas las matemáticas, la estadística y la lingüística. La civilización musulmana constituyó una cuna ideal para el criptoanálisis porque el islam exige justicia en todas las esferas de la actividad humana, y lograr esto requiere conocimiento, o *ilm.* Todo musulmán está obligado a buscar el conocimiento en todas sus formas, y el éxito económico del califato abasí significó que los eruditos tuvieron el tiempo, el dinero y los materiales necesarios para cumplir con su deber. Se esforzaron por adquirir los conocimientos de las civilizaciones anteriores, obteniendo textos egipcios, babilonios, indios, chinos, parsis, sirios, armenios, hebreos y romanos, y traduciéndolos al árabe. En el año 815, el califa Al Mamún estableció en Bagdad la Bait al Hikmah («Casa de la Sabiduría»), una biblioteca y un centro de traducción.

A la vez que ganaba conocimiento, la civilización islámica fue también capaz de esparcirlo, porque había adquirido el arte de hacer papel de los chinos. La fabricación de papel dio lugar a la profesión de *warraqin*, «los que manejan el papel», máquinas fotocopiadoras humanas que copiaban manuscritos y suministraban a la creciente industria editorial. En su punto álgido decenas de miles de libros se publicaban cada año, y en un solo suburbio de Bagdad había más de cien librerías. Junto a clásicos como los *Cuentos de las mil y una noches*, estas librerías vendían también libros de texto de todos los temas imaginables y contribuían a apoyar la sociedad más alfabetizada y culta del mundo.

Además de en una mayor comprensión de temas seculares, el invento del criptoanálisis se basó también en el crecimiento de la erudición religiosa. Se establecieron importantes escuelas teológicas en Basora, Kufa y Bagdad, en las que los teólogos examinaban minuciosamente las revelaciones de Mahoma, tal como aparecían en el Corán. Los teólogos tenían interés en establecer la cronología de las revelaciones, lo que hacían contando las frecuencias de las palabras contenidas en cada revelación. La teoría era que ciertas palabras habían evolucionado relativamente hacía poco, y por eso, si una revelación contenía un alto número de

estas palabras más nuevas, indicaría que apareció después en la cronología. Los teólogos estudiaron también el *Hadith,* que consta de las afirmaciones diarias del Profeta. Los teólogos trataron de demostrar que cada aseveración era efectivamente atribuible a Mahoma. Esto se hizo estudiando la etimología de las palabras y la estructura de las frases, para comprobar si textos particulares mostraban consistencia con los patrones lingüísticos del Profeta.

Resulta significativo que los eruditos religiosos no limitaran su análisis minucioso al nivel de las palabras. También analizaron las letras individuales y descubrieron en particular que algunas letras son más corrientes que otras. Las letras a y 1 son las más frecuentes en árabe, en parte a causa del artículo definido al-, mientras que letras como la j sólo aparecen con una décima parte de la frecuencia. Esta observación aparentemente inocua conduciría al primer gran avance hacia el criptoanálisis.

Aunque no se sabe quién fue el primero en darse cuenta de que la variación en la frecuencia de las letras podía explotarse para descifrar cifras, la descripción más antigua que se conoce de la técnica es del científico del siglo IX Abú Yusuf Yaqub ibn Ishaq ibn as Sabbah ibn ‘omran ibn Ismail al Kindi. Conocido como «el filósofo de los árabes», Al Kindi fue el autor de 290 libros de medicina, astronomía, matemáticas, lingüística y música. Su tratado más importante, que no fue redescubierto hasta 1987 en el Archivo Sulaimaniyyah Ottoman de Estambul, se titulaba Sobre *el desciframiento de mensajes criptográficos*; la primera página se muestra en la Figura 6.

Aunque contiene detallados debates sobre estadística, fonética árabe y sintaxis árabe, el revolucionario sistema de criptoanálisis de Al Kindi está compendiado en dos breves párrafos:

> *Una manera de resolver un mensaje cifrado, si sabemos en qué lengua está escrito, es encontrar un texto llano diferente escrito en la misma lengua y que sea lo suficientemente largo para llenar alrededor de una hoja, y luego contar cuántas veces aparece cada letra. A la letra que aparece con más frecuencia la llamamos «primera», a la siguiente en frecuencia la llamamos «segunda», a la siguiente «tercera», y así sucesivamente, hasta que hayamos*

cubierto todas las letras que aparecen en la muestra de texto llano. Luego observamos el texto cifrado que queremos resolver y clasificamos sus símbolos de la misma manera. Encontramos el símbolo que aparece con más frecuencia y lo sustituimos con la forma de la letra «primera» de la muestra de texto llano, el siguiente símbolo más corriente lo sustituimos por la forma de la letra «segunda», y el siguiente en frecuencia lo cambiamos por la forma de la letra «tercera», y así sucesivamente, hasta que hayamos cubierto todos los símbolos del criptograma que queremos resolver.

Figura 6. La primera página del manuscrito Sobre el desciframiento de mensaje criptográficos, de Al Kindi, que contiene la descripción más antigua que se conoce del criptoanálisis mediante análisis de frecuencia.

La explicación de Al Kindi es más fácil de explicar desde el punto de vista del alfabeto inglés[1]. En primer lugar, es necesario examinar un fragmento extenso de texto inglés normal, o quizá varios, para establecer la frecuencia de cada letra del alfabeto. En inglés, la e es la letra más corriente, seguida de la t, luego la a, y así sucesivamente, tal como aparece en la Tabla 1. Luego, hay que examinar el texto cifrado y determinar la frecuencia de cada letra. Si la letra más corriente en el texto cifrado es, por ejemplo, la J, entonces parecería probable que sustituyera a la e. Y si la segunda letra más frecuente en el texto cifrado es la P, probablemente sustituya a la t, y así sucesivamente. La técnica de Al Kindi, conocida como *análisis de frecuencia*, muestra que no es necesario revisar cada una de los billones de claves potenciales. En vez de ello, es posible revelar el contenido de un mensaje codificado analizando simplemente la frecuencia de los caracteres en el texto cifrado.

Letra	Porcentaje	Letra	Porcentaje
a	8,2	n	6,7
b	1,5	o	7,5
c	2,8	p	1,9
d	4,3	q	0,1
e	12,7	r	6,0
f	2,2	s	6,3
g	2,0	t	9,1
h	6,1	u	2,8
i	7,0	v	1,0
j	0,2	w	2,4
k	0,8	x	0,2
l	4,0	y	2,0
m	2,4	z	0,1

Tabla 1. Esta tabla de frecuencias relativas en la lengua inglesa se basa en pasajes tomados de periódicos y novelas, y la muestra total consistió en 100.362 caracteres alfabéticos. La tabla fue recopilada por H. Beker y F. Piper, y fue publica da originalmente en Cipher Systems: The Protection Of Communication («Sistema de cifra: La protección de la comunicación»).

[1] Evidentemente, esta afirmación viene dada por el hecho de que el libro original está escrito en inglés. En términos generales, el «alfabeto castellano» no ofrecería mayor dificultad. (N. del T.)

Sin embargo, no es posible aplicar incondicionalmente la receta de Al Kindi para el criptoanálisis, porque la lista estándar de frecuencias de la Tabla 1 es sólo un promedio y no corresponderá exactamente a las frecuencias de cada texto. Por ejemplo, un breve mensaje que trate del efecto de la atmósfera en el movimiento de los cuadrúpedos rayados de África no se ajustará al análisis de frecuencia normal: «From Zanzíbar to Zambia and Zaire, ozone zones make zebras run zany zigzags»[2]. En general, es probable que los textos cortos se desvíen significativamente de las frecuencias normales, y si tienen menos de cien letras, su desciframiento será muy difícil. Por otra parte, es más probable que los textos más extensos sigan las frecuencias normales, aunque esto no es siempre así. En 1969, el autor francés Georges Perec escribió *La Disparition*, una novela de 200 páginas en la que no utilizó ninguna palabra que contuviera la letra e. Doblemente extraordinario es el hecho de que el novelista y crítico inglés Gilbert Adair consiguiera traducir *La Disparition* al inglés siguiendo aún la norma de Perec de no utilizar la letra e. Aunque parezca mentira, la traducción de Adair, titulada *A Void*, se lee con facilidad y amenidad. Si el libro entero fuera codificado mediante una cifra de sustitución monoalfabética, un intento ingenuo de descifrarlo se vería entorpecido por la completa ausencia de la letra que aparece más frecuentemente en la lengua inglesa.

Tras haber descrito la primera herramienta del criptoanálisis, a continuación ofreceré un ejemplo de cómo se utiliza el análisis de frecuencia para descifrar un texto cifrado. No he querido saturar todo el libro con ejemplos de criptoanálisis, pero con el análisis de frecuencia hago una excepción. Esto se debe en parte a que el análisis de frecuencia no es tan difícil como parece y en parte a que es la herramienta criptoanalítica primaria. Además, el ejemplo siguiente ofrece una idea clara del *modus operandi* del criptoanalista. Aunque el análisis de frecuencia requiere una buena dosis de pensamiento lógico, se verá que también exige astucia, intuición, flexibilidad y dotes de conjetura.

3. Criptoanálisis de un texto cifrado

[2] «De Zanzíbar a Zambia y Zaire, las zonas del ozono hacen que las cebras zigzagueen de manera excéntrica». (N. del T.)

PCQ VMJYPD LBYK LYSO
KBXBJXWXV BXV ZCJPO EYPD
KBXBJYUXJ LBJOO KCPK. CP LBO
LBCMKXPV XPV IYJKL PYDBL,
QBOP KBO BXV OPVOV LBO LXRO
CI SX'XJMI, KBO JCKO XPV
EYKKOV LBO DJCMPV ZOICJO
BYS, KXUYPD: 'DJOXL EYPD, ICJ X
LBCMKXPV XPV CPO PYDBLK Y
BXNO ZOOP JOACMPLYPD LC UCM
LBO IXZROK CI FXKL XDOK XPV
LBO RODOPVK CI XPAYOPL
EYPDK. SXU Y SXEO KC ZCRV XK
LC AJXNO X IXNCMJ CI UCMJ
SXGOKLU?'

OFYRCDMO, LXROK IJCS LBO
LBCMKXPV XPV CPO PYDBLK

Imagine que hemos interceptado este mensaje codificado. Nuestro desafío es descifrarlo. Sabemos que el texto es en inglés y que ha sido codificado según una cifra de sustitución monoalfabética, pero no tenemos ni idea de la clave. Buscar todas las claves posibles es poco factible, así que debemos aplicar el análisis de frecuencia. Lo que viene a continuación es una guía detallada del criptoanálisis del texto cifrado, pero si usted se siente con mucha seguridad puede que prefiera ignorar esta guía e intentar su propio criptoanálisis independiente.

La reacción inmediata de cualquier criptoanalista al ver semejante texto cifrado es analizar la frecuencia de todas las letras, lo que da como resultado la Tabla 2. Como era de esperar, la frecuencia de las letras varía. La cuestión es: ¿podemos identificar lo que representa alguna de ellas, basándonos en sus frecuencias? El texto cifrado es relativamente corto, de forma que no podemos aplicar ciegamente el análisis de frecuencia. Sería ingenuo asumir que la letra más corriente en el texto cifrado, la O, representa a la letra más corriente en inglés, la e, o que la octava

letra más frecuente en el texto cifrado, la Y, representa a la octava letra más frecuente en inglés, la h. Una aplicación ciega del criptoanálisis daría por resultado un galimatías. Por ejemplo, la primera palabra, PCQ, sería descifrada como aov.

Sin embargo, podemos comenzar prestando atención a las tres únicas letras que aparecen más de treinta veces en el texto cifrado, es decir, la O, la X y la P. Resulta bastante seguro asumir que las letras más corrientes en el texto cifrado representan probablemente a las letras más corrientes del alfabeto inglés, pero no necesariamente en el orden correcto. En otras palabras, no podemos estar seguros de que 0=e, X=t y P=a pero podemos asumir tentativamente que:

(O = e, t o a) (X = e, t o a) (P = e, t o a)

Letra	Frecuencia		Letra	Frecuencia	
	Apariciones	Porcentaje		Apariciones	Porcentaje
A	3	0,9	N	3	0,9
B	25	7,4	O	38	11,2
C	27	8,0	P	31	9,2
D	14	4,1	Q	2	0,6
E	5	1,5	R	6	1,8
F	2	0,6	S	7	2,1
G	1	0,3	T	0	0,0
H	0	0,0	U	6	1,8
I	11	3,3	V	18	5,3
J	18	5,3	W	1	0,3
K	26	7,7	X	34	10,1
L	25	7,4	Y	19	5,6
M	11	3,3	Z	5	1,5

Tabla 2, Análisis de frecuencia del mensaje codificado.

Para continuar con confianza, y precisar la identidad de las tres letras más frecuentes, la O, la X y la P, necesitamos una forma más sutil de análisis de frecuencia. En vez de simplemente contar la frecuencia de las tres letras podemos centrarnos en lo a menudo que aparecen junto a todas las demás letras. Por ejemplo, ¿aparece la letra O antes o después de varias otras letras, o tiende a estar sólo junto a unas pocas letras especiales? Responder esta pregunta será una buena indicación de si la O representa una vocal o una consonante. Si la O representara

una vocal, aparecería antes y después de la mayoría de las demás letras, mientras que si representara una consonante, tendería a evitar a muchas de las demás letras. Por ejemplo, la letra e puede aparecer antes y después de prácticamente cualquier otra letra, pero la letra t raramente se ve antes o después de la b, la d, la g, la j, la k, la m, la q o la v.

La siguiente tabla toma las tres letras más corrientes en el texto cifrado, la O, la X y la P, y pone en una lista la frecuencia con la que cada una de ellas aparece antes o después de cada letra. Por ejemplo, la O aparece antes de la A en 1 ocasión, pero nunca aparece inmediatamente después de ella, por lo que da un total de 1 en la primera casilla. La letra O aparece junto a la mayoría de las letras, y sólo hay 7 a las que evita completamente, lo que aparece representado por los 7 ceros en la hilera de la O. La letra X es igual de sociable, porque también aparece junto a la mayoría de las letras y sólo evita a 8 de ellas. Sin embargo, la letra P es mucho menos amistosa. Tiende a mostrarse sólo junto a unas pocas letras y evita a 15 de ellas. Esta evidencia sugiere que la O y la X representan a vocales, mientras que la P representa a una consonante.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
O	1	9	0	3	1	1	1	0	1	4	6	0	1	2	2	8	0	4	1	0	0	3	0	1	1	2
X	0	7	0	1	1	1	1	0	2	4	6	3	0	3	1	9	0	2	4	0	3	3	2	0	0	1
P	1	0	5	6	0	0	0	0	0	1	1	2	2	0	8	0	0	0	0	0	0	11	0	9	9	0

Ahora debemos preguntarnos qué vocales están representadas por la O y la X. Probablemente sean la e y la a, las dos vocales más populares en la lengua inglesa, ¿es 0=e y X=a, o bien 0=a y X=e? Un rasgo interesante del texto cifrado es que la combinación OO aparece dos veces, mientras que XX no aparece en absoluto. Como ee aparece mucho más a menudo que aa en los textos llanos en inglés, es probable que 0=e y X=a

Llegado este punto, ya hemos identificado con seguridad dos de las letras del texto cifrado. Nuestra conclusión de que X=a se ve apoyada por el hecho que X aparece sola en el texto cifrado, y a una de las dos únicas palabras inglesas que sólo tienen una letra. La única otra letra que aparece sola en el texto cifrado es la Y, por lo que parece muy probable que represente a la única otra palabra inglesa de una sola

letra, que es i. Centrarse en palabras de una sola letra es un truco criptoanalítico estándar. Este truco en particular funciona solamente porque este texto cifrado aún tiene espacios entre las palabras. A menudo, el criptógrafo quitará todos los espacios para hacer que resulte más difícil para un enemigo interceptor descifrar el mensaje.

Aunque tenemos espacios entre las palabras, el siguiente truco también funcionaría aunque el texto cifrado apareciera fundido en una sola serie de caracteres. El truco nos permite localizar la letra h, una vez que hayamos identificado la letra e. En la lengua inglesa, la letra h aparece frecuentemente ante la letra e (como en the, then, they, etc.), pero muy raramente después de la e. La siguiente tabla muestra la frecuencia en que O, que creemos que representa a la e, aparece antes y después de las demás letras en el texto cifrado. La tabla sugiere que B representa a la h, porque aparece 9 veces ante 0, pero nunca detrás de ella. Ninguna otra letra en la tabla tiene una relación tan asimétrica con O.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
tras O	1	0	0	1	0	1	0	0	1	0	4	0	0	0	2	5	0	0	0	0	0	2	0	1	0	0
ante O	0	9	0	2	1	0	1	0	0	4	2	0	1	2	2	3	0	4	1	0	0	1	0	0	1	2

Cada letra de la lengua inglesa tiene su propia personalidad, que incluye su frecuencia y su relación con las demás letras. Es esta personalidad la que nos permite establecer la verdadera identidad de una letra, incluso cuando ha sido disfrazada mediante la sustitución monoalfabética.

Ya hemos establecido con seguridad cuatro letras, 0=e, X=a, Y=i y B=h, y podemos comenzar a reemplazar algunas de las letras del texto cifrado por sus equivalentes de texto llano. Me ajustaré a la convención de mantener las letras de texto cifrado en mayúscula, poniendo las letras de texto llano en minúscula. Esto ayudará a distinguir entre aquellas letras que aún debemos identificar y las que ya han sido identificadas.

PCQ VMJiPD LhiK LiSe KhahJaWaV
haV ZCJPe EiPD KhahJiUaJ LhJee
KCPK. CP Lhe LhCMKaPV aPV liJKL
PiDhL, QheP Khe haV ePVeV Lhe LaRe
CI Sa'aJMI, Khe JCKe aPV EiKKev Lhe
DJCMPV ZelCJe hiS, KaUiPD: 'DJeaL
EiPD, ICJ a LhCMKaPV aPV CPe
PiDhLK i haNe ZeeP JeACMPLiPD LC
UCM Lhe laZReK CI FaKL aDeK aPV
Lhe ReDePVK CI aPAiePL EiPDK. SaU
i SaEe KC ZCRV aK LC AJaNe a
IaNCMJ CI UCMJ SaGeKLU?'

eFiRCDMe, LaReK IJCS Lhe
LhCMKaPV aPV CPe PiDhLK

Este simple paso nos ayuda a identificar varias otras letras, porque podemos adivinar algunas de las palabras del texto cifrado. Por ejemplo, las palabras de tres letras más corrientes en inglés son the y and, y éstas resultan relativamente fáciles de localizar: Lhe, que aparece seis veces, y aPV, que aparece cinco veces. Por tanto, la L probablemente represente a la t, la P probablemente represente a la n y la V probablemente represente a la d. Ahora podemos reemplazar estas letras del texto cifrado por sus valores verdaderos:

nCQ dMJinD thiK tiSe KhahJaWad had
ZCJne EinD KhahJiUaJ thJee KCnK.
Cn the thCMKand and liJKt niDht, Qhen
Khe had ended the taRe CI Sa'aJMI,
Khe JCKe and EiKKed the DJCMnd
ZeICJe hiS, KaUinD: 'DJeat EinD, ICJ a
thCMKand and Cne niDhtK i haNe Zeen
JeACMntinD tC UCM the laZReK CI
FaKt aDeK and the ReDendK CI
anAient EinDK. SaU i SaEe KC ZCRd
aK tC AJaNe a laNCMJ CI UCMJ
SaGeKtU?'
eFiRCDMe, taReK IJCS the thCMKand
and Cne niDhtK

Una vez que hemos identificado unas pocas letras, el criptoanálisis avanza rápidamente. Por ejemplo, la palabra al comienzo de la segunda frase es Cn. Toda palabra inglesa contiene al menos una vocal, así que C debe ser una vocal. Sólo quedan dos vocales sin identificar, la u y la o; la u no encaja, así que C debe representar a la o. También tenemos la palabra Khe, lo que implica que K representa a la t o a la s. Pero ya sabemos que L = t, así que queda claro que K=s. Una vez identificadas estas dos letras, las insertamos en el texto cifrado, y entonces aparece la frase thoMsand and one niDhts. Una suposición razonable sería que se trata de *thousand and one nights* (mil y una noches), y parece probable asumir que la línea final nos está diciendo que se trata de un fragmento de los *Cuentos de las mil y una noches.* Esto implica que M = u, l = f, J = r, D = g, R = 1 y S = m
Podríamos continuar intentando identificar otras letras adivinando otras palabras, pero en vez de ello observemos lo que sabemos sobre el alfabeto llano y el alfabeto cifrado. Estos dos alfabetos forman la clave y fueron utilizados por el criptógrafo para llevar a cabo la sustitución que codificó el mensaje. Hasta ahora, identificando los valores verdaderos de las letras del alfabeto cifrado hemos estado deduciendo

eficazmente los detalles del alfabeto cifrado. Un resumen de nuestros logros, hasta estos momentos, muestra los siguientes alfabetos llano y cifrado:

Alfabeto llano	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Alfab. cifrado	X	-	-	V	O	I	D	B	Y	-	-	R	S	P	C	-	-	J	K	L	M	-	-	-	-	-

Examinando el alfabeto cifrado parcial, podemos completar el criptoanálisis. La secuencia VOIDBY en el alfabeto cifrado sugiere que el criptógrafo ha elegido una frase clave como base para la clave. Un poco de imaginación es suficiente para sugerir que la frase clave podría ser A VOID BY GEORGES PEREC[3] , que se reduce a AVOIDBYGERSPC tras quitar los espacios y las repeticiones. Después de eso, las letras continúan en orden alfabético, omitiendo cualquiera que ya haya aparecido en la frase clave. En este caso particular, el criptógrafo tomó la poco habitual medida de no empezar la frase clave al principio del alfabeto cifrado, sino tres letras después. Esto se debe posiblemente a que la frase clave comienza con la letra A, y el criptógrafo quería evitar codificar a como A. Finalmente, después de establecer el alfabeto cifrado completo, podemos descifrar el texto cifrado entero y el criptoanálisis está terminado.

Alfabeto llano	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Alfab. cifrado	X	Z	A	V	O	I	D	B	Y	G	E	R	S	P	C	F	H	J	K	L	M	N	Q	T	U	W

Now during this time Shahrazad had borne King Shahriyar three sons. Onthe thousand and first night, when she had ended the tale of Ma'aruf, she rose and kissed the ground before him, saying: 'Great King, for a thousand and one nights I have been recounting to you the fables of past ages and the legends of ancient kings. May I make so bold as to crave a favour of your majesty?'
Epilogue, Tales from the Thousand and One Nights[4]

[3] «A void, de Georges Perec». Se trata, pues, del libro de Perec comentado anteriormente, pero con el título de su traducción al inglés. (N. del T.)
[4] «Durante ese tiempo Sherezade había dado tres hijos al rey Shahriyar. En la noche mil y una, cuando hubo finalizado la historia de Maaruf, Sherezade se levantó y besó el suelo ante él, diciendo: "Gran Rey, durante mil y

3. El Renacimiento en Occidente

Entre los años 800 y 1200, los eruditos árabes disfrutaron un vigoroso período de logros intelectuales. Al mismo tiempo, Europa estaba firmemente estancada en la Edad Media, conocida también como la Edad de las Tinieblas. Mientras Al Kindi estaba describiendo la invención del criptoanálisis, los europeos aún se hallaban forcejeando con los elementos básicos de la criptografía. Las únicas instituciones europeas que alentaban el estudio de la escritura secreta eran los monasterios, en los que los monjes estudiaban la Biblia buscando significados ocultos, una fascinación que ha persistido a lo largo de los tiempos modernos (véase el Apéndice A).

Los monjes medievales se sentían intrigados por el hecho que el Antiguo Testamento contuviera ejemplos deliberados y obvios de criptografía. Por ejemplo, el Antiguo Testamento incluye partes de texto codificado con *atbash*, una forma tradicional de cifra de sustitución hebrea. Atbash consiste en tomar cada letra, anotar el número de lugares en que está con respecto al principio del alfabeto y sustituirla por la letra que se halla a un mismo número de lugares con respecto al final del alfabeto. En castellano esto significaría que la a, que está al principio del alfabeto, sería reemplazada por la Z, que está al final del alfabeto; la b sería sustituida por la Y, y así sucesivamente. El término mismo, atbash, sugiere la sustitución que describe, porque consta de la primera letra del alfabeto hebreo, *aleph,* seguida de la última letra, *taw,* y luego la segunda letra, *beth,* seguida de la segunda empezando por el final, *shin.* Un ejemplo de atbash aparece en Jeremías 25:26 y 51:41, donde «Babel» es reemplazado por la palabra «Sheshach»; la primera letra de Babel es *beth,* la segunda letra del alfabeto hebreo, que es reemplazada por *shin,* la segunda empezando por el final; la segunda letra de Babel es también *beth,* por lo que es asimismo reemplazada por *shm,* y la última letra de Babel es *lamed*, la doceava letra del alfabeto hebreo, que es reemplazada por *kaph,* la doceava empezando por el final.

Probablemente, la intención al utilizar atbash y otras cifras bíblicas similares era añadir misterio, más que ocultar el significado, pero su presencia fue suficiente para

una noches te he estado contando las fábulas de las eras pasadas y las leyendas de los antiguos reyes. ¿Puedo tener la osadía de solicitar un favor de vuestra majestad?"». Epílogo, Cuentos de las mil y una noches.

despertar el interés en la criptografía seria. Los monjes europeos comenzaron a redescubrir viejas cifras de sustitución, inventaron otras nuevas y, a su debido curso, ayudaron a reintroducir la criptografía en la civilización occidental. El primer libro europeo conocido que describe el uso de la criptografía fue escrito en el siglo XIII por el monje franciscano y erudito inglés Roger Bacon. *La Epístola sobre las obras de arte secretas y la nulidad de la magia* incluía siete métodos para mantener secretos los mensajes y advertía: «Sólo un loco escribe un secreto de una forma que no lo oculte del vulgo».

Ya en el siglo XIV, el uso de la criptografía se había extendido considerablemente, puesto que los alquimistas y los científicos la utilizaban para mantener en secreto sus descubrimientos. Aunque es mucho más conocido por sus logros literarios, Geoffrey Chaucer era también astrónomo y criptógrafo, y es el responsable de uno de los ejemplos más famosos de temprana codificación europea. Su *Tratado sobre el astrolabio* contenía algunas notas adicionales tituladas «El Ecuador de los Planetas», que incluían varios párrafos cifrados. La codificación de Chaucer reemplazaba letras del alfabeto llano con símbolos, por ejemplo, la b con §. Puede que un texto cifrado que consiste en símbolos extraños en vez de letras a primera vista parezca más complicado, pero esencialmente es equivalente a la tradicional sustitución letra-por-letra. El proceso de codificación y el nivel de seguridad son exactamente los mismos.

En el siglo XV, la criptografía europea era una industria floreciente. El resurgimiento de las artes, de las ciencias y de la erudición durante el Renacimiento nutrió el desarrollo de la criptografía, mientras que la explosión de las maquinaciones políticas ofreció motivaciones abundantes para la comunicación secreta. Italia, en particular, proveyó el ambiente ideal para la criptografía. Además de encontrarse en pleno corazón del Renacimiento, estaba formada por ciudades-estado independientes y cada una de ellas trataba de superar estratégicamente a las demás. La diplomacia floreció, y cada estado enviaba embajadores a la corte de los demás. Cada embajador recibía mensajes de su respectivo jefe de Estado, describiendo los detalles de la política de asuntos exteriores que debía implementar. Como respuesta, cada embajador enviaba cualquier información que hubiera obtenido. Obviamente, existía un gran incentivo para las comunicaciones cifradas en

ambas direcciones, de manera que cada estado estableció una oficina de cifras y cada embajador tenía un secretario de cifras.

Al mismo tiempo que la criptografía se estaba convirtiendo en una herramienta diplomática rutinaria, la ciencia del criptoanálisis empezaba a surgir en Occidente. Los diplomáticos acababan de familiarizarse con las habilidades requeridas para establecer comunicaciones seguras, y ya había individuos que trataban de destruir esta seguridad. Es bastante probable que el criptoanálisis fuera descubierto independientemente en Europa, pero también existe la posibilidad de que fuera introducido desde el mundo árabe. Los descubrimientos islámicos en la ciencia y las matemáticas habían influido poderosamente en el renacimiento de la ciencia en Europa, y puede que el criptoanálisis estuviera entre los conocimientos importados.

Podría decirse que el primer gran criptoanalista europeo fue Giovanni Soro, nombrado secretario de cifras en Venecia en 1506. La reputación de Soro se extendía a Italia entera, y los estados amigos enviaban los mensajes que interceptaban para que los criptoanalizaran en Venecia. Incluso el Vaticano, probablemente el segundo centro de criptoanálisis más activo, enviaba a Soro mensajes aparentemente impenetrables que habían caído en sus manos. En 1526, el papa Clemente VII le envió dos mensajes cifrados y los dos fueron devueltos tras haber sido criptoanalizados con éxito. Y cuando uno de los propios mensajes cifrados del papa fue capturado por los florentinos, el pontífice envió una copia a Soro confiando que le tranquilizara comunicándole que era indescifrable. Soro afirmó que no podía descifrar la cifra del papa, dando a entender que tampoco los florentinos serían capaces de descifrarla. Sin embargo, puede que esto fuera un ardid para infundir a los criptógrafos vaticanos una falsa sensación de seguridad. Puede que Soro se sintiera reacio a señalar los puntos débiles de la cifra papal, porque esto sólo habría servido para alentar al Vaticano a cambiar a una cifra más segura, una nueva cifra que quizá Soro no habría podido descifrar.

En el resto de Europa, las demás cortes empezaban también a emplear hábiles criptoanalistas, como Philibert Babou, criptoanalista del rey Francisco I de Francia. Babou había adquirido la reputación de ser increíblemente persistente, trabajando día y noche y perseverando durante semanas y semanas para descifrar un mensaje interceptado. Desgraciadamente para Babou, esto proporcionó al rey abundantes

oportunidades para tener una larga aventura amorosa con su esposa. Hacia el final del siglo XVI, los franceses consolidaron su habilidad descifradora con la llegada de François Viéte, que obtenía un placer especial descifrando las cifras españolas. Los criptógrafos españoles, que según parece eran más ingenuos que sus rivales en el resto de Europa, no podían creerlo cuando descubrieron que sus mensajes eran transparentes para los franceses. El rey Felipe II llegó a presentar una petición ante el Vaticano, afirmando que la única explicación posible del criptoanálisis de Viéte era que éste fuera un «enemigo jurado confabulado con el diablo». Felipe alegó que Viéte debía ser juzgado ante el tribunal de un cardenal por sus actos diabólicos; pero el papa, que sabía que sus propios criptoanalistas habían estado leyendo las cifras españolas durante años, rechazó la petición española. Las noticias sobre la petición pronto se extendieron a los expertos en cifras de varios países y los criptógrafos españoles se convirtieron en el hazmerreír de Europa.

La vergüenza española era sintomática del estado de la batalla entre los criptógrafos y los criptoanalistas. Era éste un período de transición, en el que los criptógrafos aún confiaban en la cifra de sustitución monoalfabética, mientras que los criptoanalistas comenzaban a utilizar el análisis de frecuencia para descifrarla. Los que aún no habían descubierto el poder del análisis de frecuencia continuaban confiando en la sustitución monoalfabética, sin darse cuenta de hasta qué medida criptoanalistas como Soro, Babou y Viéte podían leer sus mensajes.

Mientras tanto, los países alertados de los puntos débiles de la cifra de sustitución monoalfabética sencilla se sentían ansiosos por desarrollar una cifra mejor, algo que protegiera los mensajes de su propia nación para que no fueran descifrados por los criptoanalistas enemigos. Una de las mejoras más sencillas de la seguridad de la cifra de sustitución monoalfabética fue la introducción de *nulos*, es decir, símbolos o letras que no eran sustitutos de letras auténticas, sino meros huecos que no representaban nada. Por ejemplo, era posible sustituir cada letra llana por un número entre 1 y 99, lo que dejaba 73 números que no representaban nada y que podían ser salpicados aleatoriamente y con frecuencias variables por todo el texto cifrado. Los nulos no supondrían ningún problema para el receptor a quien se dirigía el mensaje, que sabía que debía ignorarlos. Sin embargo, los nulos desconcertarían a un enemigo interceptor, porque confundirían el análisis de frecuencia. Un avance

igualmente sencillo fue que los criptógrafos a veces deletreaban mal algunas palabras deliberadamente antes de codificar el mensaje. Ezto tyenne ell hefezto dhe dyztorrcihonarr hel hekilyvrio deh laas frhekuenzyas, dificultando considerablemente la aplicación del análisis de frecuencias. Sin embargo, el receptor a quien va dirigido, que sabe la clave, puede descifrar el mensaje y luego vérselas con las faltas ortográficas que, aunque dificultan su lectura, no hacen que el texto sea totalmente ilegible.

Otra tentativa de reforzar la cifra de sustitución monoalfabética conllevó la introducción de códigos. El término *código* tiene un significado muy amplio en el lenguaje cotidiano y a menudo se utiliza para describir cualquier método de comunicación secreta. Sin embargo, como ya mencioné en la Introducción, en realidad tiene un significado muy específico y se aplica sólo a una cierta forma de sustitución. Hasta ahora nos hemos concentrado en la idea de la cifra de sustitución, en la que cada letra es reemplazada por una letra, número o símbolo diferente. No obstante, también es posible tener una sustitución a un nivel mucho más alto, en el que cada palabra es representada por otra palabra o símbolo, esto sería un código. Por ejemplo,

asesinar	= D	general	= Σ	inmediatamente	= 08
chantajear	= P	rey	= Ω	hoy	= 73
capturar	= J	ministro	= ψ	esta noche	= 28
proteger	= Z	príncipe	= θ	mañana	= 43

mensaje llano = asesinad al rey esta noche
mensaje codificado = D–Ω–28

Técnicamente, un *código* se define como una sustitución al nivel de las palabras o las frases, mientras que una *cifra* se define como una sustitución al nivel de las letras. Por eso, el término *cifrar* significa ocultar un mensaje utilizando una cifra, mientras que *codificar* significa ocultar un mensaje utilizando un código. De manera similar, el término *descifrar* se aplica a la resolución de un mensaje cifrado, es

decir, en cifra, y el término *descodificar* a la resolución de un mensaje codificado. Los términos *codificar y descodificar* son más generales, y tienen relación tanto con códigos como con cifras. La Figura 7 presenta un breve resumen de estas definiciones. En general, me ajustaré a estas definiciones, pero cuando el sentido esté claro, puede que use términos como «descifrar un código» para describir un proceso que técnicamente se llamaría «descifrar una cifra» —el uso generalizado de estos términos hace que estén ampliamente aceptados[5].

Figura 7. La ciencia de la escritura secreta y sus ramas principales.

A primera vista, los códigos parecen ofrecer más seguridad que las cifras, porque las palabras son mucho menos vulnerables al análisis de frecuencia que las letras. Para descifrar una cifra monoalfabética sólo se necesita identificar el valor verdadero de cada uno de los 26 caracteres, mientras que para descifrar un código se necesita identificar el valor verdadero de cientos, o incluso miles de palabras codificadas. No obstante, si examinamos los códigos más detalladamente, vemos que tienen dos defectos prácticos cuando se los compara con las cifras. En primer lugar, una vez que el emisor y el receptor se han puesto de acuerdo con respecto a las 26 letras del alfabeto cifrado (la clave) pueden codificar cualquier mensaje, pero para lograr el mismo nivel de flexibilidad utilizando un código necesitarían pasar por la ardua y minuciosa tarea de definir una palabra codificada para cada una de las miles de palabras posibles en un texto llano. El libro de códigos tendría cientos de páginas y sería como un diccionario. En otras palabras, redactar un libro de códigos es una tarea muy ardua y tener que llevarlo encima es un gran inconveniente.

En segundo lugar, las consecuencias de que el enemigo capture un libro de códigos son devastadoras.

[5] En esta misma tónica, en castellano —y también concretamente en esta traducción— se utiliza «descifrar», «cifrar» y «codificar» para remitir a procesos relacionados tanto con cifras como con códigos. (N. del T.)

Inmediatamente, todas las comunicaciones codificadas se volverían transparentes para el enemigo. Los emisores y receptores tendrían que pasar por la ardua tarea de tener que redactar un libro de códigos totalmente nuevo, y luego este pesado tomo nuevo tendría que ser distribuido a todos los participantes en la red de comunicaciones, lo que indudablemente significaría transportarlo a todos los embajadores en todos los estados. En comparación, si el enemigo consigue capturar una clave resulta relativamente fácil compilar un nuevo alfabeto cifrado de 26 letras, que puede ser fácilmente memorizado y distribuido.

Incluso en el siglo XVI, los criptógrafos comprendieron la debilidad inherente de los códigos, y por ello confiaron en gran medida en las cifras o, a veces, en los *nomencladores.* Un nomenclador es un sistema de codificación que se basa en un alfabeto cifrado, el cual se utiliza para codificar la mayor parte de un mensaje, y en una lista limitada de palabras codificadas. Por ejemplo, un libro nomenclador podría consistir de una portada que contiene el alfabeto cifrado y una segunda página que contiene una lista de palabras codificadas. A pesar del añadido de palabras codificadas, un nomenclador no es mucho más seguro que una cifra corriente, porque la mayor parte del mensaje puede ser descifrado utilizando el análisis de frecuencia y las palabras codificadas restantes pueden ser adivinadas por el contexto.

Además de enfrentarse a la introducción del nomenclador, los mejores criptoanalistas también fueron capaces de afrontar mensajes mal deletreados y la presencia de nulos. Resumiendo, fueron capaces de descifrar la mayoría de los mensajes codificados. Su habilidad procuró un flujo constante de secretos descubiertos, que influyeron en las decisiones de sus señores y señoras, afectando de esta forma a la historia de Europa en los momentos críticos.

En ninguna parte queda ilustrado más dramáticamente el impacto de criptoanálisis que en el caso de María Estuardo. El desenlace de su juicio dependía enteramente de la batalla entre sus creadores de códigos y los descifradores de la reina Isabel. María era una de las figuras más significativas del siglo XVI —reina de Escocia, reina de Francia, aspirante al trono inglés— y, sin embargo, su destino lo decidiría una hoja de papel, el mensaje que contenía, y si ese mensaje podía ser descifrado o no.

4. La conspiración Babington

El 24 de noviembre de 1542, las fuerzas inglesas de Enrique VIII demolieron el ejército escocés en la batalla de Solway Moss. Parecía que Enrique estaba a punto de conquistar y arrebatar la corona al rey Jacobo V Después de la batalla, el angustiado rey escocés sufrió un colapso mental y físico completo, y se retiró al palacio de Falkland. Ni siquiera el nacimiento de su hija, María, justo dos semanas después, consiguió revivir al enfermo rey. Era como si hubiera estado esperando la nueva de un heredero o heredera para poder morirse en paz, con la seguridad de que había cumplido con su deber. Justo una semana después del nacimiento de María, el rey Jacobo X que sólo tenía treinta y tres años, murió. La princesa bebé era ya María, reina de Escocia.

María había nacido prematuramente, e inicialmente se extendió el miedo de que no sobreviviera. Los rumores en Inglaterra sugerían que había muerto, pero se trataba meramente de ilusiones que se hacía la corte inglesa, quienes estaban deseando oír noticias que pudieran desestabilizar Escocia. En realidad, María pronto se puso fuerte y sana, y a la edad de nueve meses, el 9 de septiembre de 1543, fue coronada en la capilla del castillo de Stirling, rodeada de tres condes, que llevaban en su nombre la corona real, el cetro y la espada.

El hecho de que María fuese tan joven ofreció a Escocia un respiro con respecto a las incursiones inglesas. Se habría considerado poco caballeroso si Enrique VIII hubiera tratado de invadir el país de un rey recién muerto, ahora bajo el reinado de una reina bebé. En vez de ello, el monarca inglés decidió seguir una política de ir ganándose a María con la esperanza de concertar un matrimonio entre ella y su propio hijo Eduardo, uniendo de esta manera las dos naciones bajo un soberano Tudor. Enrique comenzó sus maniobras poniendo en libertad a los nobles escoceses capturados en Solway Moss, con la condición de que hicieran campaña a favor de la unión con Inglaterra.

Sin embargo, tras considerar la oferta de Enrique, la corte escocesa la rechazó a favor de un matrimonio con Francisco, el delfín de Francia. Escocia elegía así aliarse con una nación católica como ella, una decisión que agradó a la madre de María, María de Guise, cuyo matrimonio con Jacobo V había tenido lugar para consolidar la relación entre Escocia y Francia. María y Francisco aún eran niños, pero el plan para

el futuro era que llegado el momento se casarían, y que Francisco ascendería al trono francés con María como su reina, uniendo de esta forma Escocia y Francia. Mientras tanto, Francia defendería a Escocia contra cualquier ataque inglés.

La promesa de protección era tranquilizadora, sobre todo porque Enrique VIII había cambiado de política, pasando de la diplomacia a la intimidación para persuadir a los escoceses de que su propio hijo era un pretendiente más merecedor para María, reina de Escocia. Sus fuerzas cometieron actos de piratería, destruyeron cosechas, quemaron aldeas y atacaron pueblos y ciudades a lo largo de toda la frontera. El «duro cortejo», como se conoce a estas acciones, continuó incluso después de la muerte de Enrique en 1547. Bajo los auspicios de su hijo, el rey Eduardo VI (el aspirante a pretendiente), los ataques culminaron en la batalla de Pinkie Cleugh, en la que el ejército escocés sufrió una derrota aplastante. Como consecuencia de esta matanza, se decidió que, por su propia seguridad, María se fuese a Francia, a resguardo de la amenaza inglesa, donde se prepararía para su matrimonio con Francisco. El 7 de agosto de 1548, con seis años de edad, embarcó en el puerto de Roscoff.

Los primeros años de María en la corte francesa serían los más idílicos de su vida. Estaba rodeada de lujo, protegida de todo mal, y llegó a amar a su futuro marido, el delfín. A la edad de dieciséis años se casaron, y al año siguiente Francisco y María se convirtieron en rey y reina de Francia. Todo parecía dispuesto para su regreso triunfal a Escocia, hasta que su marido, que siempre había tenido poca salud, se puso gravemente enfermo. Una infección de oído que había padecido desde niño empeoró, la inflamación se extendió hasta el cerebro y comenzó a producirse un absceso. En 1560, antes de un año de su coronación, Francisco murió y María quedó viuda.

Desde entonces, la vida de María sería golpeada por la tragedia repetidamente. En 1561 regresó a Escocia, donde encontró una nación transformada. Durante su larga ausencia, María había acrecentado su fe católica, mientras que sus súbditos escoceses se habían ido acercando a la Iglesia protestante. María toleró los deseos de la mayoría y al principio reinó con relativo éxito, pero en 1565 se casó con su primo, Enrique Estuardo, conde de Darnley, un acto que precipitó una espiral de declive. Darnley era un hombre malicioso y brutal, cuya implacable ansia de poder

hizo que María perdiese la lealtad de los nobles escoceses. Al año siguiente, María fue testigo del horror de la naturaleza brutal de su marido cuando éste asesinó a David Riccio, el secretario de María, delante de ella. Quedó claro para todos que por el bien de Escocia era necesario librarse de Darnley. Los historiadores debaten si fue María o los nobles escoceses quienes instigaron la conspiración, pero el hecho es que la noche del 9 de febrero de 1567 la casa de Darnley sufrió una explosión y cuando él trataba de escapar, fue estrangulado. Lo único bueno que salió de ese matrimonio fue un hijo y heredero, Jacobo.

El siguiente matrimonio de María, con James Hepburn, el cuarto conde de Bothwell, no tuvo mucho más éxito. Para el verano de 1567, los nobles escoceses protestantes se habían desilusionado completamente de su reina católica y exiliaron a Bothwell e hicieron prisionera a María, forzándola a abdicar a favor de su hijo de catorce meses, Jacobo VI. El hermanastro de la reina, el conde de Moray, actuaría como regente. Al año siguiente, María escapó de la prisión, reunió un ejército de seis mil monárquicos e hizo una tentativa final de recuperar su corona. Sus soldados se enfrentaron al ejército del regente en el pequeño pueblo de Langside, cerca de Glasgow, y María presenció la batalla desde una colina cercana. Aunque sus tropas eran más numerosas, les faltaba disciplina, y María pudo contemplar cómo eran aniquiladas. Cuando vio que la derrota era inevitable, huyó de allí. Lo ideal hubiera sido dirigirse al este, hacia la costa, y luego continuar hasta Francia, pero esto hubiera significado cruzar el territorio leal a su hermanastro, así que se dirigió hacia el sur, hacia Inglaterra, confiando que su prima, la reina Isabel I, le daría refugio.

Esta decisión de María resultó ser un terrible error. Lo único que Isabel ofreció a María fue otra prisión. La razón oficial para su detención fue en conexión con el asesinato de Darnley, pero el verdadero motivo era que María suponía una amenaza para Isabel, porque los católicos ingleses consideraban que María era la auténtica reina de Inglaterra. A través de su abuela, Margarita Tudor, la hermana mayor de Enrique VIII, María podía ciertamente aspirar al trono, pero la única hija de Enrique VIII que había sobrevivido, Isabel I, parecería tener un derecho aún mayor. Sin embargo, para los católicos

Isabel era ilegítima, porque era hija de Ana Bolena, la segunda esposa de Enrique, después de que éste se divorciara de Catalina de Aragón desafiando al papa. Los

católicos ingleses no reconocieron el divorcio de Enrique VIII, así como tampoco su siguiente matrimonio con Ana Bolena, y desde luego no aceptaban a su hija Isabel como reina, considerándola una usurpadora bastarda.

María fue encarcelada en una serie de castillos y casas solariegas. Aunque Isabel la consideraba una de las figuras más peligrosas de Inglaterra, muchos ingleses confesaban admirar su aire cortés, su obvia inteligencia y su gran belleza. William Cecil, el gran ministro de Isabel, comentó «la manera ingeniosa y endulzada con que entretenía a todos los hombres», y Nicholas White, el emisario de Cecil, hizo una observación similar: «Ella tiene además una gracia seductora, un bonito acento escocés y un ingenio penetrante, dulcificado por la amabilidad». Pero, según fueron pasando los años, su apariencia menguó, su salud se deterioró y empezó a perder la esperanza. Su carcelero, *sir* Amyas Paulet, un puritano, era inmune a sus encantos y la trataba con creciente dureza.

En 1586, tras dieciocho años de encarcelamiento, había perdido todos sus privilegios. Fue confinada en Chartley Hall, en Staffordshire, y ya no se le permitió tomar las aguas en Buxton, lo que hasta entonces había ayudado a aliviar sus frecuentes enfermedades. En su última visita a Buxton utilizó un diamante para grabar un mensaje en un cristal: «Buxton, cuyas cálidas aguas han hecho famoso tu nombre, tal vez ya no te vuelva a visitar. Adiós». Parece que sospechaba que estaba a punto de perder la poca libertad que tenía. La creciente tristeza de María se veía agravada por la conducta de su hijo de diecinueve años, el rey Jacobo VI de Escocia.

Ella siempre había confiado que un día lograría escapar y volver a Escocia para compartir el poder con su hijo, a quien no había visto desde que él tenía un año. Sin embargo, Jacobo no sentía el mismo afecto por su madre. Siendo educado por los enemigos de María, le habían enseñado que su madre había asesinado a su padre para casarse con su amante. Jacobo la despreciaba y temía que si volvía podía arrebatarle la corona. El odio que sentía por María lo patentizaba el hecho de que no le producía ningún escrúpulo procurar un matrimonio con Isabel I, la mujer responsable del encarcelamiento de su madre (y que, además, era treinta años mayor que él). Isabel no aceptó la oferta.

María escribió a su hijo en un intento de convencerlo, pero sus cartas nunca

llegaron a la frontera escocesa. Para entonces, María estaba más aislada que nunca: todas las cartas que enviaba eran confiscadas y la correspondencia entrante se la quedaba su carcelero. La moral de María estaba en su punto más bajo, y parecía que ya no quedaba ninguna esperanza. Fue en estas severas y desesperadas circunstancias cuando, el 6 de enero de 1586, recibió un sorprendente paquete de cartas.

Se trataba de cartas escritas por los partidarios de María en Europa, y quien había logrado introducirlas en su prisión fue Gilbert Giffbrd, un católico que había abandonado Inglaterra en 1577 preparándose para ser sacerdote en el Colegio Inglés de Roma. Al regresar a Inglaterra en 1585, aparentemente deseoso de servir a María, se puso en contacto inmediatamente con la embajada francesa en Londres, donde se había acumulado un montón de correspondencia. La embajada sabía que si enviaban las cartas por los conductos formales nunca llegarían a María. Sin embargo, Gifford afirmó que él podría hacer pasar las cartas a Chartley Hall, y ciertamente supo cumplir su palabra. Esta entrega fue la primera de otra muchas, y así comenzó la carrera de Gifford como mensajero, no sólo pasando cartas a María, sino también recogiendo sus respuestas. Tenía una manera bastante ingeniosa de pasar cartas a hurtadillas a Chartley Hall. Llevaba los mensajes a un cervecero local, que los ponía en una bolsa de cuero, la cual luego escondía en un tapón hueco usado para cerrar un barril de cerveza. El cervecero llevaba el barril a Chartley Hall, y entonces uno de los sirvientes de María abría el tapón y llevaba su contenido a la reina de Escocia. El proceso funcionaba igualmente bien para sacar mensajes de Chartley Hall.

Mientras tanto, sin que María lo supiera, en las tabernas de Londres se estaba urdiendo un plan para rescatarla. En el centro de la conspiración estaba Anthony Babington, que sólo tenía cuarenta y cuatro años pero que ya era muy conocido en la ciudad como vividor atractivo, encantador e ingenioso. De lo que muchos de sus admiradores contemporáneos no se daban cuenta era que Babington sentía un profundo menosprecio por el sistema, que le había perseguido a él, a su familia y a su fe. La política anticatólica del Estado había alcanzado nuevas cotas de horror, acusando de traición a los sacerdotes y castigando a cualquiera que los albergase con el potro, la mutilación o el destripamiento en vida. La misa católica fue

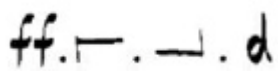
oficialmente prohibida y las familias que permanecían leales al papa fueron obligadas a pagar agobiantes impuestos. La animosidad de Babington la había estimulado la muerte de lord Darcy, su bisabuelo, que había sido decapitado por su participación en la Peregrinación de la Gracia, una sublevación católica contra Enrique VIII.

La conspiración comenzó una tarde de marzo de 1586, en la que Babington y seis confidentes se reunieron en The Plough, un mesón situado fuera de Bar Temple. Como señaló el historiador Philip Caraman, «con la fuerza de su excepcional encanto y personalidad, atrajo a muchos jóvenes caballeros católicos de su mismo rango, gallardos, aventurados y audaces en la defensa de la fe católica en sus días difíciles; y listos para cualquier empresa ardua que pudiera contribuir al avance de la común causa católica». Durante los meses siguientes se trazó un ambicioso plan para liberar a María, reina de Escocia, asesinar a la reina Isabel e incitar una rebelión apoyada por una invasión desde el extranjero.

Los conspiradores acordaron que la «conspiración Babington», como ya se la llamaba, no podía continuar sin la aprobación de María, pero no parecía haber ninguna manera de comunicarse con ella. Entonces, el 6 de julio de 1586, Gifford se presentó en el umbral de Babington. Traía una carta de María, que explicaba lo que había oído acerca de Babington a través de los adeptos que la reina tenía en París y que estaba deseando tener noticias suyas. Como respuesta, Babington redactó una carta detallada en la que resumía su plan, incluida una referencia a la excomunión de Isabel, dictada por el papa Pío V en 1570, lo que, en su opinión, legitimaba su asesinato.

> *Yo mismo con diez caballeros y una centena de nuestros seguidores emprenderemos la liberación de vuestra real persona de las manos de vuestros enemigos. Para librarnos de la usurpadora, cuya excomunión nos libera de prestarle obediencia, hay seis nobles, todos ellos amigos míos personales, que por el celo que guardan a la causa católica y al servicio de vuestra majestad llevarán a cabo esa trágica ejecución.*

Como antes, Gifford utilizó su truco de poner el mensaje en el tapón de un barril de cerveza para ocultarlo de los guardas de María. Esto puede considerarse una forma de esteganografía, porque se estaba ocultando la carta. Como precaución adicional, Babington codificó su carta para que, incluso si era interceptada por el carcelero de María, resultara indescifrable y no se pudiera descubrir la conspiración. Utilizó una cifra que no era una simple sustitución monoalfabética, sino más bien un nomenclador, tal como se muestra en la Figura 8. Consistía de 23 símbolos que sustituían a las letras del alfabeto (menos la j, la v y la w) y otros 35 símbolos que representaban palabras o frases. Asimismo, había 4 nulos



y el símbolo

que significaba que el símbolo siguiente representaba una letra doble.

Figura 8. El nomenclador de María Estuardo, que consistía de un alfabeto cifrado y palabras codificadas.

Gifford todavía era joven, más joven aún que Babington, y, sin embargo, llevaba a cabo sus entregas con confianza y astucia. Sus alias, como Sr. Colerdin, Pietro y Cornelys, le permitían viajar por el país sin despertar sospechas, y sus contactos en el seno de la comunidad católica le proporcionaron una serie de casas seguras entre Londres y Chartley Hall. Sin embargo, cada vez que Gifford viajaba a o desde Chartley Hall daba un rodeo. Aunque aparentemente Gifford actuaba como agente al servicio de María, en realidad era un agente doble. En 1585, antes de su regreso a Inglaterra, Gifford había escrito a *sir* Francis Walsingham, secretario principal de la reina Isabel, ofreciendo sus servicios. Gifford se dio cuenta de que su origen y formación católica le servirían de máscara perfecta para infiltrarse en las conspiraciones contra la reina Isabel. En la carta que envió a Walsingham escribió: *«He oído acerca del trabajo que usted realiza y quiero serviros. No tengo escrúpulos ni temo el peligro. Cualquier cosa que me ordenéis la llevaré a cabo»*.

Walsingham era el ministro más implacable de Isabel. Era una figura maquiavélica, el jefe de espionaje responsable de la seguridad de la reina. Había heredado una pequeña red de espías, que inmediatamente expandió por Europa, donde se estaban tramando muchas conspiraciones contra Isabel. Después de su muerte se descubrió que había estado recibiendo regularmente informes desde doce lugares de Francia, nueve de Alemania, cuatro de Italia, cuatro de España y tres de los Países

Bajos, además de tener informantes en Constantinopla, Argel y Trípoli.

Walsingham reclutó a Gifford como espía y, de hecho, fue él quien ordenó a Gifford que fuera a la embajada francesa y se ofreciera como mensajero. Cada vez que Gifford recibía un mensaje para o de María, primero se lo llevaba a Walsingham El alertado jefe de espionaje se lo pasaba primero a sus falsificadores, que rompían el sello de lacre de cada carta, hacían una copia de la misma y luego volvían a lacrar la carta original con un sello idéntico antes de devolvérsela a Gifford. La carta, aparentemente intacta, podía entregarse entonces a María o a sus corresponsales, que no eran conscientes de lo que pasaba.

Cuando Gifford entregó a Walsingham una carta de Babington dirigida a María, su primer objetivo fue descifrarla. Walsingham había descubierto los códigos y las cifras en un libro escrito por el matemático y criptógrafo italiano Girolamo Cardano

(el cual, por cierto, propuso una forma de escritura para los ciegos basada en el tacto, manifestándose así como precursor de Braille). El libro de Cardano despertó el interés de Walsingham, pero fue un desciframiento realizado por el criptoanalista flamenco Philip van Marnix lo que terminó de convencerlo del poder que supondría contar con un descifrador a su servicio. En 1577, el rey Felipe II de España utilizaba cifras para mantener correspondencia con su hermanastro, don Juan de Austria, católico como él y que controlaba gran parte de los Países Bajos. Una carta de Felipe describía un plan para invadir Inglaterra, pero fue interceptada por Guillermo de Orange, que se la pasó a Marnix, su secretario de cifras. Marnix descifró el plan y Guillermo pasó la información a Daniel Rogers, un agente inglés que trabajaba en Europa, quien, a su vez, advirtió a Walsingham de la invasión. Los ingleses reforzaron sus defensas, lo que fue suficiente para impedir la tentativa de invasión.

Entonces, completamente consciente del valor del criptoanálisis, Walsingham creó una escuela de cifras en Londres. Como su secretario de cifras nombró a Thomas Phelippes, un hombre «de poca estatura, muy delgado, con el pelo rubio oscuro en la cabeza y rubio claro en la barba, con la cara comida por la viruela, corto de vista, con apariencia de tener unos treinta años». Phelippes era un lingüista que hablaba francés, italiano, español, latín y alemán y, lo que era aún más importante, uno de los mejores criptoanalistas de Europa.

Siempre que recibía algún mensaje de o para María, Phelippes lo devoraba. Era un maestro del análisis de frecuencia, y encontrar la solución era sólo cuestión de tiempo. Estableció la frecuencia de cada símbolo y tentativamente propuso valores para los que aparecían más a menudo. Cuando un enfoque particular empezaba a parecer absurdo daba marcha atrás y probaba otras sustituciones alternativas. Gradualmente, lograba identificar los nulos, las pistas falsas criptográficas y ponerlos de lado. Al final, lo único que quedaba era un puñado de palabras codificadas, cuyo significado podía adivinarse gracias al contexto.

Cuando Phelippes descifró el mensaje que Babington dirigía a María, en el que proponía claramente el asesinato de Isabel, remitió inmediatamente el texto condenatorio a su jefe. Walsingham podía haberse abalanzado sobre Babington en ese momento, pero quería algo más que la ejecución de un puñado de rebeldes. Prefirió esperar, confiando que María respondería y autorizaría la conspiración,

incriminándose a sí misma. Walsingham había deseado la muerte de María durante mucho tiempo, pero era consciente de las reticencias de Isabel a ejecutar a su prima. Sin embargo, si lograba demostrar que María estaba respaldando una tentativa de asesinar a Isabel, entonces con toda seguridad su reina permitiría la ejecución de su rival católica. Las esperanzas de Walsingham pronto se vieron cumplidas.

El 17 de julio, María respondió a Babington, firmando en realidad su propia sentencia de muerte. Escribió explícitamente sobre el «plan», mostrando una preocupación particular por el hecho de que debían liberarla al mismo tiempo o antes del asesinato de Isabel, porque de otra forma la noticia podía llegar a su carcelero, que podría entonces decidir matarla. Antes de llegar a Babington, la carta hizo su desvío habitual a las manos de Phelippes. Como ya había criptoanalizado el mensaje anterior, pudo descifrar éste con facilidad, leer su contenido y marcarlo con un Π: el signo de la horca.

Walsingham tenía la prueba que requería para arrestar a María y a Babington, pero aún no estaba satisfecho. Para destruir completamente la conspiración necesitaba los nombres de todos los implicados. Para conseguirlos, pidió a Phelippes que falsificara una posdata a la carta de María que tentara a Babington a dar nombres. Uno de los talentos adicionales de Phelippes era el de falsificador y se decía que tenía la habilidad de «escribir con la letra de cualquiera, con sólo haberla visto una vez, como si la persona misma la hubiera escrito». La Figura 9 muestra la posdata que fue añadida al final de la carta de María a Babington. Puede ser descifrada utilizando el nomenclador de María, que aparece en la Figura 8, para revelar el siguiente texto llano:

> *Me alegraría conocer los nombres y las cualidades de los seis caballeros que llevarán a cabo el plan; porque puede ser que, conociendo a los participantes, yo pueda daros algún consejo necesario para seguirlo en eso, así como de vez en cuando los particulares de cómo proceder: y en cuanto podáis, con el mismo propósito, quiénes conocen ya, y en qué medida, los detalles de esta cuestión.*

La cifra de María Estuardo demuestra claramente que una codificación débil puede ser peor que no codificación en absoluto. Tanto María como Babington escribieron explícitamente sus intenciones porque creían que sus comunicaciones eran seguras, mientras que si se hubieran comunicado abiertamente se habrían referido a su plan de una manera más discreta.

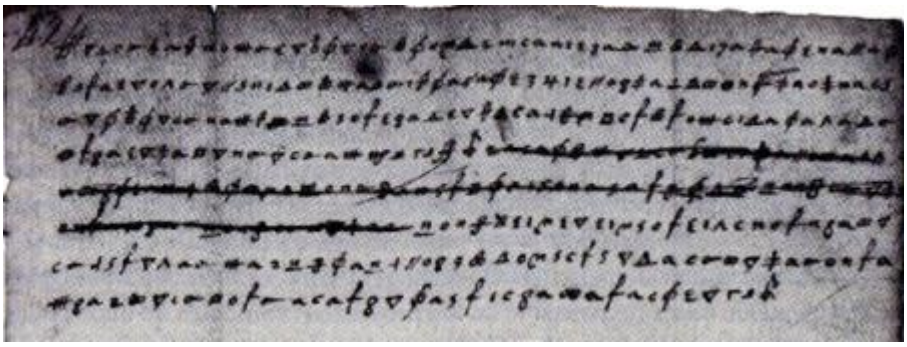


Figura 9, La posdata falsificada añadida por Thomas Phelippes al mensaje de María. Se puede descifrar consultando el nomenclador de María (Figura 8).

Además, su fe en su cifra los hizo particularmente vulnerables a aceptar la falsificación de Phelippes. El emisor y el receptor a menudo tienen tanta confianza en la solidez de su cifra que consideran imposible que el enemigo pueda imitar la cifra e insertar un texto falsificado. El uso correcto de una cifra fuerte constituye una clara ventaja para el emisor y el receptor pero el uso incorrecto de una cifra débil puede generar una sensación muy falsa de seguridad.

Poco después de recibir el mensaje y su posdata, Babington necesitaba ir al extranjero para organizar la invasión, y tenía que inscribirse en el departamento de Walsingham para conseguir un pasaporte. Éste habría sido un momento ideal para capturar al traidor, pero el burócrata que atendía la oficina, John Scudamore, no esperaba que el traidor más buscado de Inglaterra se presentara ante su puerta. Scudamore, que no contaba con ayuda a mano, llevó al confiado Babington a una taberna cercana, haciendo tiempo mientras su asistente organizaba un grupo de soldados. Poco después llegó una nota a la taberna, informando a Scudamore que había llegado el momento de la detención. Sin embargo, Babington la vio. Como si tal cosa, dijo que iba a pagar la cerveza y la comida y se levantó, dejando su espada y su abrigo en la mesa, dando a entender que volvería en un momento. En lugar de eso, se escurrió por la puerta trasera y escapó, primero a St. John's Wood

y luego a Harrow. Intentó disfrazarse, cortándose el pelo y tiñéndose la piel con zumo de nueces para ocultar su origen aristocrático. Consiguió eludir la captura durante diez días, pero el 15 de agosto, Babington y sus seis colegas fueron capturados y llevados a Londres.

Las campanas de las iglesias de toda la ciudad repicaron a triunfo. Sus ejecuciones fueron extremadamente espantosas. Según relata el historiador isabelino William Camden, «*los acuchillaron por todas partes, les cortaron sus partes privadas, les sacaron las entrañas en vivo y haciéndoles mirar, y fueron cuarteados*».

Mientras tanto, el 11 de agosto, se otorgó a María Estuardo y a su séquito el privilegio excepcional de dar un paseo a caballo por el terreno de Chartley Hall. Cuando María cruzaba los páramos divisó a varios jinetes que se acercaban e inmediatamente pensó que debían ser los hombres de Babington que venían a rescatarla. Pronto quedó claro que estos hombres habían venido a arrestarla, no a liberarla. María había estado implicada en la conspiración Babington y fue acusada conforme a la Ley de Asociación, una Ley del Parlamento aprobada en 1584, concebida específicamente para condenar a cualquiera que estuviese implicado en una conspiración contra Isabel.

El juicio se celebró en el castillo de Fotheringhay, un lugar desolado y mísero en medio de las monótonas marismas de East Anglia. Comenzó el miércoles 15 de octubre, frente a dos jueces principales, otros cuatro jueces, el lord canciller, el lord tesorero, Walsingham, y varios condes, caballeros y barones. En la parte de atrás de la sala de justicia había espacio para espectadores, como los aldeanos locales y los sirvientes de los comisarios, todos ellos ansiosos por ver a la humillada reina escocesa pedir perdón y suplicar por su vida. Sin embargo, María permaneció digna y tranquila a lo largo del juicio. Su defensa principal consistía en negar toda conexión con Babington. «¿Se me puede hacer responsable de los proyectos criminales de unos pocos hombres desesperados», proclamaba, «que planearon sin mi conocimiento o participación?». Su alegato tuvo muy poco impacto frente a la evidencia que existía contra ella.

María y Babington habían confiado en una cifra para mantener sus planes en secreto, pero vivían en un período en que la criptografía se estaba debilitando ante los avances del criptoanálisis. Aunque su cifra habría procurado suficiente protección

contra los ojos entrometidos de un aficionado, no tenía la más mínima posibilidad contra un experto en análisis de frecuencia. En la galería de los espectadores estaba sentado Phelippes, observando en silencio cómo presentaban la prueba que había logrado entresacar de las cartas codificadas.

El juicio entró en su segundo día y María seguía negando todo conocimiento de la conspiración Babington Cuando finalizó el juicio dejó a los jueces para que decidieran su futuro, perdonándoles de antemano la inevitable decisión. Diez días después, el Tribunal de Inquisición se reunió en Westminster y concluyó que María había sido culpable de «*urdir e imaginar desde el primero de junio asuntos tendentes a la muerte de y destrucción de la reina de Inglaterra*». Recomendaron la pena de muerte e Isabel firmó la sentencia.

El 8 de febrero de 1587, en la gran sala del castillo de Fotheringhay, una audiencia de trescientas personas se reunió para ver la decapitación. Walsingham estaba resuelto a minimizar la influencia de María como mártir y ordenó que el patíbulo, las vestimentas de María y todo lo demás relacionado con la ejecución fuera quemado para evitar la creación de cualquier santa reliquia. También planeó una fastuosa procesión fúnebre en honor de su yerno, *sir* Philip Sidney, que tendría lugar la semana siguiente. Sidney, una figura heroica y popular, había muerto luchando contra los católicos en los Países Bajos y Walsingham creía que un desfile magnífico en su honor empañaría la lástima por María. Sin embargo, María estaba igualmente decidida a que su aparición final fuera un gesto desafiante, una oportunidad para reafirmar su fe católica e inspirar a sus seguidores.

Mientras el deán de Peterborough conducía las oraciones, María dijo en voz alta sus propias oraciones por la salvación de la Iglesia católica inglesa, por su hijo y por Isabel. Recordando el lema de su familia, «*En mi fin está mi principio*», se armó de compostura y se aproximó al patíbulo. Los verdugos solicitaron su perdón y ella replicó: «*Os perdono de todo corazón, porque ahora confío en que pondréis fin a todos mis pesares*». Richard Wingfield, en su Narración de los últimos días de la reina de Escocia, describe sus momentos finales:

> *Entonces se apoyó sobre el patíbulo con completa calma y extendiendo los brazos y las piernas gritó «In manus tuas domine»*

tres o cuatro veces, y finalmente, mientras uno de los verdugos la sujetaba suavemente con una de sus manos, el otro dio dos golpes con el hacha antes de que se cortara su cabeza, y aún quedó un poco de cartílago y entonces ella hizo una serie de pequeños ruidos y no movió ninguna de sus partes del lugar en que yacía... Sus labios se movieron casi un cuarto de hora después de que le cortaran la cabeza.

Entonces uno de sus verdugos que le arrancaba las ligaduras vio a su pequeño perro que se había deslizado bajo su ropa y que no pudo ser sacado más que a la fuerza y después no podía alejarse de su cadáver, sino que vino y yació entre la cabeza y los hombros de ella, algo anotado con diligencia.

Figura 10. La ejecución de María, reina de Escocia.

Capítulo 2

Le chiffre indéchiffrable

Contenido:

Durante siglos, la cifra de sustitución monoalfabética simple había sido suficiente para asegurar el secreto. El subsiguiente desarrollo del análisis de frecuencia, primero en el mundo árabe y luego en Europa, destruyó su seguridad. La trágica ejecución de María, reina de Escocia, fue una dramática ilustración de las debilidades de la sustitución monoalfabética, y en la batalla entre los criptógrafos y los criptoanalistas estaba claro que estos últimos llevaban las de ganar. Cualquiera que enviaba un mensaje codificado tenía que aceptar que un descifrador enemigo experto podría interceptar y descifrar sus más valiosos secretos.

Obviamente, incumbía a los criptógrafos inventar una nueva cifra más sólida, algo que pudiera despistar a los criptoanalistas. Aunque dicha cifra no surgiría hasta el final del siglo XVI, sus orígenes se remontan al polifacético erudito florentino del siglo XV León Battista Alberti. Nacido en 1404, Alberti fue una de las figuras principales del Renacimiento: pintor, compositor, poeta y filósofo, además de autor del primer análisis científico de la perspectiva, de un tratado sobre la mosca y de una oración fúnebre para su perro. Es probablemente más conocido como arquitecto, ya que diseñó la primera fuente de Trevi en Roma, y escribió *De re aedificatoria*, el primer libro impreso sobre arquitectura, que sirvió como catalizador para la transición del diseño gótico al renacentista.

En algún momento de la década de 1460, Alberti paseaba por los jardines del Vaticano cuando se encontró con su amigo Leonardo Dato, el secretario pontificio, que comenzó a hablarle de los aspectos más admirables de la criptografía. Esta conversación fortuita incitó a Alberti a escribir un ensayo sobre ese tema, esbozando lo que él consideraba una nueva forma de cifra. En aquellos tiempos,

todas las cifras de sustitución requerían un solo alfabeto cifrado para codificar cada mensaje. Sin embargo, Alberti propuso utilizar dos o más alfabetos cifrados, alternando entre ellos durante la codificación, confundiendo de esta manera a los potenciales criptoanalistas.

Alfabeto llano	a b c d e f g h i j k l m n o p q r s t u v w x y z
Alfab. cifrado 1	F Z B V K I X A Y M E P L S D H J O R G N Q C U T W
Alfab. cifrado 2	G O X B F W T H Q I L A P Z J D E S V Y C R K U H N

Por ejemplo, aquí tenemos dos posibles alfabetos cifrados, y podríamos cifrar un mensaje alternando entre ellos. Para cifrar el mensaje aquello, codificaríamos la primera letra según el primer alfabeto cifrado, de forma que a se convierte en F, pero codificaríamos la segunda letra según el segundo alfabeto cifrado, de forma que q se convierte en E. Para cifrar la tercera letra volvemos al primer alfabeto cifrado, para la cuarta acudimos al segundo alfabeto cifrado, y así sucesivamente. Esto significa que u es codificada como N, e como F, la primera L como P, mientras que la segunda L se convierte en A, y la o final en D. El texto cifrado completo sería FENFPAD. La ventaja crucial del sistema de Alberti es que una misma letra del texto llano no aparece necesariamente como la misma letra en el texto cifrado, de forma que, por ejemplo, las dos L que aparecen en aquello se codifican de manera diferente en cada caso. De manera similar, las dos F que aparecen en el texto cifrado representan a una letra diferente del texto llano en cada caso: la primera representa una a y la segunda una e.

Aunque había dado con el avance más significativo en codificación en más de mil años, Alberti no logró desarrollar su concepto y convertirlo en un sistema de codificación plenamente formado.

Esa tarea recayó sobre un diverso grupo de intelectuales, que se basaron en su idea original. El primero fue Johannes Trithemius, un abad alemán nacido en 1462; luego vino Giovanni Porta, un científico italiano nacido en 1535, y finalmente Blaise de Vegenère, un diplomático francés nacido en 1523. Vegenère conoció los escritos de Alberti, Trithemius y Porta cuando fue enviado a Roma, a los veintiséis años, en una misión diplomática de dos años. Al principio, su interés en la criptografía era meramente práctico y se relacionaba con su trabajo diplomático. Después, a la edad

de treinta y nueve años, Vegenère decidió que ya había acumulado suficiente dinero como para abandonar su carrera y dedicar su vida al estudio. Fue sólo entonces cuando estudió en detalle las ideas de Alberti, Trithemius y Porta, combinándolas hasta lograr una nueva cifra, coherente y poderosa.

Figura 11. Blaise de Vegenère.

Aunque tanto Alberti como Trithemius y Porta aportaron una contribución vital, la cifra se conoce como la cifra Vegenère en honor al hombre que la desarrolló en su forma definitiva. La fuerza de la cifra Vegenère radica en que no utiliza uno, sino 26 alfabetos cifrados distintos para cifrar un mensaje. El primer paso de la codificación es trazar lo que se denomina un cuadro Vegenère, tal como se muestra en la Tabla 3. Se trata de un alfabeto llano seguido de 26 alfabetos cifrados, consiguiéndose cada uno de ellos comenzando en la siguiente letra que el anterior. De esta forma, la línea 1 representa un alfabeto cifrado con un cambio del César de una posición, lo que significa que se podría usar para poner en práctica una cifra de cambio del César en la que cada letra del texto llano es reemplazada por la letra siguiente del

alfabeto. De manera similar, la línea 2 representa un alfabeto cifrado con un cambio del César de dos posiciones, y así sucesivamente. La línea superior del cuadro, en minúsculas, representa las letras del texto llano. Se podría codificar cada letra del texto llano según uno de los 26 alfabetos cifrados. Por ejemplo, si se utiliza el alfabeto cifrado número 2, entonces la letra a se codifica como C, pero si se usa el alfabeto cifrado número 12, entonces la a se codifica como M.

Llano	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
1	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V

23	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
26	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Tabla 3. Un cuadro de Vegenère

Si el emisor sólo utilizara uno de los alfabetos cifrados para codificar todo un mensaje, se trataría realmente de una simple cifra del César, lo que sería una forma muy débil de codificación, fácilmente descifrable por un interceptor enemigo. Sin embargo, en la cifra Vegenère se usa una línea diferente del cuadro Vegenère (un alfabeto cifrado diferente) para cifrar las diferentes letras del mensaje. En otras palabras, el emisor podría cifrar la primera letra según la línea 5, la segunda según la línea 14, la tercera según la línea 21, y así sucesivamente.

Para descifrar el mensaje, el receptor a quien va dirigido necesita saber qué línea del cuadro Vegenère ha sido utilizada para codificar cada letra, de manera que tiene que haber un sistema acordado para cambiar de línea. Esto se logra utilizando una palabra clave. Para ilustrar cómo se utiliza una clave con el cuadro Vegenère para cifrar un mensaje corto vamos a descifrar la frase desvíe tropas a la loma este, utilizando la clave HIELO. Para empezar, se deletrea la clave sobre el mensaje, repitiéndola las veces que sea necesario hasta que cada letra del mensaje quede asociada con una letra de la clave. El texto cifrado se genera de la manera siguiente. Para cifrar la primera letra, d, hay que comenzar por identificar la letra clave que hay sobre ella, H, que a su vez define una línea particular en el cuadro Vegenère. La línea que comienza con H, la línea 7, es el alfabeto cifrado que se utilizará para encontrar la letra que sustituirá a la d del texto llano. Observamos dónde se cruza la columna que comienza por d con la línea que comienza por H y resulta ser en la letra K Por consiguiente, a esa letra d del texto llano la representa la Ken el texto cifrado.

Clave	H	I	E	L	O	H	I	E	L	O	H	I	E	L	O	H	I	E	L	O	H	I	E			
Texto llano	d	e	s	v	i	e	t	r	o	p	a	s	a	l	a	l	o	m	a	e	s	t	e			
T. cifrado	K	M	W	G	W	L	B	V	Z	D	H	A	E	T	O	S	W	Q	L	S	Z	B	I			

Para codificar la segunda letra del mensaje, e, repetimos el proceso. La letra clave que hay sobre la e es la I, así que la codificamos mediante una línea diferente del cuadro Vegenère: la línea I (línea 8), que es un nuevo alfabeto cifrado. Para codificar la e observamos dónde se cruza la columna que empieza por e con la línea que comienza por I, y resulta ser en la letra M. Por consiguiente, a esa letra e del texto llano la representa la M en el texto cifrado. Cada letra de la clave indica un alfabeto cifrado determinado en el cuadro de Vegenère. La quinta letra del mensaje se codifica según la quinta letra de la clave, O, pero para codificar la sexta letra del mensaje tenemos que volver a la primera letra de la clave, H. Una palabra clave más larga, o quizá una frase clave, introduciría más líneas en el proceso de codificación e incrementaría la complejidad de la cifra. La Tabla 4 muestra un cuadro Vegenère, marcando las cinco líneas (esto es, los cinco alfabetos cifrados) definidos por la clave HIELO. Tabla 4. Un cuadro Vegenère con las líneas definidas por la palabra HIELO tramadas.

Llano	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
1	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M

14	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
26	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Tabla 4

La gran ventaja de la cifra Vegenère es que resulta inexpugnable para el análisis de frecuencia descrito en el Capítulo 1. Por ejemplo, un criptoanalista que aplica el análisis de frecuencia a un texto cifrado, generalmente comienza identificando la letra más corriente en el texto cifrado, que en este caso es la W, y entonces asume que representa a la letra más frecuente en castellano, la a. Pero, en realidad, la W representa tres letras diferentes, la s, la i y la o, pero no la a. Esto presenta un claro problema para el criptoanalista. El hecho de que una letra que aparece varias veces en el texto cifrado pueda representar en cada ocasión una letra diferente del texto llano genera una ambigüedad tremenda para el criptoanalista. Igualmente confuso es el hecho de que una letra que aparece varias veces en el texto llano pueda estar representada por diferentes letras en el texto cifrado. Por ejemplo, la letra e aparece dos veces en este, pero es sustituida por dos letras diferentes: la primera, por S, y la segunda, por I

Además de ser invulnerable al análisis de frecuencia, la cifra Vegenère tiene un número enorme de claves. El emisor y el receptor pueden acordar usar cualquier palabra del diccionario, cualquier combinación de palabras, o incluso crear palabras. Un criptoanalista sería incapaz de descifrar el mensaje buscando todas las claves

posibles porque el número de opciones es simplemente demasiado grande.

La obra de Vegenère culminó con su *Traicté des Chiffres*, publicado en 1586. Irónicamente, se trataba del mismo año en que Thomas Phelippes estaba descifrando la cifra de la reina María Estuardo. Si el secretario de María hubiera leído este tratado habría aprendido la cifra Vegenère, los mensajes de María a Babington habrían desconcertado a Phelippes y puede que la vida de María se hubiera salvado.

A causa de su solidez y su garantía de seguridad parecería natural que la cifra de Vegenère hubiera sido adoptada rápidamente por los secretarios de cifras de toda Europa. ¿No les hubiera supuesto un gran alivio tener acceso, de nuevo, a una forma segura de codificación? Por el contrario, los secretarios de cifras parecen haber desdeñado la cifra de Vegenère. Este sistema, a todas luces perfecto, permanecería prácticamente ignorado durante los dos siglos siguientes.

1. Del ignorado Vegenère al Hombre de la Máscara de Hierro

Las formas tradicionales de cifra de sustitución, las que ya existían antes de la cifra Vegenère, se llamaban cifras de sustitución monoalfabética porque utilizaban sólo un alfabeto cifra en cada mensaje. En cambio, la cifra Vegenère pertenece a una clase conocida como *polialfabética*, porque emplea varios alfabetos cifra en cada mensaje. La naturaleza polialfabética de la cifra Vegenère es lo que le da su fuerza, pero también hace que sea mucho más complicada de usar. El esfuerzo adicional requerido para poner en práctica la cifra Vegenère disuadió a mucha gente de utilizarla.

Para muchas de las finalidades del siglo XVII, la cifra de sustitución monoalfabética resultaba perfectamente adecuada. Si querías asegurarte de que tu criado no pudiera leer tu correspondencia privada, o si querías proteger tu diario de los ojos entrometidos de tu cónyuge, entonces el tipo de cifra tradicional era ideal. La sustitución monoalfabética era rápida, fácil de usar y segura contra gente sin conocimientos de criptoanálisis. De hecho, la cifra de sustitución monoalfabética simple perduró en diversas formas durante muchos siglos (véase el Apéndice B). Para aplicaciones más serias, tales como las comunicaciones militares y gubernamentales, en las que la seguridad era de suma importancia, la cifra

monoalfabética directa resultaba claramente inadecuada. Los criptógrafos profesionales en guerra con los criptoanalistas profesionales necesitaban algo mejor y, sin embargo, se mostraban reticentes a adoptar la cifra poli alfabética a causa de su complejidad. Las comunicaciones militares, en particular, requerían velocidad y simplicidad, ya que, como una oficina diplomática podía enviar y recibir cientos de mensajes cada día, el tiempo era esencial. Por consiguiente, los criptógrafos buscaron una cifra intermedia, que fuera más difícil de descifrar que una cifra monoalfabética directa, pero más sencilla de utilizar que una cifra polialfabética.

Entre las candidatas estaba la extraordinariamente efectiva *cifra de sustitución homofónica.* En ella, cada letra es reemplazada por una variedad de sustitutos, y el número de sustitutos potenciales es proporcional a la frecuencia de la letra. Por ejemplo, la letra a supone aproximadamente el 8 por ciento de todas las letras del inglés escrito, de manera que asignaríamos ocho símbolos para representarla. Cada vez que aparece una a en el texto llano sería reemplazada en el texto cifrado por uno de los ocho símbolos elegidos al azar, de forma que para el final de la codificación cada símbolo constituiría aproximadamente el 1 por ciento del texto codificado. En cambio, la letra b supone solamente el 2 por ciento de todas las letras, de manera que sólo asignaríamos dos símbolos para representarla. Cada vez que aparece la b en el texto llano se puede elegir uno de esos dos símbolos, y para el final de la codificación cada símbolo constituiría aproximadamente el 1 por ciento del texto codificado. Este proceso de asignar varios números o símbolos para que actúen como sustitutos de cada letra continúa con todas las demás letras, hasta llegar a la z, que es tan infrecuente que sólo tiene un símbolo que la sustituya. En el ejemplo ofrecido en la Tabla 5, los sustitutos en el alfabeto cifra son cifras de dos números, y hay entre uno y doce sustitutos para cada letra del alfabeto llano, dependiendo de la relativa abundancia de cada letra en el uso ordinario.

Podemos considerar que todos los números de dos cifras que corresponden a la letra a del texto llano representan el mismo sonido en el texto cifrado, concretamente el sonido de la letra a. De ahí el origen del término «sustitución homofónica»: *hornos* significa «mismo» y *phone* significa «sonido» en griego. El propósito de ofrecer varias opciones de sustitución para las letras frecuentes es mantener el equilibrio de los símbolos en el texto cifrado. Si codificamos un mensaje

utilizando el alfabeto cifrado de la Tabla 5, cada uno de los números constituiría aproximadamente el 1 por ciento del texto entero. Si ningún símbolo aparece con más frecuencia que ningún otro, un intento de descifrамiento usando el análisis de frecuencia se ve seriamente amenazado. ¿Ofrece, por tanto, una seguridad perfecta? No del todo.

a	b	c	d	e	f	s	h	i	i	k	i	m	n	o	p	q	r	s	t	u	v	w	x	y	z
0	4	1	0	1	1	0	2	3	1	0	2	2	1	0	3	9	2	1	1	0	3	6	2	2	0
9	8	3	1	4	0	6	3	2	5	4	6	2	8	0	8	4	9	1	7	8	4	0	8	1	2
1	8	4	0	1	3	2	3	7			3	2	5	0	9		3	1	2	6		8		5	
2	1	1	3	6	1	5	9	0			7	7	8	5	5		5	9	0	1		9		2	
3		6	4	2			5	7			5		5	0			4	3	3	6					
3		2	5	4			0	3			1		9	7			0	6	0	3					
4			7	4			5	8			8		6	5			4	7	4						
7			9	4			6	3			4		6	4			2	6	3						
5				4			6	8					7	7			7	8	4						
3				6			5	8					1	2			7	6	9						
6				5			6	9					9	9			8	9	6						
7				5			8	3					1	0			0	6	9						
7				5										9					7						
8				7										9					5						
9				6															8						
2				4															5						
				7															9						
				4															7						
				8																					
				2																					
				8																					
				7																					
				9																					
				8										.											

Tabla 5. Un ejemplo de cifra de sustitución homofónica. La línea superior representa

el alfabeto llano, mientras que los números de abajo representan el alfabeto cifrado, con varias opciones dependiendo de la frecuencia de las letras en inglés escrito.

El texto cifrado todavía contiene muchas pistas sutiles para el criptoanalista hábil. Como ya vimos en el Capítulo 1, cada letra de un idioma tiene su propia personalidad, determinada por su relación con todas las demás letras, y estos rasgos aún se pueden discernir, incluso si la codificación se realiza mediante la sustitución homofónica. En inglés, el ejemplo más extremo de una letra con personalidad distintiva es la letra q, que sólo aparece seguida por una letra, concretamente la u. Si estuviésemos tratando de descifrar un texto cifrado, podríamos comenzar por notar que la q es una letra infrecuente y, por tanto, es probable que esté representada sólo por un símbolo, y sabemos que la u, que supone aproximadamente el 3 por ciento de todas las letras, probablemente esté representada por tres símbolos. Así que, si encontramos un símbolo en el texto cifrado que sólo esté seguido por tres símbolos particulares, entonces sería razonable asumir que el primer símbolo representa la letra q y los otros tres símbolos representan a la u. Otras letras son más difíciles de localizar, pero también las delata su relación con las demás letras. Aunque la cifra homofónica es descifrable, es mucho más segura que una cifra monoalfabética simple.

Una cifra homofónica puede parecer similar a una cifra polialfabética en la medida en que cada letra de texto llano se puede codificar de muchas maneras, pero existe una diferencia crucial, y la cifra homofónica es en realidad un tipo de cifra monoalfabética. En la tabla homofónica anterior (Tabla 5), la letra a puede ser representada por ocho números. Característicamente, estos ochos números representan sólo a la letra a. En otras palabras, una letra del texto llano puede ser representada por varios símbolos, pero cada símbolo sólo puede representar a una letra. En una cifra polialfabética, una letra del texto llano también será representada por diferentes símbolos, pero —y esto es lo que la hace más confusa— estos símbolos representarán a letras diferentes a lo largo del proceso de una codificación.

Posiblemente, la razón fundamental por la que la cifra homofónica es considerada monoalfabética es que, una vez ha sido establecido el alfabeto cifrado, permanece

constante durante todo el proceso de codificación. El hecho de que el alfabeto cifrado contenga varias opciones para codificar cada letra es irrelevante. Sin embargo, un criptógrafo que utilice una cifra polialfabética debe cambiar continuamente entre alfabetos cifrados claramente diferentes durante el proceso de codificación.

La alteración de la cifra monoalfabética básica de diversas maneras, tales como añadir homófonos, hizo posible cifrar mensajes de forma segura, sin tener que recurrir a las complejidades de la cifra polialfabética. Uno de los ejemplos más notables de una cifra monoalfabética mejorada lo constituyó la Gran Cifra de Luis XIV la cual fue utilizada para cifrar los mensajes más secretos del rey, protegiendo los detalles de sus planes, conspiraciones y maquinaciones políticas. Uno de estos mensajes mencionaba a uno de los personajes más enigmáticos de la Historia de Francia, el Hombre de la Máscara de Hierro, pero la solidez de la Gran Cifra significó que el mensaje y su extraordinario contenido permanecerían sin ser descifrados y, por tanto, leídos, durante dos siglos.

La Gran Cifra fue inventada por el equipo formado por un padre y su hijo, Antoine y Bonaventure Rossignol. Antoine había alcanzado prominencia por vez primera en 1626, cuando le entregaron una carta codificada capturada a un mensajero que abandonaba la sitiada ciudad de Réalmont. Antes de que acabara el día ya había descifrado la carta, revelando que el ejército hugonote que había mantenido la ciudad estaba a punto de caer. Los franceses, que hasta entonces no habían sido conscientes de la desesperada situación de los hugonotes, devolvieron la carta acompañada de su desciframiento. Los hugonotes, al saber ahora que su enemigo no cedería, no tardaron en rendirse. El desciframiento había tenido como resultado una cómoda victoria francesa.

El poder del desciframiento de cifras se hizo obvio, y los Rossignol obtuvieron puestos elevados en la corte. Después de servir a Luis XIII trabajaron como criptoanalistas para Luis XIII que estaba tan impresionado que trasladó las oficinas de los Rossignol junto a sus propios aposentos para que Rossignol *pére et fils* tuvieran un papel central en el desarrollo de la política diplomática francesa. Uno de los mayores tributos a sus habilidades lo constituye el hecho que la palabra *rossignol* se convirtió en argot francés para designar un artificio que abre

cerraduras, un reflejo de su destreza para abrir cifras.

El talento de los Rossignol para descifrar cifras les proporcionó la comprensión para crear una forma más sólida de codificación y fueron ellos los que inventaron la denominada Gran Cifra, tan segura que desafió los esfuerzos de todos los criptoanalistas enemigos que trataron de robar secretos franceses. Por desgracia, después de la muerte del padre y del hijo la Gran Cifra cayó en desuso y sus detalles exactos se perdieron rápidamente, lo que significó que los documentos cifrados de los archivos franceses ya no podían ser leídos. La Gran Cifra era tan sólida que incluso desafió los esfuerzos de las siguientes generaciones de descifradores.

Los historiadores sabían que los documentos cifrados por la Gran Cifra ofrecerían una idea única de las intrigas de la Francia del siglo XVII, pero ni siquiera para finales del siglo XIX habían conseguido descifrarlos. Entonces, en 1890, Víctor Gendron, un historiador militar que investigaba las campañas de Luis XIV sacó a la luz una nueva serie de cartas codificadas con la Gran Cifra. Incapaz de encontrarles algún sentido, se las pasó al comandante Étienne Bazeries, un distinguido experto del Departamento Criptográfico del Ejército francés. Bazeries vio en las cartas el desafío supremo y se pasó los tres años siguientes de su vida tratando de descifrarlas.

Las páginas cifradas contenían miles de números, pero sólo 587 diferentes. Era obvio que la Gran Cifra era más complicada que una cifra de sustitución simple, porque ésta sólo requeriría 26 números diferentes, uno por cada letra. Inicialmente, Bazeries pensó que los números sobrantes representaban homófonos, y que varios números representaban a la misma letra. Explorar esta posibilidad le llevó meses de esfuerzo concienzudo, pero todo fue en vano. La Gran Cifra no era una cifra homofónica.

A continuación, se le ocurrió que cada número podía representar un par de letras, o *dígrafo.* Sólo hay 26 letras individuales, pero hay 676 posibles pares de letras, y esa cifra corresponde aproximadamente a la variedad de números que aparecen en esos textos cifrados. Bazeries intentó un desciframiento buscando los números más frecuentes en los textos cifrados (22, 42, 124, 125 y 341), asumiendo que posiblemente representaban los dígrafos más frecuentes en francés (es, en, ou, de,

nt). En realidad, estaba aplicando el análisis de frecuencia al nivel de los pares de letras. Por desgracia, y de nuevo tras meses de trabajo, esta teoría tampoco produjo ningún desciframiento significativo.

Bazeries debía estar a punto de abandonar su obsesión cuando se le ocurrió una nueva línea de ataque. Quizá, la idea del dígrafo no estaba tan desencaminada. Comenzó a considerar la posibilidad de que cada número representara, no un par de letras, sino una sílaba entera. Trató de emparejar cada número con una sílaba, suponiendo que los números que aparecían con más frecuencia representaban las sílabas francesas más corrientes. Probó varias permutaciones tentativas, pero todas ellas dieron como resultado un galimatías, hasta que logró identificar una palabra particular. Un grupo de números (124-22-125-46-345) aparecía varias veces en cada página, y Bazeries postuló que representaban «les-en-ne- mi-s», es decir, «les enemis» (los enemigos). Esto resultó ser un avance crucial.

Bazeries pudo entonces continuar examinado otras partes de los textos cifrados donde aparecían estos números dentro de palabras diferentes. A continuación, insertó los valores silábicos derivados de «les enemis», lo que reveló partes de otras palabras. Como cualquier adicto a los crucigramas sabe, cuando una palabra está parcialmente rellenada, a menudo es posible adivinar el significado de esa palabra. Según Bazeries iba completando nuevas palabras, identificaba también nuevas sílabas, que a su vez llevaban a otras palabras, y así sucesivamente. Con frecuencia, se quedaba perplejo, en parte porque los valores silábicos nunca eran obvios, en parte porque algunos de los números representaban letras sueltas en vez de sílabas, y en parte porque los Rossignol habían puesto trampas dentro de la cifra. Por ejemplo, había un número que no representaba ni una sílaba ni una letra, sino que taimadamente suprimía el número previo.

Cuando el desciframiento se completó finalmente, Bazeries se convirtió en la primera persona que veía los secretos de Luis XIV en doscientos años. El recién descifrado material fascinó a los historiadores, que se centraron en una carta particularmente tentadora. Parecía resolver unos de los grandes misterios del siglo XVII: la verdadera identidad del Hombre de la Máscara de Hierro.

El Hombre de la Máscara de Hierro había sido objeto de mucha especulación desde que fue encarcelado en la fortaleza francesa de Pignerole, en Savoy. Cuando fue

trasladado a la Bastilla en 1698, los campesinos trataron de verlo, aunque fuera fugazmente, y dieron muchas versiones contradictorias, afirmando algunos que era bajo y otros altos, rubios unos y moreno otros, joven algunos y viejo algunos otros... Hubo quienes llegaron a afirmar que no era un hombre, sino una mujer. Con tan pocos hechos, todo el mundo, de Voltaire a Benjamin Franklin, creó su propia teoría para explicar el caso del Hombre de la Máscara de Hierro. La teoría conspiratoria más popular con relación a la Máscara (como a veces se le denominaba) sugería que se trataba del gemelo de Luis XIY condenado al encarcelamiento para evitar cualquier controversia sobre quién era el legítimo heredero al trono. Una versión de esta historia alega que existieron descendientes de la Máscara y, por tanto, una dinastía real oculta. Un librillo publicado en 1801 decía que Napoleón mismo era un descendiente de la Máscara, un rumor que, como realzaba su posición, el emperador no negó.

El mito de la Máscara inspiró incluso poesía, prosa y teatro. En 1848 Víctor Hugo había comenzado a escribir una obra teatral titulada Gemelos, pero cuando descubrió que Alejandro Dumas ya había optado por el mismo argumento, abandonó los dos actos que había escrito. Desde entonces, ha sido el nombre de Diurnas el que ha quedado asociado con la historia del Hombre de la Máscara de Hierro. El éxito de su novela reforzó la idea de que la Máscara estaba emparentado al rey, y esta teoría ha persistido a pesar de la evidencia revelada en uno de los desciframientos de Bazeries.

Bazeries había descifrado una carta escrita por Frangís de Louvois, el ministro de la Guerra de Luis XIV La carta comenzaba enumerando los delitos de Vivien de Bulonde, el comandante responsable de conducir un ataque a la ciudad de Cuneo, en la frontera francoitaliana. Aunque le habían ordenado quedarse y resistir, Bulonde se sintió preocupado por la posible llegada de tropas enemigas desde Austria y huyó, dejando atrás sus municiones y abandonando a muchos de sus soldados heridos. Según el ministro de la Guerra, estas acciones pusieron en peligro toda la campaña de Piedmont, y la carta dejaba muy claro que el rey consideraba las acciones de Bulonde como un acto de extrema cobardía:

Su Majestad conoce mejor que nadie las consecuencias de este acto,

y también es consciente de lo profundamente que nuestra fallida tentativa de tomar la plaza perjudicará nuestra causa, un fracaso que hay que reparar durante el invierno. Su Majestad desea que arrestéis inmediatamente al general Bulonde y hagáis que sea conducido a la fortaleza de Pignerole, donde lo encerrarán en una celda guardada por la noche, permitiéndosele caminar por las almenas durante el día cubierto con una máscara.

Ésta era una referencia explícita a un prisionero enmascarado en Pignerole, y a un delito suficientemente serio, con fechas que parecen encajar con el mito del Hombre de la Máscara de Hierro. ¿Esclarece esto el misterio? Como no era de extrañar, los que están a favor de soluciones más conspiratorias han encontrado fallos en Bulonde como candidato. Por ejemplo, existe el argumento de que si Luis XIV estaba realmente tratando de encarcelar secretamente a su gemelo no reconocido habría dejado una serie de pistas falsas. Quizá, la carta codificada se había escrito con la intención de que fuera descifrada. Quizá, el descifrador del siglo XIX había caído en una trampa del siglo XVTT.

2. Las Cámaras Negras

Reforzar la cifra monoalfabética aplicándola a las sílabas o añadiendo homófonos puede que fuera suficiente durante el siglo XVII, pero para el XVII el criptoanálisis empezaba a industrializarse, con equipos de criptoanalistas gubernamentales que trabajaban juntos para descifrar muchas de las cifras monoalfabéticas más complejas. Cada poder europeo tenía su propia Cámara Negra, como se denominaba a los centros neurálgicos para descifrar mensajes y acumular inteligencia. La Cámara Negra más célebre, disciplinada y eficiente era el Geheime Kabinets-Kanzlei de Viena.

Operaba según un horario riguroso, porque era vital que sus infames actividades no interrumpiesen el fluido funcionamiento del servicio postal. Las cartas que debían ser entregadas en las embajadas que había en Viena primero se mandaban a la Cámara Negra, a la que llegaban a las siete de la mañana. Los secretarios fundían los sellos de lacre, y un equipo de esteganógrafos trabajaba paralelamente para

hacer copias de las cartas. Si era necesario, un especialista en idiomas se responsabilizaría de duplicar escrituras inusuales. En menos de tres horas las cartas habían vuelto a ser selladas en sus sobres y devueltas a la oficina de correos central, para poder ser entregadas en su destino previsto. El correo que estaba meramente en tránsito por Austria llegaba a la Cámara Negra a las 10 de la mañana y el correo que salía de las embajadas de Viera con destino al extranjero llegaba a la Cámara a las cuatro de la tarde. Todas estas cartas también eran copiadas antes de poder continuar su viaje. Cada día se filtraban unas cien cartas por la Cámara Negra de Viena.

Las copias pasaban a los criptoanalistas, que se sentaban en pequeñas cabinas, listos para extraer el significado de los mensajes. Además de suministrar inteligencia valiosísima a los emperadores de Austria, la Cámara Negra de Viena vendía la información que acumulaba a otros poderes europeos. En 1774 se llegó a un acuerdo con Abbot Georgel, el secretario de la embajada francesa, que le proporcionó acceso a un paquete de información dos veces por semana a cambio de 1000 ducados. Él enviaba entonces estas cartas, que contenían los planes supuestamente secretos de varios monarcas, directamente a Luis XV en París.

Las Cámaras Negras estaban logrando volver inseguras todas las formas de cifra monoalfabética. Enfrentados a semejante oposición criptoanalítica profesional, los criptógrafos se vieron forzados por fin a adoptar la cifra Vegenère, más compleja pero más segura. Gradualmente, los secretarios de cifras comenzaron a pasarse a las cifras polialfabéticas.

Además de un criptoanálisis más eficaz, había otra presión que favorecía el paso hacia formas más seguras de codificación: el desarrollo del telégrafo, y la necesidad de proteger los telegramas de poder ser interceptados y descifrados.

Aunque el telégrafo, junto a la subsiguiente revolución de las telecomunicaciones, apareció en el siglo XIX, sus orígenes se remontan a 1753. Una carta anónima en una revista escocesa describió cómo se podía enviar un mensaje a través de grandes distancias conectando al emisor y al receptor con 26 cables, uno por cada letra del alfabeto. El emisor podía entonces deletrear el mensaje enviando pulsaciones de electricidad por cada cable. Por ejemplo, para deletrear hola, el emisor comenzaría enviando una señal por el cable h, luego por el cable o, y así

sucesivamente. El receptor sentiría de alguna forma la corriente eléctrica que surgía de cada cable y leería el mensaje. Sin embargo, este «expeditivo método de transmitir inteligencia», como lo llamó su inventor, nunca llegó a construirse, porque existían varios obstáculos técnicos que debían ser superados.

Por ejemplo, los ingenieros necesitaban un sistema suficientemente sensible para detectar señales eléctricas. En Inglaterra, *sir* Charles Wheatstone y William Fothergill Cooke construyeron detectores a partir de agujas magnetizadas, que podían hacerse girar en presencia de una corriente eléctrica entrante. En 1839, el sistema Wheatstone-Cooke se utilizaba para enviar mensajes entre las estaciones de ferrocarril de West Drayton y Paddington, a una distancia de 29 km. La reputación del telégrafo y su extraordinaria velocidad de comunicación no tardó en extenderse, y lo que más contribuyó a popularizar su poder fue el nacimiento del segundo hijo de la reina Victoria, el príncipe Alfred, el 6 de agosto de 1844 en Windsor. La noticia del nacimiento se telegrafió a Londres, y en menos de una hora *The Times* estaba en las calles anunciando la nueva. El periódico daba crédito a la tecnología que le había permitido esta hazaña, mencionando que estaba «en deuda con el extraordinario poder del Telégrafo Electro-Magnético». Al año siguiente, el telégrafo ganó aún más fama cuando ayudó a capturar a John Tawell, que había asesinado a su amante en Slough, tratando de escapar saltando a un tren que se dirigía a Londres. La policía local telegrafió la descripción de Tawell a Londres, y éste fue arrestado en cuanto llegó a la estación de Paddington.

Mientras tanto, en Norteamérica, Samuel Morse acababa de construir su primera línea de telégrafo, un sistema que abarcaba los 60 km que separan a Baltimore de Washington. Morse utilizó un electroimán para mejorar la señal, de manera que al llegar al receptor fuera lo suficientemente fuerte para hacer una serie de marcas cortas y largas —puntos y rayas— sobre una hoja de papel. También desarrolló el código Morse, que ahora nos es tan familiar, para traducir cada letra del alfabeto a una serie de puntos y rayas, tal como aparece en la Tabla 6. Para completar su sistema diseñó una caja sonora, para que el receptor oyera cada letra como una serie de puntos y rayas audibles.

En Europa, el sistema Morse ganó gradualmente en popularidad al Wheatstone-Cooke, y en 1851 una versión europea del código Morse, que incluía letras

acentuadas, fue adoptada por todo el continente. Según pasaban los años, el código Morse y el telégrafo tenían cada vez más influencia en el mundo, permitiendo a la policía capturar más criminales, ayudando a los periódicos a traer las noticias más recientes, proveyendo de valiosa información a las empresas y posibilitando que compañías muy distantes hicieran tratos instantáneos.

Sin embargo, proteger estas comunicaciones, a menudo tan delicadas, era una gran preocupación. El código Morse mismo no es una forma de criptografía, porque no hay una ocultación del mensaje. Los puntos y las rayas son simplemente una forma conveniente de representar las letras para el medio telegráfico; en realidad, el código Morse no es otra cosa que un alfabeto alternativo.

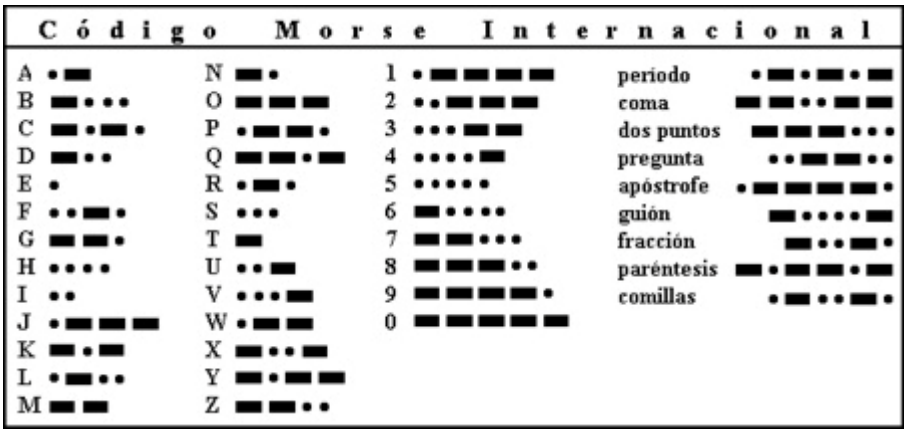


Tabla 6. Símbolos del código Morse internacional.

El problema de la seguridad surgió primordialmente porque cualquiera que quisiera enviar un mensaje había de entregarlo a un operador del código Morse, un telegrafista, que tenía que leerlo para transmitirlo. Los telegrafistas tenían acceso a todos los mensajes y, por tanto, existía el riesgo de que una empresa sobornase a un telegrafista para tener acceso a las comunicaciones de su rival. Este problema fue esbozado en un artículo sobre la telegrafía publicado en 1853 en la revista inglesa *Quarterly Review.*

> *También deberían tomarse medidas para evitar una gran objeción que se presenta en estos momentos con respecto a enviar comunicaciones privadas por telégrafo —la violación del secreto— porque en cualquier caso media docena de personas deben tener*

> *conocimiento de cada una de las palabras dirigidas por una persona a otra. Los empleados de la Compañía Inglesa de Telégrafo están bajo juramento de guardar secreto, pero a menudo escribimos cosas que resulta intolerable ver cómo personas extrañas leen ante nuestros ojos. Esta es una penosa falta del telégrafo, y debe ser remediada de un modo u otro.*

La solución consistía en codificar el mensaje antes de entregárselo al telegrafista. Entonces, éste traduciría el texto cifrado al código Morse antes de transmitirlo. Además de evitar que los telegrafistas viesen material delicado, la codificación también entorpecía los esfuerzos de cualquier espía que tratara de intervenir el cable telegráfico. Obviamente, la polialfabética cifra Vegenère era la mejor forma de asegurar el secreto para las comunicaciones de negocios importantes. Era considerablemente indescifrable, y se la conoció como *le chiffre indéchiffrable.* Al menos por ahora, los criptógrafos tenían una clara ventaja sobre los criptoanalistas.

3. Babbage contra la cifra Vegenère

La figura más fascinante del criptoanálisis del siglo XIX es Charles Babbage, el excéntrico genio británico más conocido por desarrollar el precursor del ordenador moderno. Nació en 1791, hijo de Benjamin Babbage, un rico banquero de Londres. Cuando Charles se casó sin el permiso de su padre perdió el acceso a la fortuna Babbage, pero todavía tenía suficiente dinero para gozar de seguridad económica y vivió como un erudito errante, aplicando su talento a cualquier problema que excitaba su imaginación. Sus inventos incluyen el velocímetro y el avisador de vacas, un aparato que se podía sujetar a la parte delantera de las locomotoras de vapor para apartar a las vacas de las vías del ferrocarril. Desde el punto de vista de los avances científicos, fue el primero en darse cuenta de que la anchura del anillo de un árbol dependía del tiempo que había hecho ese año, y dedujo que era posible determinar los climas pasados estudiando árboles muy antiguos. También se sentía fascinado por la estadística, y para divertirse trazó una serie de tablas de mortalidad, una herramienta básica para las compañías de seguros actuales.

Babbage no se limitó a abordar problemas científicos y de ingeniería. El coste de

enviar una carta dependía de la distancia que tenía que viajar dicha carta, pero Babbage señaló que el coste del trabajo requerido para calcular el precio de cada carta era superior al coste del franqueo. Por eso, propuso el sistema que todavía utilizamos hoy día: un precio único para todas las cartas, independientemente de en qué parte del país viva el destinatario. También le interesaban la política y los temas sociales, y hacia el final de su vida comenzó una campaña para deshacerse de los organilleros y de los músicos callejeros que deambulaban por Londres. Se quejó de que la música «a menudo da lugar a un baile de golfillos harapientos, y a veces de hombres medio embriagados, que en ocasiones acompañaban el ruido con sus propias voces disonantes. Otro grupo muy partidario de la música callejera es el de las mujeres de virtud elástica y tendencias cosmopolitas, a las que ofrece una excusa decente para exhibir sus fascinaciones en sus ventanas abiertas». Por desgracia para Babbage, los músicos se defendieron reuniéndose en grandes grupos en torno a su casa y tocando lo más fuerte que podían.

Figura 12. Charles Babbage

El momento decisivo de la vida científica de Babbage llegó en 1821, cuando él y el astrónomo John Herschel examinaron una serie de tablas matemáticas, de las que se usan como base para los cálculos de astronomía, ingeniería y navegación. Los dos hombres se sentían indignados por la cantidad de errores que había en las tablas, que a su vez generarían fallos en cálculos importantes. Una serie de tablas, las *Efemérides náuticas para encontrar la latitud y la longitud en el mar*, contenía más de mil errores. De hecho, se culpaba a las tablas defectuosas de causar muchos naufragios y desastres de ingeniería.

Estas tablas matemáticas se calculaban a mano, y los errores eran simplemente el resultado de errores humanos. Esto hizo que Babbage exclamara: *«¡Por Dios, ojalá hubiera realizado estos cálculos una máquina a vapor!»*. Esto marcó el principio de un esfuerzo extraordinario por construir una máquina capaz de calcular correctamente las tablas con un alto grado de exactitud. En 1823 Babbage diseñó el «Motor de Diferencias N.° 1», una excelente máquina calculadora que constaba de 25.000 piezas de precisión y que se debía construir con financiación del gobierno. Aunque Babbage era un brillante innovador, no se le daba tan bien poner en práctica sus ideas. Tras diez años de trabajo agotador, abandonó el «Motor de Diferencias N.° 1», inventó un diseño totalmente nuevo y se puso a construir el «Motor de Diferencias N.° 2».

Cuando Babbage abandonó su primera máquina, el gobierno perdió la confianza en él y decidió cortar por lo sano y retirarse del proyecto; ya había gastado 17.470 libras esterlinas, suficiente para construir un par de acorazados. Probablemente fue esta retirada de apoyo lo que provocó la siguiente queja de Babbage:

> *«Propón a un inglés cualquier principio, o cualquier instrumento y, por admirables que éstos sean, verás que todo el esfuerzo de la mente inglesa se concentra en encontrar una dificultad, un defecto o una imposibilidad en ellos. Si le hablas de una máquina para pelar patatas, dirá que es imposible: si pelas una patata con esa máquina delante de él, dirá que no sirve para nada, porque no puede cortar una papa en rodajas».*

La falta de financiación gubernamental significó que Babbage nunca completó el Motor de Diferencias N.° 2. La tragedia científica era que la máquina de Babbage habría ofrecido la característica única de ser programable. En vez de meramente calcular una serie específica de tablas, el Motor de Diferencias N.° 2 habría podido resolver una gran variedad de problemas matemáticos, dependiendo de las instrucciones que se le dieran. De hecho, el Motor de Diferencias N.° 2 suministró el modelo, la plantilla, para los ordenadores modernos. El diseño incluía una «reserva» (memoria) y un «molino» (procesador), que le permitirían tomar decisiones y repetir instrucciones, que son equivalentes a los comandos «SI... ENTONCES...» y «RIZO» de la programación moderna.

Un siglo después, durante el curso de la segunda guerra mundial, las primeras encarnaciones electrónicas de la máquina de Babbage tendrían un profundo efecto en el criptoanálisis, pero durante su propia vida, Babbage hizo una contribución igualmente importante al desciframiento de códigos: consiguió descifrar la cifra Vegenère y al hacerlo realizó el mayor avance criptoanalítico desde que los eruditos árabes del siglo IX descifraron la cifra monoalfabética inventando el análisis de frecuencia. El trabajo de Babbage no requirió cálculos mecánicos ni cómputos complejos. Por el contrario, lo único que utilizó fue pura astucia.

A Babbage le interesaban las cifras desde que era muy joven. Más adelante, recordó cómo esa afición de su infancia a veces le causó problemas: «Los chicos mayores hacían cifras, pero si yo conseguía unas pocas palabras, generalmente descubría la clave. En ocasiones, la consecuencia de este ingenio resultó dolorosa: los dueños de las cifras detectadas a veces me daban una paliza, a pesar de que la culpa la tenía su propia estupidez». Estas palizas no le desanimaron y continuó cautivado por el criptoanálisis. En su autobiografía escribió que «descifrar es, en mi opinión, una de las artes más fascinantes».

Pronto adquirió reputación en la sociedad londinense como criptoanalista dispuesto a abordar cualquier mensaje cifrado, y a veces se le acercaban extraños para consultarle todo tipo de problemas. Por ejemplo, Babbage ayudó a un biógrafo desesperado que trataba de descifrar las notas de taquigrafía de John Flamsteed, el primer astrónomo real de Inglaterra. También auxilió a un historiador resolviendo una cifra de Enriqueta María, la esposa de Carlos I de Inglaterra. En 1854 colaboró

con un abogado y utilizó el criptoanálisis para revelar una prueba crucial en un caso legal. A lo largo de los años, acumuló un gran archivo de mensajes cifrados, que planeaba usar como base para un libro seminal sobre el criptoanálisis, titulado *The Philosophy of Decyphering* («La filosofía del desciframiento»). El libro contendría dos ejemplos de todos los tipos de cifras, uno que sería descifrado como demostración y otro que sería dejado como ejercicio para el lector. Desgraciadamente, como sucedió con muchos otros de sus grandes planes, el libro nunca se completó.

Mientras la mayoría de los criptoanalistas habían abandonado toda esperanza de llegar a descifrar la cifra Vi gene re, a Babbage le animó a intentar el desciframiento un intercambio de cartas con John Hall Brock Thwaites, un dentista de Bristol con un concepto bastante inocente de las cifras. En 1854, Thwaites afirmó haber inventado una nueva cifra, que, en realidad, era equivalente a la cifra Vegenère. Escribió al *Journal of the Society of Arts* con la intención de patentar su idea, por lo visto sin darse cuenta de que llegaba con varios siglos de retraso. Babbage escribió a esa sociedad señalando que «la cifra... es muy antigua, y aparece en la mayoría de los libros». Thwaites no ofreció ningún tipo de disculpas y desafió a Babbage a descifrar su cifra. Que fuera o no descifrable no tenía nada que ver con el hecho de si era nueva o no, pero la curiosidad de Babbage se excitó lo suficiente como para embarcarse en la búsqueda de un punto débil en la cifra Vegenère.

Descifrar una cifra difícil es similar a escalar la cara muy escarpada de un acantilado. El criptoanalista busca cualquier resquicio o arista que pudiera proveer el más ligero apoyo. En una cifra monoalfabética, el criptoanalista se agarrará a la frecuencia de las letras, porque las letras más corrientes —en inglés, la e, la t y la a— destacarán no importa cómo hayan sido escondidas. En la polialfabética cifra Vegenère, las frecuencias están mucho más equilibradas, porque se usa la palabra cifra para cambiar entre diferentes alfabetos cifrados. Por eso, a primera vista, la roca parece perfectamente lisa.

Recuerde, la gran fuerza de la cifra Vegenère es que la misma letra será codificada de maneras diferentes. Por ejemplo, si la palabra clave es KING (rey), entonces cada letra del texto llano puede ser potencialmente codificada de cuatro maneras diferentes, porque la clave tiene cuatro letras. Cada letra de la clave define un

alfabeto cifrado diferente en el cuadro Vegenère, tal como se muestra en la Tabla 7. La columna e del cuadro ha sido marcada para mostrar cómo se codifica de manera distinta dependiendo de qué letra de la clave defina la codificación:

Si se usa la K de KING para codificar la e, la letra resultante en el texto cifrado es la O.

Si se usa la I de KING para codificar la e, la letra resultante en el texto cifrado es la M.

Si se usa la N de KING para codificar la e, la letra resultante en el texto cifrado es la R.

Si se usa la G de KING para codificar la e, la letra resultante en el texto cifrado es la K.

Llano	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
1	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q

18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
26	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Tabla 7. Un cuadro Vegenère utilizado en combinación con la clave KING. La clave define cuatro alfabetos cifrados separados, de forma que la letra e puede ser codificada como O, M, R o K.

De manera similar, palabras enteras serán descifradas de maneras diferentes: la palabra the, por ejemplo, podría ser codificada como DPR, BUK, GNO o ZRM, dependiendo de su posición en relación con la clave. Aunque esto dificulta muchísimo el criptoanálisis, tampoco hace que sea imposible. El dato importante que hay que notar es que si sólo hay cuatro maneras de codificar la palabra the, y el mensaje original contiene varios casos de la palabra the, entonces es altamente probable que alguna de las cuatro codificaciones posibles se repetirá en el texto cifrado. Vamos a demostrarlo con el siguiente ejemplo, en el que la línea The Sun and the Man in the Moon («El sol y el hombre en la luna») ha sido codificada usando la cifra Vigenére y la clave KING

Clave	K I N G K I N G K I N G K I N G K I N G K I N G
Texto llano	t h e s u n a n d t h e m a n i n t h e m o o n
Texto cifrado	D P R Y E V N T N B U K W I A O X B U K W W B T

La palabra the es codificada como DPR en el primer caso, y luego como BUK en la segunda y en la tercera ocasión. La causa de la repetición de BUK es que el segundo the está a ocho letras de distancia del tercer the, y ocho es un múltiplo del número de letras de la clave, que, como sabemos, tiene cuatro letras. En otras palabras, el segundo the fue codificado según su relación con la palabra clave (the

cae debajo de ING), y para cuando llegamos al tercer the, la clave ha pasado exactamente dos veces, de manera que se repite esa relación y, por tanto, la codificación.

Figura 13. El texto cifrado, codificado utilizando la cifra Vegenère.

Babbage se dio cuenta de que este tipo de repetición le suministraba exactamente la asidera que necesitaba para conquistar la cifra Vegenère. Logró definir una serie de pasos relativamente simples que cualquier criptoanalista podía seguir para descifrar la hasta entonces *chiffre indéchiffrable*. Para demostrar su brillante técnica, imaginemos que hemos interceptado el texto cifrado que aparece en la Figura 13. Sabemos que ha sido codificado utilizando la cifra Vegenère, pero no sabemos nada sobre el mensaje original, y la clave es un misterio.

La primera fase del criptoanálisis de Babbage consiste en buscar secuencias de letras que aparecen más de una vez en el texto cifrado. Hay dos maneras en las

que podrían surgir semejantes repeticiones. La más probable es que la misma secuencia de letras del texto llano haya sido codificada usando la misma parte de la clave. Como alternativa, existe una ligera posibilidad de que dos secuencias de letras diferentes del texto llano hayan sido codificadas usando diferentes partes de la clave, resultando por casualidad en una secuencia idéntica en el texto cifrado. Si nos limitamos a secuencias largas, entonces podemos descartar en gran medida la segunda posibilidad y en este caso, sólo consideramos las secuencias repetidas que tengan cuatro letras o más. La Tabla 8 es un registro de tales repeticiones y de los espacios que hay entre la repetición. Por ejemplo, la secuencia E-F-I-Q aparece en la primera línea del texto cifrado y luego en la quinta línea, separada por 95 letras.

Además de utilizarse para codificar el texto llano y convertirlo en el texto cifrado, la clave la usa también el receptor para descifrar el texto cifrado y volverlo a convertir en el texto llano. Por eso, si pudiéramos identificar la clave, descifrar el texto no sería difícil. En esta fase aún no disponemos de suficiente información para deducir la clave, pero la Tabla 8 nos proporciona indicios muy buenos sobre su longitud. Tras enumerar qué secuencias se repiten, así como los espacios que hay entre las repeticiones, el resto de la Tabla se dedica a identificar los *factores* de los espaciamientos: los números por los que se pueden dividir los espaciamientos. Por ejemplo, la secuencia W-C-X-Y-M se repite tras 20 letras, por lo que los números 1, 2, 4, 5, 10 y 20 son factores, ya que pueden dividir exactamente a 20 sin dejar decimales. Estos factores sugieren seis posibilidades:

1. La clave tiene 1 letra y se recicla 20 veces entre las codificaciones.
2. La clave tiene 2 letras y se recicla 10 veces entre las codificaciones.
3. La clave tiene 4 letras y se recicla 5 veces entre las codificaciones.
4. La clave tiene 5 letras y se recicla 4 veces entre las codificaciones.
5. La clave tiene 10 letras y se recicla 2 veces entre las codificaciones.
6. La clave tiene 20 letras y se recicla 1 vez entre las codificaciones.

La primera posibilidad puede ser excluida, porque una clave que sólo tenga una letra da lugar a una cifra monoalfabética, sólo se usaría una línea del cuadro Vegenère para toda la codificación, y el alfabeto cifrado permanecería inalterado; es muy improbable que un criptógrafo hiciera algo así. Para indicar cada una de las

demás posibilidades se ha colocado un signo ✓ en la columna apropiada de la Tabla 8. Cada ✓indica una longitud potencial de la clave.

Secuencia repetida	Espacio entre repeticiones	Posible longitud de la clave (o factores)																	
		2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
E-F-I-Q	95				✓														✓	
P-S-D-L-P	5				✓															
W-C-X-Y-M	20	✓		✓	✓					✓										✓
E-T-R-L	120	✓	✓	✓	✓	✓		✓		✓		✓			✓					✓

Tabla 8. Repeticiones y espacios entre ellas en el texto cifrado

Para identificar si la clave tiene 2, 4, 5, 10 o 20 letras necesitamos observar los factores de todos los demás espaciamientos. Como la clave parece tener 20 letras o menos, la Tabla 8 enumera los factores equivalentes para cada uno de los espaciamientos. Hay una clara propensidad por el espaciamiento divisible por 5. De hecho, todos los espaciamientos que aparecen son divisibles por 5. La primera secuencia repetida, E-F-I-Q, se puede explicar con una clave de 5 letras, reciclada 19 veces entre la primera codificación y la segunda. La segunda secuencia repetida, P-S-D-L-P, se puede explicar con una clave de 5 letras, reciclada sólo una vez entre la primera codificación y la segunda. La tercera secuencia repetida, W-C-X-Y-M, se puede explicar con una clave de 5 letras, reciclada 4 veces entre la primera codificación y la segunda. La cuarta secuencia repetida, E-T-R-L, se puede explicar con una clave de 5 letras, reciclada 24 veces entre la primera codificación y la segunda. En resumen, todo concuerda con una clave de 5 letras.

Asumiendo que la clave tiene efectivamente 5 letras, el siguiente paso es deducir cuáles son exactamente esas letras. Por ahora, llamemos a la clave L_1-L_2-L_3-L_4-L_5, de forma que L_1 represente a la primera letra de la clave, y así sucesivamente. El proceso de codificación habría empezado codificando la primera letra del texto llano según la primera letra de la clave, L_1 La letra L_1 define una línea del cuadro Vegenère, y de hecho proporciona un alfabeto cifrado de sustitución monoalfabética para la primera letra del texto llano. Sin embargo, a la hora de codificar la segunda letra del texto llano, el criptógrafo habría usado L_2 para definir una línea distinta del

cuadro Vegenère, proporcionando de este modo un alfabeto cifrado de sustitución monoalfabética diferente. La tercera letra del texto llano se codificaría según L_3, la cuarta según L_4 y la quinta según L_5. Cada letra de la clave proporciona un alfabeto cifrado diferente para la codificación. Sin embargo, la sexta letra del texto llano sería codificada de nuevo según L_1 la séptima letra del texto llano sería codificada de nuevo según L_2 y el ciclo se repite después de eso. En otras palabras, la cifra polialfabética consta de cinco cifras monoalfabéticas, cada cifra monoalfabética es responsable de la codificación de un quinto del mensaje total y, lo que es más importante, ya sabemos cómo criptoanalizar las cifras monoalfabéticas.

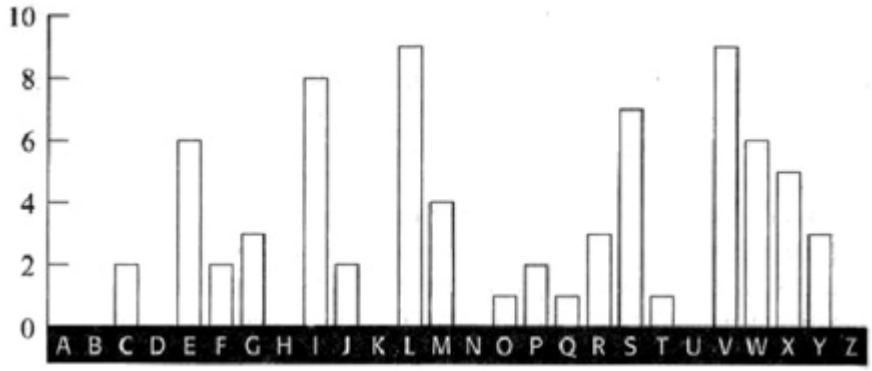


Figura 14. Distribución de frecuencias para las letras del texto cifrado, codifica do utilizando el alfabeto cifrado L, (número de apariciones).

Procederemos de la siguiente manera. Sabemos que una de las líneas del cuadro Vegenère, definida por L_1 proporciona el alfabeto cifrado para codificar las letras 1ª, 6ª, 11ª, 16ª... del mensaje. Por eso, si observamos las letras 1ª, 6ª, 11ª, 16ª... del texto cifrado podríamos utilizar el análisis de frecuencia tradicional para deducir el alfabeto cifrado en cuestión.

La Figura 14 muestra la distribución de la frecuencia de las letras que aparecen en las posiciones 1ª, 6ª, 11ª, 16ª... del texto cifrado, que son W, I, R, E. Es preciso recordar ahora que cada alfabeto cifrado del cuadro Vegenère es simplemente un alfabeto normal desplazado entre 1 y 26 posiciones. Por eso, la distribución de frecuencias de la Figura 14 debería tener rasgos similares a la distribución de frecuencias de un alfabeto normal, excepto que habrá sido desplazado unas cuantas posiciones. Al comparar la distribución con la distribución normal debería ser posible

calcular ese desplazamiento. La Figura 15 muestra la distribución de frecuencias normal en un fragmento de texto llano en inglés.

Figura 15. Distribución de frecuencias normal en inglés (número de apariciones jasado en un fragmento de texto llano que contiene el mismo número de letras que el texto cifrado).

La distribución normal muestra cimas, mesetas y valles, y para hacerla encajar con la distribución de la cifra ^ buscamos la combinación de rasgos más sobresaliente. Por ejemplo, los tres pilares de R-S-T en la distribución normal (Figura 15) y la larga depresión a su derecha, que se extiende a lo largo de seis letras, de la U hasta la Z: ambas cosas juntas forman un par muy característico de rasgos. Los únicos rasgos similares en la distribución L_1 (Figura 14) son los tres pilares de V-W- X, seguidos de la depresión que se extiende a lo largo de seis letras, de la Y a la D. Esto sugeriría que todas las letras codificadas según L, se han desplazado cuatro posiciones o, en otras palabras, que define un alfabeto cifrado que comienza E, F, G, H A su vez, esto significa que la primera letra de la clave, L_b es probablemente la E. Esta hipótesis se puede poner a prueba desplazando la distribución L_1 cuatro lugares y comparándola con la distribución normal. La Figura 16 muestra ambas distribuciones para poder comparar. La coincidencia entre las cimas mayores es muy grande, implicando que resulta seguro asumir que la clave comienza efectivamente por E.

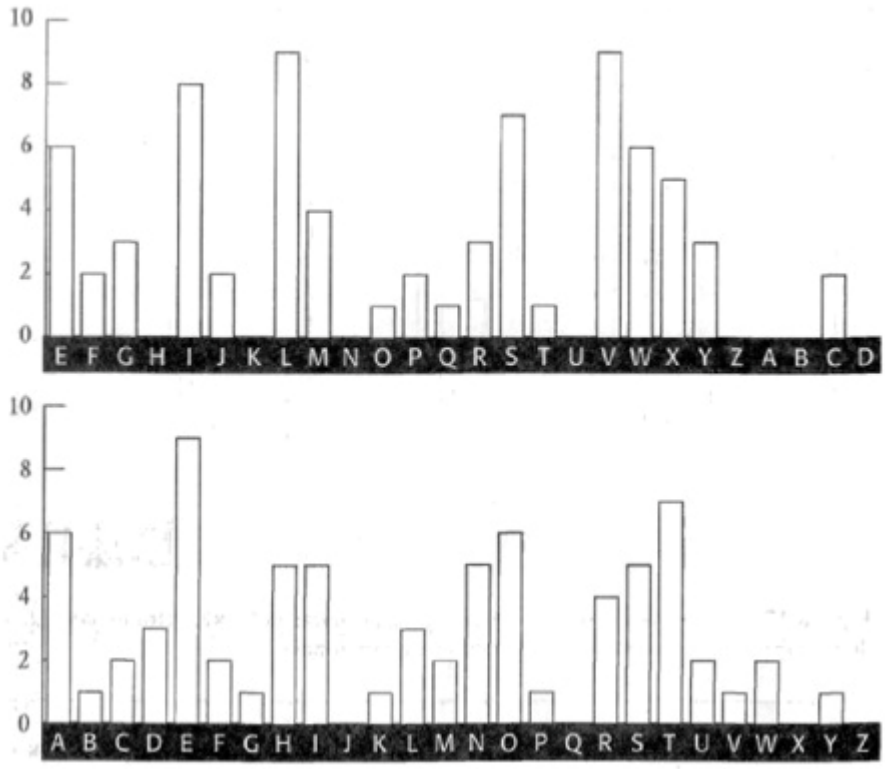


Figura 16. La distribución L_1 desplazada cuatro lugares (arriba)» comparada con la distribución de frecuencias normal (abajo). Todas las cimas y las depresiones principales encajan.

Resumiendo, buscar repeticiones en el texto cifrado nos ha permitido identificar la longitud de la clave, que resultó ser de cinco letras. Esto nos permitió dividir el texto cifrado en cinco partes, cada una de ellas codificada según una sustitución monoalfabética definida por una letra de la clave. Analizando la fracción del texto cifrado que fue codificada según la primera letra de la clave, hemos podido mostrar que esta letra L_1 es probablemente la E. Este proceso se repite para identificar la segunda letra de la clave. Así, establecemos una distribución de frecuencias para las letras 2ª, 7ª, 12ª, 17ª... del texto cifrado. De nuevo, la distribución resultante, que se muestra en la Figura 17, se compara con la distribución normal para deducir el desplazamiento.

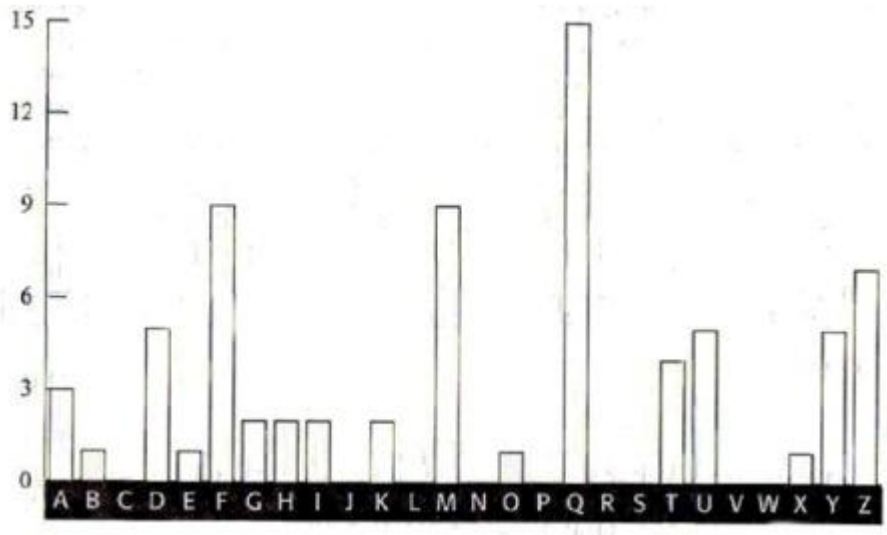


Figura 17. Distribución de frecuencias para las letras del texto cifrado, codificado usando el alfabeto cifrado L_1 (número de apariciones).

Esta distribución es más difícil de analizar. No hay candidatas obvias para las tres cimas vecinas que se corresponden con R-S-T en la distribución normal. No obstante, la depresión que se extiende de la G a la L es muy característica, y probablemente se corresponde con la depresión que esperamos ver extendiéndose de la U a la Z en la distribución normal. Si esto fuera así, esperaríamos que las tres cimas R-S-T aparecerían en la D, la E y la F, pero falta la cima de la E. Por ahora, desestimaremos la cima que falta como una irregularidad estadística y seguiremos nuestra reacción inicial, que es que la depresión de la G a la L es un rasgo apreciable de desplazamiento.

Esto sugeriría que todas las letras codificadas según L_2 han sido desplazadas 12 posiciones, o, en otras palabras, que define un alfabeto cifrado que comienza M, N, O, P... y que la segunda letra de la clave, L_2, es la M. Una vez más, esta hipótesis se puede poner a prueba desplazando la distribución L_2 doce lugares y comparándola con la distribución normal. La Figura 18 muestra ambas distribuciones y se ve que las cimas mayores encajan muchísimo, dando a entender que resulta seguro asumir que la segunda letra de la clave es efectivamente la M.

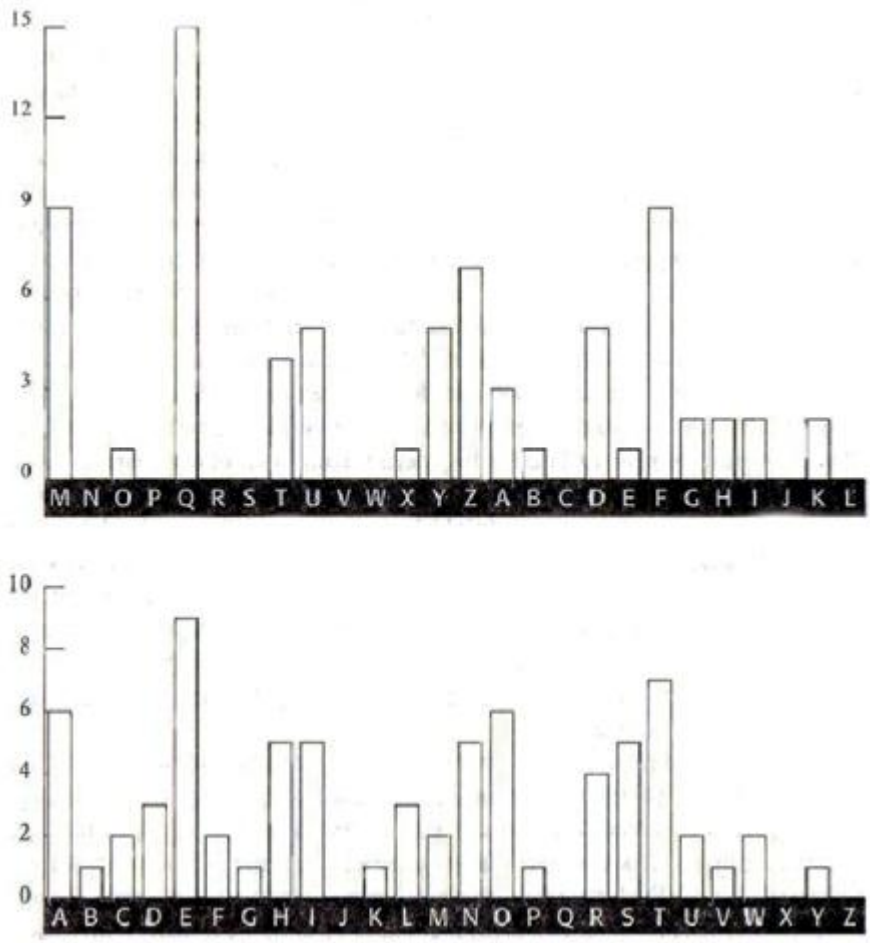


Figura 18. La distribución L_2 desplazada doce letras (arriba), comparada con la distribución de frecuencias normal (abajo). La mayoría de las principales cimas y depresiones coinciden.

No voy a continuar el análisis; baste decir que al analizar las letras 3ª, 8ª, 13ª... se deduce que la tercera letra de la clave es la I; al analizar las letras 4ª, 9ª, 14ª... se deduce que la cuarta letra es la L; y al analizar las letras 5ª, 10ª, 15ª... se deduce que la quinta letra es la Y. La clave es EMILY. Ahora es posible invertir la cifra Vegenère y completar el criptoanálisis. La primera letra del texto cifrado es la W, y fue codificada según la primera letra de la clave, la E. Invirtiendo el proceso, miramos el cuadro Vegenère y encontramos la W en la línea que comienza por E, y de esta forma descubrimos qué letra encabeza esa columna. Se trata de la S, por lo que la ponemos como la primera letra del texto llano. Repitiendo este proceso, vemos que el texto llano comienza

sittheedownandhavenoshame- cheekby-jowl...

Insertando las separaciones entre palabras y la puntuación adecuadas, llegamos por fin a:

Sit thee down, and have no shame,
Cheek by jowl, and knee by knee:
What care I for any name?
What for order or degree?

Let me screw thee up a peg:
Let me loose thy tongue with wine:
Callest thou that thing a leg?
Which is thinnest? thine or mine?

Thou shalt not be saved by works:
Thou hast been a sinner too:
Ruined trunks on withered forks,
Empty scarecrows, I and you!

Fill the cup, and fill the can:
Have a rouse before the morn:
Every moment dies a man,
Every moment one is born[6] .

[6] *«Siéntate y no tengas vergüenza*
codo con codo, y rodilla con rodilla
¿Qué me importa a mí un nombre?
¿O el orden, o un diploma?

Déjame que te enrosque a una clavija:
Déjame que suelte tu lengua con vino:
¿Llamas a eso una pierna?
¿Cuál es más flaca? ¿la tuya o la mía?
No te salvarán las obras:
Tú también has sido una pecadora:
¡Troncos estropeados sobre horquillas rotas,
Espantapájaros vacíos, yo y tú!

Llena la copa, y llena el bidón:

Son versos de un poema de Alfred Tennyson titulado «The Vision of Sin» («La visión del pecado»). La clave resulta ser el nombre de pila de la esposa de Tennyson, Emily Sellwood. Decidí utilizar un fragmento de este poema en particular para un ejemplo de criptoanálisis porque inspiró una curiosa correspondencia entre Babbage y el gran poeta. Como agudo estadístico y compilador de índices de mortalidad, a Babbage le irritaban los versos

«Cada momento muere un hombre,
Cada momento nace uno»,

que son las últimas líneas del texto llano previo. Por consiguiente, ofreció una corrección al poema de Tennyson, «por lo demás muy hermoso»:

Hay que señalar que si eso fuera cierto, la población del mundo estaría estancada... Yo le sugeriría que en la próxima edición de su poema, éste dijera:

«Cada momento muere un hombre,
Cada momento nace 1 $^{1}/_{16}$ »...

La cifra exacta es tan larga que no la puedo incluir en un verso, pero creo que la cifra 1 $^{1}/_{16}$ será suficientemente exacta para la poesía.
Muy atentamente, etc., Charles Babbage.

El satisfactorio criptoanálisis de la cifra Vegenère realizado por Babbage fue logrado probablemente en 1854, poco después de su altercado con Thwaites, pero su descubrimiento no fue reconocido en absoluto, porque nunca lo publicó. El descubrimiento no salió a la luz hasta el siglo XX, cuando algunos eruditos examinaron las extensas notas de Babbage. Mientras tanto, su técnica fue descubierta independientemente por Friedrich Wilhelm Kasiski, un oficial retirado del ejército prusiano. Desde 1863, cuando publicó su gran avance criptoanalítico en *Die*

Tómate un barril antes de que amanezca:
Cada momento muere un hombre
cada momento nace uno». (N.del T.)

Geheimschriften und die Dechiffrirkunst («La escritura secreta y el arte del desciframiento»), la técnica ha sido conocida como la Prueba Kasiski, y la contribución de Babbage ha sido ignorada en gran medida.

Pero ¿por qué no publicó Babbage su desciframiento de una cifra tan vital? Ciertamente, tenía el hábito de no acabar sus proyectos y no publicar sus descubrimientos, lo que podría sugerir que éste es simplemente un ejemplo más de su actitud indolente. Sin embargo, hay una explicación alternativa. Su descubrimiento sucedió poco después del estallido de la guerra de Crimea, y una teoría es que ese descubrimiento proporcionó a los británicos una clara ventaja sobre su enemigo ruso. Es muy posible que la Inteligencia británica exigiera que Babbage mantuviese secreto su trabajo, proporcionándoles de esta forma una ventaja de nueve años sobre el resto del mundo. Si esto fuera así, encajaría con la ya antigua tradición de encubrir los logros del desciframiento en beneficio de la seguridad nacional, una práctica que ha continuado en el siglo XX.

4. De las columnas de la agonía al tesoro escondido

Gracias a los avances realizados por Charles Babbage y Friedrich Kasiski, la cifra Vegenère ya no era segura. Los criptógrafos ya no podían garantizar el secreto ahora que los criptoanalistas habían contraatacado para recuperar el control en la guerra de las comunicaciones. Aunque los criptógrafos trataron de diseñar nuevas cifras, nada de gran importancia surgió durante la segunda mitad del siglo XIX, y la criptografía profesional estaba en desorden. No obstante, este mismo período presenció un enorme crecimiento del interés en las cifras entre el público en general.

El desarrollo del telégrafo, que había introducido un interés comercial en la criptografía, fue también el responsable de generar un interés público en la criptografía. El público se dio cuenta de la necesidad de proteger los mensajes personales de naturaleza altamente sensible, y si era necesario utilizaba la codificación, a pesar de que esto tardaba más tiempo en enviarse, por lo que subía el precio del telegrama. Los operadores Morse podían enviar un texto en inglés normal a una velocidad de hasta 35 palabras por minuto, porque podían memorizar frases enteras y transmitirlas de una sola vez, mientras que el revoltijo de letras

que constituye un texto cifrado era considerablemente más lento de transmitir, porque el operador tenía que consultar continuamente el mensaje escrito del emisor para revisar la secuencia de letras. Las cifras usadas por el público en general no habrían resistido el ataque de un criptoanalista profesional, pero eran suficiente para proteger el mensaje contra los fisgones fortuitos.

Según la gente fue sintiéndose cómoda con la codificación, empezó a expresar sus habilidades criptográficas de muy diversas maneras. Por ejemplo, en la Inglaterra victoriana con gran frecuencia se prohibía a los jóvenes amantes que expresaran su afecto en público, y ni siquiera podían comunicarse por carta por si sus padres interceptaban y leían su contenido. Esto tuvo como resultado que los amantes se intercambiaban mensajes cifrados a través de las columnas personales de los periódicos. Estas «columnas de la agonía», como se las llamaba, provocaron la curiosidad de los criptoanalistas, que escudriñaban las notas y trataban de descifrar su excitante contenido. Se sabe que Charles Babbage se deleitó en esta actividad, así como sus amigos *sir* Charles Wheatstone y el barón Lyon Playfair, que juntos fueron los responsables de la creación de la hábil *cifra Playfair* (descrita en el Apéndice C). En una ocasión, Wheatstone descifró una nota, aparecida en *The Times*, de un estudiante de Oxford, proponiendo a su amor verdadero que se fugaran. Unos pocos días después, Wheatstone insertó su propio mensaje, codificado con la misma cifra, aconsejando a la pareja que no llevase a cabo ese acto rebelde y precipitado. Poco después, apareció un tercer mensaje, esta vez sin codificar y remitido por la dama en cuestión:

«Querido Charlie, No escribas más.
Han descubierto nuestra cifra».

A su debido tiempo, una variedad más amplia de notas codificadas apareció en los periódicos. Los criptógrafos comenzaron a insertar trozos de textos cifrados simplemente para desafiar a sus colegas. En otras ocasiones, se utilizaron notas codificadas para criticar a figuras u organizaciones públicas. *The Times* publicó una vez sin darse cuenta la siguiente noticia cifrada: *«The Times* es el Jeffreys de la prensa». Estaban comparando al periódico con el notorio juez Jeffreys, del siglo XVII, dando a entender que era una publicación implacable e intimidadora que

actuaba como portavoz del gobierno.

Otro ejemplo de la familiaridad del público con la criptografía fue el amplio uso de la codificación por pinchazo. El antiguo historiador griego Eneas el Estratega sugirió comunicar un mensaje secreto pinchando agujeros diminutos bajo letras determinadas en una página de texto aparentemente inocua, igual que aparecen puntos bajo algunas letras de este párrafo. Estas letras deletreaban un mensaje secreto, fácil de leer para el receptor a quien iba dirigido. Sin embargo, si un intermediario miraba la página, probablemente no se daría cuenta del mensaje secreto. Dos mil años después, muchos escritores de cartas británicos usaron exactamente el mismo método, no para lograr el secreto, sino para evitar pagar precios de envío excesivos. Antes de la revisión del sistema postal inglés a mitad del siglo XIX, enviar una carta costaba alrededor de un chelín por cada mil millas, lo que resultaba impagable para la mayoría de la gente. Sin embargo, los periódicos se podían enviar gratis, y esto proporcionó un respiro a los ahorradores Victorianos. En vez de escribir y enviar cartas, la gente empezó a utilizar pinchazos para deletrear un mensaje en la portada de un periódico. Podían enviar el periódico por correo sin tener que pagar ni un penique.

La creciente fascinación del público con las técnicas criptográficas significó que los códigos y las cifras pronto se abrieron paso en la literatura del siglo XIX. En *Viaje al centro de la Tierra*, de Julio Verne, el desciframiento de un pergamino repleto de caracteres rúnicos provoca el primer paso del viaje épico. Los caracteres son parte de una cifra de sustitución que genera una escritura latina, que a su vez sólo tiene sentido si se invierten las letras: «Desciende el cráter del volcán de Sneffels cuando la sombra de Scartaris llega a acariciarlo antes de las calendas de julio, audaz viajero, y llegarás al centro de la Tierra». En 1885, Verne usó también una cifra como elemento fundamental en su novela Matías Sandorff.

En Gran Bretaña, uno de los mejores escritores de ficción criptográfica era sir Arthur Conan Doyle. No es raro, entonces, que Sherlock Holmes fuera un experto en criptografía y, como explicó al doctor Watson, Hiera también «el autor de una monografía insignificante en la que analizo ciento sesenta cifras diferentes». El desciframiento más famoso de Holmes se relata en La aventura de los hombres danzantes, que trata de una cifra que consiste en monigotes, en la que cada

postura representa una letra distinta.

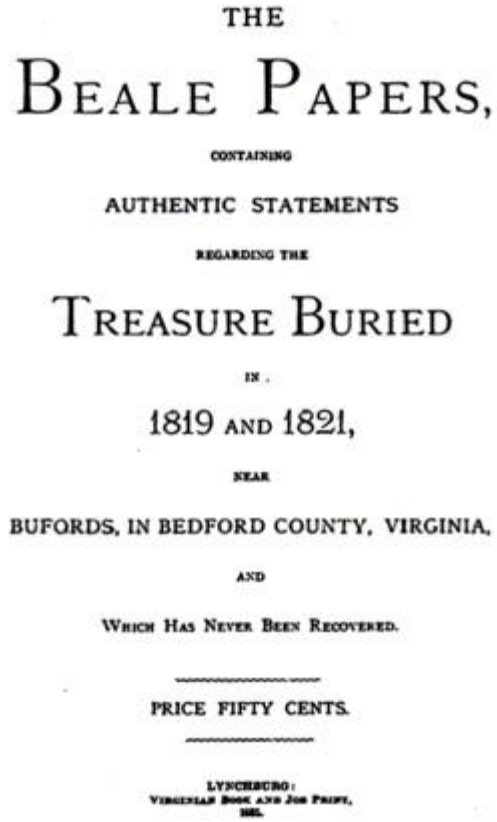
Figura 19. Una parte del texto cifrado que aparece en La aventura de los hombres danzantes, una aventura de Sherlock Holmes escrita por sir Arthur Conan Doyle.

Al otro lado del Atlántico, Edgar Allan Poe también estaba interesándose más y más por el criptoanálisis. Escribiendo para la revista de Filadelfia *Alexander Weekly Messenger*, propuso un desafío a sus lectores, afirmando que podía descifrar cualquier cifra de sustitución monoalfabética. Cientos de lectores enviaron sus textos cifrados y él logró descifrarlos todos ellos con éxito. Aunque esto no requería otra cosa que el análisis de frecuencia, los lectores de Poe estaban muy asombrados por sus logros. Un admirador embelesado lo proclamó «el criptógrafo más profundo y hábil que jamás haya vivido».

En 1843, deseoso de explotar el interés que había generado, Poe escribió un relato sobre las cifras, reconocido ampliamente por los criptógrafos profesionales como el mejor caso de literatura de ficción sobre el tema. El escarabajo de oro cuenta la historia de William Legrande, que descubre un escarabajo poco común, el insecto de oro, y lo recoge utilizando un trozo de papel que había tirado al lado. Esa noche dibuja el escarabajo en el mismo trozo de papel y luego pone el dibujo a la luz para comprobar su exactitud. Sin embargo, su dibujo es borrado por una tinta invisible, que se ha vuelto visible por la proximidad de las llamas. Legrande examina los caracteres que han aparecido y queda convencido de que tiene en sus manos las instrucciones cifradas para encontrar el tesoro del capitán Kidd. El resto de la historia es una demostración clásica del análisis de frecuencia, que resulta en el desciframiento de las pistas del capitán Kidd y el descubrimiento de su tesoro enterrado.

Aunque El escarabajo de oro es pura ficción, hay una historia verdadera del siglo XIX que contiene muchos de los mismos elementos. El caso de las cifras Beale incluye aventuras del salvaje Oeste, un vaquero que amasó una gran fortuna, un

tesoro enterrado valorado en 20 millones de dólares y unos misteriosos papeles cifrados que describen su paradero. Gran parte de lo que se conoce de esta historia, incluidos los papeles cifrados, lo contiene un folleto publicado en 1885. Aunque sólo tiene 23 páginas, el folleto ha desconcertado a generaciones de criptoanalistas y cautivado a cientos de cazadores de tesoros.



THE

BEALE PAPERS,

CONTAINING

AUTHENTIC STATEMENTS

REGARDING THE

TREASURE BURIED

IN

1819 AND 1821,

NEAR

BUFORDS, IN BEDFORD COUNTY, VIRGINIA,

AND

WHICH HAS NEVER BEEN RECOVERED.

PRICE FIFTY CENTS.

LYNCHBURG:

Figura 20. La portada de The Beale Papen («Los papeles de Beale»), el folleto que contenía todo lo que sabemos acerca del misterio del tesoro Beale.

La historia comienza en el hotel Washington de Lynchburg, Virginia, sesenta y cinco años antes de la publicación del folleto. Según éste, el hotel y su dueño, Robert Morriss, gozaban de mucha consideración: «Su carácter amable, estricta probidad, excelente gerencia y su casa tan ordenada pronto lo hicieron famoso como anfitrión, y su reputación se extendió incluso a otros Estados. Su casa era la casa por excelencia en la ciudad, y no había reunión a la moda que se celebrara en otro

lugar». En enero de 1820, un extraño llamado Thomas J. Beale entró a caballo en Lynchburg y se registró en el hotel Washington. «En persona, medía unos seis pies», recordaba Morriss, «tenía los ojos negros como el azabache y el pelo del mismo color, y lo llevaba más largo de como dictaba la moda en aquella época. Su figura era simétrica y daba prueba de una fuerza y una actividad excepcionales; pero su rasgo distintivo era su tez oscura, como si haber estado expuesto tanto al sol lo hubiera bronceado y descolorido completamente; esto, sin embargo, no restaba valor a su apariencia y pensé que era el hombre más guapo que había visto». Aunque Beale pasó el resto del invierno con Morriss y era «extremadamente popular con todos, sobre todo con las damas», nunca habló de su pasado, su familia o el propósito de su visita. Luego, a finales de marzo, se fue tan repentinamente como había llegado.

Dos años después, en enero de 1822, Beale regresó al hotel Washington, «más moreno y oscuro que nunca». Una vez más, pasó el resto del invierno en Lynchburg y desapareció en primavera, pero no sin antes haber confiado a Morriss una caja de hierro cerrada con llave, que, según le dijo, contenía «papeles de mucho valor e importancia». Morriss puso la caja en una caja fuerte y no volvió a pensar en ella y su contenido hasta que recibió una carta de Beale, con fecha del 9 de mayo de 1822 y enviada desde San Luis. Tras varias frases de cortesía y un párrafo sobre el plan de viajar a las llanuras «para cazar búfalos y encontrar osos pardos salvajes», la carta de Beale revelaba la importancia de la caja:

> *Contiene papeles que afectan vitalmente a mi propia fortuna y la de otras personas que tienen negocios conmigo, y en caso de que yo muera, su pérdida podría ser irreparable. Por tanto, comprenderá usted la necesidad de guardarla con vigilancia y cuidados para evitar semejante catástrofe. Si ninguno de nosotros vuelve, por favor guarde la caja con cuidado durante diez años a partir de la fecha de esta carta, y si ni yo, ni alguien con mi autorización, pedimos su devolución durante ese tiempo, ábrala, lo que podrá hacer quitando la cerradura. Encontrará, además de los papeles dirigidos a usted, otros papeles que serán incomprensibles sin la ayuda de una clave. Esa clave la he dejado en manos de un amigo en esta localidad,*

sellada y dirigida a usted, y con instrucciones de que no se entregue hasta junio de 1832. Con ella comprenderá totalmente todo lo que tendrá que hacer.

Morriss continuó guardando la caja como se le había indicado, esperando que Beale la recogería, pero el misterioso hombre de tez morena nunca volvió a Lynchburg. Desapareció sin ninguna explicación y nunca se le volvió a ver. Diez años después, Morriss podría haber seguido las instrucciones de la carta y haber abierto la caja, pero parece ser que se sentía reacio a romper la cerradura. La carta de Beale había mencionado que se enviaría una nota a Morriss en junio de 1832, que supuestamente explicaría cómo descifrar el contenido de la caja. Sin embargo, la nota nunca llegó y quizá Morriss sintió que no merecía la pena abrir la caja si no podía descifrar lo que había dentro de ella. Finalmente, en 1845, la curiosidad de Morriss pudo más que él y forzó la cerradura. La caja contenía tres hojas de caracteres codificados, y una nota escrita por Beale en inglés normal.

La fascinante nota revelaba la verdad sobre Beale, la caja y las claves. Explicaba que en abril de 1817, casi tres años antes de su primer encuentro con Morriss, Beale y otros 29 habían emprendido un viaje por Estados Unidos. Después de viajar por los ricos territorios de caza de las llanuras occidentales llegaron a Santa Fe, y pasaron el invierno en la «pequeña ciudad mexicana». En marzo se dirigieron hacia el norte y comenzaron a seguir la pista de una «inmensa manada de búfalos», matando todos los que podían por el camino. Luego, según Beale, les sonrió la buena suerte:

Un día, mientras los seguíamos, el grupo acampó en un pequeño barranco, a unas 250 o 300 millas al norte de Santa Fe, y, con los caballos atados, se estaban preparando la cena, cuando uno de los hombres descubrió en una grieta de las rocas algo que parecía oro. Al enseñarlo a los demás, se declaró que era oro, y el entusiasmo fue la consecuencia natural.

La carta continuaba explicando que Beale y sus hombres, con la ayuda de la tribu local, minaron el lugar durante los dieciocho meses siguientes, para cuando ya

habían acumulado una gran cantidad de oro, además de algo de plata que se encontró cerca de allí. A su debido tiempo acordaron que su recién encontrada riqueza debía ser trasladada a un lugar seguro y decidieron llevarla de vuelta a casa, a Virginia, donde la ocultarían en un emplazamiento secreto. En 1820, Beale viajó a Lynchburg con el oro y la plata, encontró una ubicación apropiada y lo enterró. Fue en aquella ocasión cuando se hospedó por vez primera en el hotel Washington y conoció a Morriss. Cuando Beale se fue al finalizar el invierno se reunió de nuevo con sus hombres, que habían continuado trabajando en la mina durante su ausencia.

Después de otros dieciocho meses, Beale volvió a visitar Lynchburg con todavía más para añadir a su colección oculta. Esta vez tenía una razón adicional para su viaje:

> *Antes de dejar a mis compañeros en las llanuras se sugirió que, en caso de que sufriésemos algún accidente, el tesoro escondido se perdería, no pudiendo llegar a nuestros familiares a no ser que se tomasen precauciones contra tal eventualidad. Por consiguiente, me pidieron que eligiera alguna persona completamente de fiar, si es que se podía encontrar alguna, a la que debería confiarse, si el grupo lo consideraba aceptable, que llevase a cabo los deseos de sus integrantes en relación con sus partes respectivas de lo encontrado.*

Beale creía que Morriss era un hombre íntegro, por lo que le confió la caja que contenía las tres hojas codificadas, las denominadas cifras Beale. Cada hoja codificada contenía una selección de números (reproducidos aquí en las Figuras 21, 22 y 23) y el desciframiento de los números revelaría todos los detalles relevantes. La primera hoja describía la ubicación del tesoro, la segunda esbozaba su contenido y la tercera enumeraba los familiares de los hombres que debían recibir una parte del tesoro. Cuando Morriss leyó todo esto, habían pasado unos veintitrés años desde que había visto a Thomas Beale por última vez. Dando por sentado que Beale y sus hombres habían muerto, Morriss se sintió obligado a encontrar el oro y distribuirlo entre los familiares señalados. Sin embargo, sin la clave prometida estaba forzado a descifrar las cifras partiendo de cero, una tarea que le preocupó

durante los siguientes veinte años y que terminó en fracaso.


71, 194, 38, 1701, 89, 76, 11, 83, 1629, 48, 94, 63, 132, 16, 111, 95, 84, 341, 975,
14, 40, 64, 27, 81, 139, 213, 63, 90, 1120, 8, 15, 3, 126, 2018, 40, 74, 758, 485,
604, 230, 436, 664, 582, 150, 251, 284, 308, 231, 124, 211, 486, 225, 401, 370,
11, 101, 305, 139, 189, 17, 33, 88, 208, 193, 145, 1, 94, 73, 416, 918, 263, 28, 500,
538, 356, 117, 136, 219, 27, 176, 130, 10, 460, 25, 485, 18, 436, 65, 84, 200, 283,
118, 320, 138, 36, 416, 280, 15, 71, 224, 961, 44, 16, 401, 39, 88, 61, 304, 12, 21,
24, 283, 134, 92, 63, 246, 486, 682, 7, 219, 184, 360, 780, 18, 64, 463, 474, 131,
160, 79, 73, 440, 95, 18, 64, 581, 34, 69, 128, 367, 460, 17, 81, 12, 103, 820, 62,
116, 97, 103, 862, 70, 60, 1317, 471, 540, 208, 121, 890, 346, 36, 150, 59, 568,
614, 13, 120, 63, 219, 812, 2160, 1780, 99, 35, 18, 21, 136, 872, 15, 28, 170, 88, 4,
30, 44, 112, 18, 147, 436, 195, 320, 37, 122, 113, 6, 140, 8, 120, 305, 42, 58, 461,
44, 106, 301, 13, 408, 680, 93, 86, 116, 530, 82, 568, 9, 102, 38, 416, 89, 71, 216,
728, 965, 818, 2, 38, 121, 195, 14, 326, 148, 234, 18, 55, 131, 234, 361, 824, 5,
81, 623, 48, 961, 19, 26, 33, 10, 1101, 365, 92, 88, 181, 275, 346, 201, 206, 86,
36, 219, 324, 829, 840, 64, 326, 19, 48, 122, 85, 216, 284, 919, 861, 326, 985,
233, 64, 68, 232, 431, 960, 50, 29, 81, 216, 321, 603, 14, 612, 81, 360, 36, 51, 62,
194, 78, 60, 200, 314, 676, 112, 4, 28, 18, 61, 136, 247, 819, 921, 1060, 464, 895,
10, 6, 66, 119, 38, 41, 49, 602, 423, 962, 302, 294, 875, 78, 14, 23, 111, 109, 62,
31, 501, 823, 216, 280, 34, 24, 150, 1000, 162, 286, 19, 21, 17, 340, 19, 242, 31,
86, 234, 140, 607, 115, 33, 191, 67, 104, 86, 52, 88, 16, 80, 121, 67, 95, 122, 216,
548, 96, 11 , 201, 77, 364, 218, 65, 667, 890, 236, 154, 211, 10, 98, 34, 119, 56,
216, 119, 71, 218, 1164, 1496, 1817, 51, 39, 210, 36, 3, 19, 540, 232, 22, 141, 617,
84, 290, 80, 46, 207, 411, 150, 29, 38, 46, 172, 85, 194, 39, 261, 543, 897, 624, 18,
212, 416, 127, 931, 19, 4, 63, 96, 12, 101, 418, 16, 140, 230, 460, 538, 19, 27, 88,
612, 1431, 90, 716, 275, 74, 83, 11, 426, 89, 72, 84, 1300, 1706, 814, 221, 132,
40, 102, 34, 868, 975, 1101, 84, 16, 79, 23, 16, 81, 122, 324, 403, 912, 227, 936,
447, 55, 86, 34, 43, 212, 107, 96, 314, 264, 1065, 323, 428, 601, 203, 124, 95, 216,
814, 2906, 654, 820, 2, 301, 112, 176, 213, 71, 87, 96, 202, 35, 10, 2, 41, 17, 84,
221, 736, 820, 214, 11, 60, 760.

Figura 21. La primera cifra Beale

115, 73, 24, 807, 37, 52, 49, 17, 31, 62, 647, 22, 7, 15, 140, 47, 29, 107, 79, 84, 56,
239, 10, 26, 811, 5, 196, 308, 85, 52, 160, 136, 59, 211, 36, 9, 46, 316, 554, 122,
106, 95, 53, 58, 2, 42, 7, 35, 122, 53, 31, 82, 77, 250, 196, 56, 96, 118, 71, 140,
287, 28, 353, 37, 1005, 65, 147, 807, 24, 3, 8, 12, 47, 43, 59, 807, 45, 316, 101, 41,
78, 154, 1005, 122, 138, 191, 16, 77, 49, 102, 57, 72, 34, 73, 85, 35, 371, 59, 196,
81, 92, 191, 106, 273, 60, 394, 620, 270, 220, 106, 388, 287, 63, 3, 6, 191, 122, 43,
234, 400, 106, 290, 314, 47, 48, 81, 96, 26, 115, 92, 158, 191, 110, 77, 85, 197, 46,
10, 113, 140, 353, 48, 120, 106, 2, 607, 61, 420, 811, 29, 125, 14, 20, 37, 105, 28,
248, 16, 159, 7, 35, 19, 301, 125, 110, 486, 287, 98, 117, 511, 62, 51, 220, 37, 113,
140, 807, 138, 540, 8, 44, 287, 388, 117, 18, 79, 344, 34, 20, 59, 511, 548, 107,
603, 220, 7, 66, 154, 41, 20, 50, 6, 575, 122, 154, 248, 110, 61, 52, 33, 30, 5, 38, 8,
14, 84, 57, 540, 217, 115, 71, 29, 84, 63, 43, 131, 29, 138, 47, 73, 239, 540, 52, 53,
79, 118, 51, 44, 63, 196, 12, 239, 112, 3, 49, 79, 353, 105, 56, 371, 557, 211, 515,
125, 360, 133, 143, 101, 15, 284, 540, 252, 14, 205, 140, 344, 26, 811, 138, 115,
48, 73, 34, 205, 316, 607, 63, 220, 7, 52, 150, 44, 52, 16, 40, 37, 158, 807, 37, 121,
12, 95, 10, 15, 35, 12, 131, 62, 115, 102, 807, 49, 53, 135, 138, 30, 31, 62, 67, 41,
85, 63, 10, 106, 807, 138, 8, 113, 20, 32, 33, 37, 353, 287, 140, 47, 85, 50, 37, 49,
47, 64, 6, 7, 71, 33, 4, 43, 47, 63, 1, 27, 600, 208, 230, 15, 191, 246, 85, 94, 511, 2,
270, 20, 39, 7, 33, 44, 22, 40, 7, 10, 3, 811, 106, 44, 486, 230, 353, 211, 200, 31,
10, 38, 140, 297, 61, 603, 320, 302, 666, 287, 2, 44, 33, 32, 511, 548, 10, 6, 250,
557, 246, 53, 37, 52, 83, 47, 320, 38, 33, 807, 7, 44, 30, 31, 250, 10, 15, 35, 106,
160, 113, 31, 102, 406, 230, 540, 320, 29, 66, 33, 101, 807, 138, 301, 316, 353,
320, 220, 37, 52, 28, 540, 320, 33, 8, 48, 107, 50, 811, 7, 2, 113, 73, 16, 125, 11,
110, 67, 102, 807, 33, 59, 81, 158, 38, 43, 581, 138, 19, 85, 400, 38, 43, 77, 14, 27,
8, 47, 138, 63, 140, 44, 35, 22, 177, 106, 250, 314, 217, 2, 10, 7, 1005, 4, 20, 25,
44, 48, 7, 26, 46, 110, 230, 807, 191, 34, 112, 147, 44, 110, 121, 125, 96, 41, 51,
50, 140, 56, 47, 152, 540, 63, 807, 28, 42, 250, 138, 582, 98, 643, 32, 107, 140,
112, 26, 85, 138, 540, 53, 20, 125, 371, 38, 36, 10, 52, 118, 136, 102, 420, 150,
112, 71, 14, 20, 7, 24, 18, 12, 807, 37, 67, 110, 62, 33, 21, 95, 220, 511, 102, 811,
30, 83, 84, 305, 620, 15, 2, 108, 220, 106, 353, 105, 106, 60, 275, 72, 8, 50, 205,
185, 112, 125, 540, 65, 106, 807, 188, 96, 110, 16, 73, 33, 807, 150, 409, 400, 50,
154, 285, 96, 106, 316, 270, 205, 101, 811, 400, 8, 44, 37, 52, 40, 241, 34, 205,
38, 16, 46, 47, 85, 24, 44, 15, 64, 73, 138, 807, 85, 78, 110, 33, 420, 505, 53, 37,
38, 22, 31, 10, 110, 106, 101, 140, 15, 38, 3, 5, 44, 7, 98, 287, 135, 150, 96, 33, 84
125, 807, 191, 96, 511, 118, 440, 370, 643, 466, 106, 41, 107, 603, 220, 275, 30,
150, 105, 49, 53, 287, 250, 208, 134, 7, 53, 12, 47, 85, 63, 138, 110, 21, 112, 140,
485, 486, 505, 14, 73, 84, 575, 1005, 150, 200, 16, 42, 5, 4, 25, 42, 8, 16, 811,
125, 160, 32, 205, 603, 807, 81, 96, 405, 41, 600, 136, 14, 20, 28, 26, 353, 302,
246, 8, 131, 160, 140, 84, 440, 42, 16, 811, 40, 67, 101, 102, 194, 138, 205, 51,
63, 241, 540, 122, 8, 10, 63, 140, 47, 48, 140, 288.

Figura 22. La segunda cifra Beale

317, 8, 92, 73, 112, 89, 67, 318, 28, 96, 107, 41, 631, 78, 146, 397, 118, 98, 114,
246, 348, 116, 74, 88, 12, 65, 32, 14, 81, 19, 76, 121, 216, 85, 33, 66, 15, 108, 68,
77, 43, 24, 122, 96, 117, 36, 211, 301, 15, 44, 11, 46, 89, 18, 136, 68, 317, 28, 90,
82, 304, 71, 43, 221, 198, 176, 310, 319, 81, 99, 264, 380, 56, 37, 319, 2, 44, 53,
28, 44, 75, 98, 102, 37, 85, 107, 117, 64, 88, 136, 48, 154, 99, 175, 89, 315, 326,
78, 96, 214, 218, 311, 43, 89, 51, 90, 75, 128, 96, 33, 28, 103, 84, 65, 26, 41, 246,
84, 270, 98, 116, 32, 59, 74, 66, 69, 240, 15, 8, 121, 20, 77, 89, 31, 11, 106, 81,
191, 224, 328, 18, 75, 52, 82, 117, 201, 39, 23, 217, 27, 21, 84, 35, 54, 109, 128,
49, 77, 88, 1, 81, 217, 64, 55, 83, 116, 251, 269, 311, 96, 54, 32, 120, 18, 132, 102,
219, 211, 84, 150, 219, 275, 312, 64, 10, 106, 87, 75, 47, 21, 29, 37, 81, 44, 18,
126, 115, 132, 160, 181, 203, 76, 81, 299, 314, 337, 351, 96, 11, 28, 97, 318, 238,
106, 24, 93, 3, 19, 17, 26, 60, 73, 88, 14, 126, 138, 234, 286, 297, 321, 365, 264,
19, 22, 84, 56, 107, 98, 123, 111, 214, 136, 7, 33, 45, 40, 13, 28, 46, 42, 107, 196,
227, 344, 198, 203, 247, 116, 19, 8, 212, 230, 31, 6, 328, 65, 48, 52, 59, 41, 122,
33, 117, 11, 18, 25, 71, 36, 45, 83, 76, 89, 92, 31, 65, 70, 83, 96, 27, 33, 44, 50, 61,
24, 112, 136, 149, 176, 180, 194, 143, 171, 205, 296, 87, 12, 44, 51, 89, 98, 34, 41,
208, 173, 66, 9, 35, 16, 95, 8, 113, 175, 90, 56, 203, 19, 177, 183, 206, 157, 200,
218, 260, 291, 305, 618, 951, 320, 18, 124, 78, 65, 19, 32, 124, 48, 53, 57, 84, 96,
207, 244, 66, 82, 119, 71, 11, 86, 77, 213, 54, 82, 316, 245, 303, 86, 97, 106, 212,
18, 37, 15, 81, 89, 16, 7, 81, 39, 96, 14, 43, 216, 118, 29, 55, 109, 136, 172, 213,
64, 8, 227, 304, 611, 221, 364, 819, 375, 128, 296, 1, 18, 53, 76, 10, 15, 23, 19, 71,
84, 120, 134, 66, 73, 89, 96, 230, 48, 77, 26, 101, 127, 936, 218, 439, 178, 171, 61,
226, 313, 215, 102, 18, 167, 262, 114, 218, 66, 59, 48, 27, 19, 13, 82, 48, 162, 119,
34, 127, 139, 34, 128, 129, 74, 63, 120, 11, 54, 61, 73, 92, 180, 66, 75, 101, 124,
265, 89, 96, 126, 274, 896, 917, 434, 461, 235, 890, 312, 413, 328, 381, 96, 105,
217, 66, 118, 22, 77, 64, 42, 12, 7, 55, 24, 83, 67, 97, 109, 121, 135, 181, 203, 219,
228, 256, 21, 34, 77, 319, 374, 382, 675, 684, 717, 864, 203, 4, 18, 92, 16, 63, 82,
22, 46, 55, 69, 74, 112, 134, 186, 175, 119, 213, 416, 312, 343, 264, 119, 186, 218,
343, 417, 845, 951, 124, 209, 49, 617, 856, 924, 936, 72, 19, 28, 11, 35, 42, 40, 66,
85, 94, 112, 65, 82, 115, 119, 236, 244, 186, 172, 112, 85, 6, 56, 38, 44, 85, 72,
32, 47, 73, 96, 124, 217, 314, 319, 221, 644, 817, 821, 934, 922, 416, 975, 10, 22,
18, 46, 137, 181, 101, 39, 86, 103, 116, 138, 164, 212, 218, 296, 815, 380, 412,
460, 495, 675, 820, 952.

Figura 23. La tercera cifra Beale

En 1862, a la edad de ochenta y cuatro años, Morriss sabía que se aproximaba el fin de su vida y que tenía que compartir el secreto de las cifras Beale, de otra forma cualquier esperanza de cumplir los deseos de Beale moriría con él. Morriss se confió a un amigo, pero por desgracia la identidad de esa persona sigue siendo un misterio. Lo único que sabemos sobre el amigo de Beale es que fue él quien escribió el folleto en 1885, así que en adelante nos referiremos a él simplemente como el *autor.* El autor explicaba las razones de su anonimato en el folleto:

> *Preveo que estos papeles tendrán una gran difusión y, para evitar la multitud de cartas con las que me asaltarían desde todos los rincones de la Unión, planteando todo tipo de preguntas, y exigiendo respuestas que, si tratara de responder, absorberían todo mi tiempo y alterarían la naturaleza de mi trabajo, he decidido retirar mi nombre de la publicación, tras asegurar a todos los*

> *interesados que he ofrecido todo lo que sé sobre este asunto, y que no puedo añadir ni una sola palabra a las declaraciones aquí contenidas.*

Para proteger su identidad, el autor pidió a James B. Ward, un respetado miembro de la comunidad local y el topógrafo de las carreteras del condado, que actuase como su agente y editor.

Todo lo que se sabe de la extraña historia de las cifras Beale está publicado en el folleto, de forma que es gracias al autor que tenemos las cifras y el relato de Morriss de la historia. Además, el autor es también el responsable del desciframiento certero de la segunda cifra Beale. Como la primera y la tercera cifras, la segunda consta de una página de números, y el autor asumió que cada número representaba una letra. Sin embargo, la gama de números sobrepasa con mucho el número de letras del alfabeto, de manera que el autor se dio cuenta de que se enfrentaba a una cifra que utiliza varios números para representar la misma letra. Una cifra que satisface este criterio es la denominada *cifra libro*, en la que un libro, o cualquier otra pieza de texto, es en sí mismo la clave.

Primero, el criptógrafo numera consecutivamente cada palabra del texto-clave. Después de eso, cada número actúa como sustituto de la letra inicial de su palabra asociada, [1]Por [2]ejemplo, [3]si [4]el [5]emisor [6]y [7]el [8]receptor [9]acordaron [10]que [11]esta [12]frase [13]sería [14]el [15]texto-clave, [16]cada [17]palabra [18]tendría [19]una [20]etiqueta [21]numérica, [22]y [23]cada [24]número [25]proporcionaría [26]la [27]base [28]para [29]la [30]codificación. A continuación se haría una lista uniendo cada número a la letra inicial de su palabra asociada:

1 = p	11 = e	21 = n
2 = e	12 = f	22 = y
3 = s	13 = s	23 = c
4 = e	14 = e	24 = n
5 = e	15 = t	25 = p
6 = y	16 = c	26 = l
7 = e	17 = p	27 = b
8 = r	18 = t	28 = p
9 = a	19 = u	29 = l
10 = q	20 = e	30 = c

Ahora podemos codificar un mensaje sustituyendo las letras del texto llano por números según la lista. En esta lista, la letra p del texto llano se podría sustituir por 1, 17, 25 o 28; la letra e del texto llano se podría sustituir por 2, 4, 5, 7, 11, 14 o 20; y así sucesivamente. Como nuestro texto-clave es una frase tan corta, no tenemos números que reemplazarían a letras infrecuentes como la x y la z, pero tenemos suficientes sustitutos para codificar la palabra Beale, que podría ser 27-2-9-29-4. Si el receptor a quien va dirigido tiene una copia del texto-clave, entonces descifrar el mensaje codificado resulta insignificante. Sin embargo, si una tercera persona intercepta sólo el texto cifrado, el criptoanálisis depende de poder identificar de alguna manera el texto-clave. El autor del folleto escribió:

> *«Con esta idea, se hizo una prueba con todo libro que pude conseguir, numerando sus letras y comparando los números con los del manuscrito; todo ello fue en vano, sin embargo, hasta que la Declaración de la Independencia proporcionó la pista para uno de los papeles, y reavivó todas mis esperanzas».*

La Declaración de la Independencia norteamericana resultó ser el texto-clave para la segunda cifra Beale, y numerando las palabras de la Declaración es posible desenmarañarla. La Figura 24 muestra el comienzo de la Declaración de la Independencia, numerando cada décima palabra para ayudar a que el lector vea cómo funciona el desciframiento. La Figura 22 muestra el texto cifrado: el primer

número es 115, y la 115ª palabra de la Declaración es «*instituted*», de manera que el primer número representa a la i. El segundo número del texto cifrado es 73, y la 73ª palabra de la declaración es «*hold*», de manera que el segundo número representa a la h. Aquí está el desciframiento entero, tal como aparecía publicado en el folleto[7].

> *He depositado en el condado de Bedford, a unas cuatro millas de Buford's, en una excavación o cámara subterránea, seis pies bajo la superficie del terreno, los siguientes artículos, que pertenecen conjuntamente a las personas cuyos nombres aparecen en el papel número «3», adjunto:*
>
> *El primer depósito consistió en mil catorce libras de oro, y tres mil ochocientas doce libras de plata, depositadas en noviembre de 1819. El segundo se realizó en diciembre de 1821, y consistía en mil novecientas siete libras de oro, y mil doscientas ochenta y ocho libras de plata; también joyas, obtenidas en San Luis a cambio de plata para facilitar el transporte, y valoradas en 13.000 dólares.*
>
> *Todo lo mencionado está embalado de manera segura en ollas de hierro, con tapas de hierro. La excavación está más o menos bordeada de piedras, y las vasijas descansan sobre roca sólida, y están cubiertas con otras. El papel número «1» describe la ubicación exacta de la excavación, para que no haya ninguna dificultad para encontrarla.*

Merece la pena destacar que hay algunos errores en el desciframiento. Por ejemplo, el desciframiento incluye las palabras *«four miles»* (cuatro millas), basándose en que la 95ª palabra de la Declaración de la Independencia comienza con la letra u. Sin embargo, la palabra 95ª es «inalienable». Esto podría ser el resultado de la codificación descuidada de Beale, o podría ser que Beale tenía una copia de la Declaración en la que la 95ª palabra era «unalienable», lo que sí aparece en algunas versiones que datan del principio del siglo XIX. En cualquier caso, el desciframiento

[7] Por supuesto, el texto descifrado está escrito en inglés, por lo que los dos ejemplos de letras descifradas remiten a ese idioma. En efecto, las dos primeras letras del texto son la i y la h, ya que éste comienza: «I have…». Si el lector realiza el desciframiento por sí mismo obtendrá el texto llano original (en inglés). (N. del T.)

certero indica claramente el valor del tesoro, al menos 20 millones de dólares según los precios de los lingotes de hoy día.

When, in the course of human events, it becomes [10]necessary for one people to dissolve the political bands which [20]have connected them with another, and to assume among the [30]powers of the earth, the separate and equal station to [40]which the laws of nature and of nature's God entitle [50]them, a decent respect to the opinions of mankind requires [60]that they should declare the causes which impel them to [70]the separation.

We hold these truths to be self-evident, [80]that all men are created equal, that they are endowed [90]by their Creator with certain inalienable rights, that among these [100]are life, liberty and the pursuit of happiness; That to [110]secure these rights, governments are instituted among men, deriving their [120]just powers from the consent of the governed; That whenever [130]any form of government becomes destructive of these ends, it [140]is the right of the people to alter or to [150]abolish it, and to institute a new government, laying its [160]foundation on such principles and organizing its powers in such [170]form, as to them shall seem most likely to effect [180]their safety and happiness. Prudence, indeed, will dictate that governments [190]long established should not be changed for light and transient [200]causes; and accordingly all experience hath shewn, that mankind are [210]more disposed to suffer, while evils are sufferable, than to [220]right themselves by abolishing the forms to which they are [230]accustomed.

But when a long train of abuses and usurpations, [240]pursuing invariably the same object evinces a design to reduce them [250]under absolute despotism, it is their right, it is their [260]duty, to throw off such government, and to provide new [270]Guards for their future security. Such has been the patient [280]sufferance of these Colonies; and such is now the necessity [290]which constrains them to alter their former systems of government. [300]The history of the present King of Great Britain is [310]a history of repeated injuries and usurpations, all having in [320]direct object the establishment of an absolute tyranny over these [330]States. To prove this, let facts be submitted to a [340]candid world.

Figura 24. Los primeros tres párrafos de la Declaración de la Independencia, con cada décima palabra numerada. Ésta es la clave para descifrar la segunda cifra Bcale.

No es de extrañar que, una vez que el autor conoció el valor del tesoro, dedicase más y más tiempo a analizar las otras dos hojas de cifras, sobre todo la primera

cifra Beale, que describe la ubicación del tesoro. A pesar de sus esfuerzos extenuantes, fracasó, y lo único que obtuvo de las cifras fue pesares:

> *Como consecuencia del tiempo perdido en la mencionada investigación, me he visto reducido de una relativa riqueza a la más absoluta miseria, acarreando sufrimiento a quienes era mi deber proteger, y esto, también, a pesar de sus amonestaciones. Mis ojos se abrieron por fin a su situación y decidí romper de inmediato, y para siempre,*
>
> *toda la conexión con el asunto, y reparar, en lo posible, mis errores. Para hacerlo, como mejor medio para evitar exponerme a la tentación, he decidido hacer público todo el asunto, y pasar la responsabilidad que recae sobre mis hombros al Sr. Morriss.*

De esta manera, las cifras, y todo lo demás que sabía el autor, fueron publicadas en 1885. Aunque un incendio en un almacén destruyó la mayoría de los folletos, los que sobrevivieron causaron gran revuelo en Lynchburg. Entre los más ardientes cazadores de tesoros atraídos por las cifras Beale estaban los hermanos Hart, George y Clayton. Se pasaron años estudiando las dos cifras que quedaban, intentando diversas formas de ataque criptoanalítico, y a veces engañándose a sí mismos creyendo que tenían una solución. Una falsa línea de ataque a veces genera unas pocas palabras tentadoras en medio de un mar de galimatías, lo que anima al criptoanalista a inventar una serie de disculpas para justificar el galimatías. Para un observador imparcial, el desciframiento obviamente no es más que una ilusión, pero para el cegado cazador de tesoros tiene absoluto sentido. Uno de los desciframientos tentativos de los Hart los animó a usar dinamita para excavar un lugar determinado; por desgracia, el cráter resultante no produjo oro. Aunque Clayton Hart desistió en 1912, George continuó ocupándose de las cifras Beale hasta 1952. Un fanático de esas cifras aún más persistente ha sido Hiram Herbert, hijo, que se interesó en ellas en 1923, y cuya obsesión continuó hasta la década de los setenta. Tampoco a él le ha reportado su trabajo ningún beneficio.

Varios criptoanalistas profesionales se han lanzado también a seguir la pista al tesoro Beale. Herbert O. Yardley, que fundó el U. S. Cipher Bureau (Oficina de

Cifras de Estados Unidos) —conocida como la Cámara Negra Americana— al final de la primera guerra mundial, se sintió intrigado por las cifras Beale, así como el coronel William Friedman, la figura dominante del criptoanálisis norteamericano durante la primera mitad del siglo XX. Mientras era el responsable del Signal Intelligence Service (Servicio de Inteligencia de Señales) convirtió a las cifras Beale en parte del programa de adiestramiento, presumiblemente porque, como dijo una vez su esposa, creía que las cifras poseían un «ingenio infernal, diseñado específicamente para seducir al lector incauto». El archivo Friedman, establecido tras su muerte en 1969 en el Centro de Investigación George C.

Marshall, es frecuentemente consultado por los historiadores militares, pero la gran mayoría de los visitantes son ansiosos adeptos de Beale, que confían seguir algunas de las pistas del gran hombre. Más recientemente, una de las mayores figuras a la caza del tesoro Beale ha sido Carl Hammer, el director retirado de un servicio de ordenadores de Sperry Univac y uno de los pioneros del criptoanálisis por ordenador. Según Hammer, «las cifras Beale han ocupado al menos al 10 por 100 de las mejores mentes criptoanalíticas del país. Y ni un céntimo de este esfuerzo debería ser escatimado. El trabajo —incluso las líneas que han conducido a callejones sin salida— ha compensado con creces haciendo avanzar y perfeccionando la investigación de los ordenadores». Hammer ha sido un miembro destacado de la Asociación de la Cifra y el Tesoro Beale, fundada en los años sesenta para fomentar el interés en el misterio Beale. Inicialmente, la Asociación requería que cualquier miembro que descubriese el tesoro lo compartiera con los demás miembros, pero esta obligación parecía disuadir de afiliarse a muchos buscadores del tesoro, de forma que la Asociación no tardó en abandonar esa condición.

A pesar de los esfuerzos combinados de la Asociación, los cazadores de tesoros aficionados y los criptoanalistas profesionales, la primera y la tercera cifras Beale han seguido siendo un misterio durante más de un siglo y el oro, la plata y las joyas aún no han sido encontrados. Muchos intentos de desciframiento han girado en torno a la Declaración de la Independencia, que fue la clave para la segunda cifra Beale. Aunque una numeración directa de las palabras de la Declaración no ofrece nada de provecho para las cifras primera y tercera, los criptoanalistas han probado

varias otras combinaciones, como numerar al revés, o numerar las palabras alternas, pero hasta ahora nada ha dado resultado. Un problema que se presenta es que la primera cifra contiene números tan altos como 2906, mientras que la Declaración sólo contiene 1322 palabras. Se han considerado otros textos y libros como claves potenciales y muchos criptoanalistas han contemplado la posibilidad de un sistema de codificación completamente diferente.

Puede que sorprenda la solidez de las cifras Beale aún no descifradas, especialmente si se tiene en cuenta que cuando dejamos la batalla continúa entre los codificadores y los descifradores, éstos llevaban la delantera. Babbage y Kasiski habían inventado una manera de descifrar la cifra Vegenère, y los codificadores se esforzaban por encontrar algo que la reemplazara. ¿Cómo pudo Beale crear algo tan formidable? La respuesta es que las cifras Beale fueron creadas en circunstancias que daban una gran ventaja al criptógrafo. Los mensajes eran algo único, y como se relacionaban con un tesoro tan valioso, puede que Beale estuviera dispuesto a crear un texto-clave especial y único para las cifras primera y tercera. Efectivamente, si el texto-clave estuviera escrito por el propio Beale, esto explicaría por qué las búsquedas de material publicado no lo han revelado. Podemos imaginar que Beale habría escrito un ensayo privado de 2000 palabras sobre el tema de la caza de búfalos, del que sólo habría una copia. Sólo el poseedor de este ensayo, el texto-clave único, sería capaz de descifrar las cifras primera y tercera. Beale mencionó que había dejado la clave «en manos de un amigo» en San Luis, pero si el amigo perdió o destruyó la clave, puede que los criptoanalistas nunca sean capaces de descifrar las cifras Beale.

Crear un texto-clave único para un mensaje es mucho más seguro que utilizar una clave basada en un libro publicado, pero sólo resulta práctico si el emisor dispone de tiempo para crear el texto-clave y es capaz de transmitirlo al receptor a quien va dirigido el mensaje, requisitos éstos que no resultan factibles para las comunicaciones rutinarias, cotidianas. En el caso de Beale, él pudo componer su texto en sus ratos de ocio, entregarlo a su amigo en San Luis cuando pasaba por allí y luego hacer que fuera enviado o recogido en alguna fecha arbitraria en el futuro, cuando el tesoro debía ser recuperado.

Una teoría alternativa para explicar la indescifrabilidad de las cifras Beale es que el

autor del folleto las saboteó deliberadamente antes de publicarlas. Quizá el autor simplemente quería hacer que apareciera la clave, que estaba aparentemente en manos del amigo de Beale en San Luis. Si hubiera publicado las cifras con exactitud, el amigo habría podido descifrarlas y recoger el oro, y el autor no habría visto recompensados sus esfuerzos. Sin embargo, si las cifras aparecían viciadas de alguna forma, el amigo se daría cuenta al fin de que necesitaba la ayuda del autor y se pondría en contacto con el editor, Ward, que a su vez contactaría con el autor. Entonces, el autor podría entregar las cifras exactas a cambio de una parte del tesoro.

También es posible que el tesoro haya sido encontrado hace muchos años, y que el descubridor se esfumó sin ser visto por los residentes locales. Los entusiastas de Beale con predilección por las teorías conspiratorias han sugerido que la NSA ya ha encontrado el tesoro. La oficina de claves del gobierno central norteamericano tiene acceso a los ordenadores más potentes y a algunas de las mentes más brillantes del mundo y puede que haya descubierto algo sobre las cifras que se le ha escapado a todos los demás. La ausencia de cualquier anuncio estaría en consonancia con la reputación secretista de la NSA: se ha sugerido que las siglas NSA no significan National Security Agency, sino más bien «Never Say Anything» («Nunca Digas Nada») o «No Such Agency» («No Hay Tal Agencia»),

Finalmente, no podemos excluir la posibilidad de que las cifras Beale sean un elaborado engaño y que Beale nunca existió. Los escépticos han sugerido que el desconocido autor, inspirado en *El escarabajo de oro* de Poe, inventó toda la historia y publicó el folleto para aprovecharse de la avaricia de los demás. Los partidarios de la teoría del engaño han buscado inconsistencias y fallos en la historia de Beale. Por ejemplo, según el folleto, la carta de Beale, que estaba encerrada en la caja de hierro y escrita supuestamente en 1822, contiene la palabra «estampida», pero esta palabra no se vio en ningún texto publicado hasta 1834. Sin embargo, es bastante posible que la palabra fuera de uso común en el salvaje Oeste muchísimo antes y Beale podría haberla aprendido en sus viajes.

Uno de los principales incrédulos es el criptógrafo Louis Kruh, que afirma haber encontrado pruebas de que el autor del folleto escribió también las cartas de Beale, la que fue supuestamente enviada desde San Luis y la que supuestamente estaba

en la caja. Kruh realizó un análisis textual de las palabras atribuidas al autor y las atribuidas a Beale para ver si presentaban características similares. Comparó aspectos tales como el porcentaje de frases que comienzan con «El», «Si» e «Y», el promedio de comas y puntos y comas por frase, y el estilo de escribir: el uso de negativos, pasivas negativas, infinitivos, frases compuestas, etcétera. Además de las palabras del autor y las cartas de Beale, el análisis incluyó también escritos de otros tres virginianos del siglo XIX. De los cinco casos de escritura, el de Beale y el del autor del folleto mostraron el parecido más cercano, sugiriendo que podrían haber sido escritos por la misma persona. En otras palabras, esto sugiere que el autor falsificó las cartas atribuidas a Beale e inventó toda la historia.

Por otra parte, varias fuentes proporcionan pruebas de la integridad de las cifras Beale. Primero, si las cifras no descifradas fueran engaños, se esperaría que el falsificador habría elegido los números con poca o ninguna atención. Sin embargo, los números dan lugar a varios patrones intricados. Uno de los patrones se puede encontrar utilizando la Declaración de la Independencia como clave para la primera cifra. Esto no produce palabras perceptibles, pero sí da lugar a secuencias como

ahfdefghiij klmmnolipp

Aunque no es una lista alfabética perfecta, ciertamente tampoco es una lista al azar. James Gillogly, presidente de la American Cryptogram Association, estimó que las posibilidades de que ésta y otras secuencias aparezcan por casualidad son de menos de una entre cien billones, dando a entender que hay un principio criptográfico subyacente en la primera cifra. Una teoría es que la Declaración es efectivamente la clave, pero el texto resultante requiere una segunda fase de desciframiento; en otras palabras, la primera cifra Beale fue codificada mediante un proceso de dos etapas, lo que se denomina supercodificación. Si esto es así, la secuencia alfabética podría haberse puesto ahí como señal de aliento, como pista de que la primera etapa de desciframiento se había completado con éxito.

Evidencia adicional a favor de la probidad de las cifras la ofrece la investigación histórica, que se puede utilizar para verificar las historias de Thomas Beale. Peter Viemeister, un historiador local, ha reunido gran parte de la investigación en su libro *El tesoro Beale —Historia de un misterio.* Viemeister comenzó preguntando si había pruebas de que Thomas Beale existió realmente. Usando el censo de 1790 y otros

documentos, Viemeister ha identificado varios Thomas Beale que nacieron en Virginia y cuyos orígenes encajan con los pocos detalles conocidos. Viemeister ha tratado también de corroborar los otros detalles del folleto, como el viaje de Beale a Santa Fe y su descubrimiento del oro. Por ejemplo, hay una leyenda cheyenne que se remonta hacia 1820 que trata de oro y plata que se tomaron del Oeste para ser enterrados en las montañas del Este. También, la lista de correos de San Luis de 1820 contiene a un «Thomas Beall», lo que encaja con lo que afirma el folleto respecto a que Beale pasó por la ciudad en 1820 en su viaje hacia el Oeste tras dejar Lynchburg. El folleto también dice que Beale envió una carta desde San Luis en 1822.

Así que la historia de las cifras Beale parece tener base y, por consiguiente, continúa cautivando a criptoanalistas y cazadores de tesoros, como Joseph Jancik, Marilyn Parsons y su perro Muffin. En febrero de 1983 fueron acusados de «violar un sepulcro», tras ser capturados cavando en el cementerio de Mountain View Church en mitad de la noche. Sin haber descubierto otra cosa que un féretro, pasaron el resto del fin de semana en la cárcel del condado y finalmente tuvieron que pagar una multa de 500 dólares. Estos sepultureros aficionados pueden consolarse a sí mismos sabiendo que apenas tuvieron menos éxito que Mel Fisher, el cazador de tesoros profesional que salvó un cargamento de oro valorado en 40 millones de dólares del galeón español hundido *Nuestra Señora de Atocha*, que descubrió cerca de Key West, Florida, en 1985. En noviembre de 1989, Fisher recibió una información de un experto en Beale de Florida, que creía que el tesoro de Beale estaba enterrado en Graham's Mill, en el condado de Bedford, Virginia. Apoyado por un equipo de ricos inversores, Fisher compró el lugar bajo el nombre de míster Voda, para no despertar sospechas. A pesar de una larga excavación, no descubrió nada.

Algunos cazadores de tesoros han abandonado la esperanza de resolver las dos hojas que quedan por descifrar, y en vez de ello se han concentrado en extraer pistas de la cifra que ha sido descifrada. Por ejemplo, además de describir el contenido del tesoro enterrado, la cifra resuelta afirma que está depositado «a unas cuatro millas de Buford», lo que probablemente remite a la localidad de Buford o, más específicamente a la taberna Buford's, situada en el centro de la figura 25. La

cifra menciona también que «la excavación está más o menos bordeada de piedras», por lo que muchos cazadores de tesoros han buscado a lo largo de Goose Creek, un lugar lleno de grandes piedras. Cada verano la región atrae a muchos aspirantes esperanzados, algunos de ellos armados con detectores de metal, otros acompañados de médiums o adivinos. La cercana ciudad de Bedford tiene varios negocios que gustosamente alquilan equipamiento, incluso excavadoras industriales. Los granjeros locales tienden a ser menos acogedores con los extraños, que a menudo entran sin permiso en su tierra, dañan sus cercas y cavan hoyos gigantes.

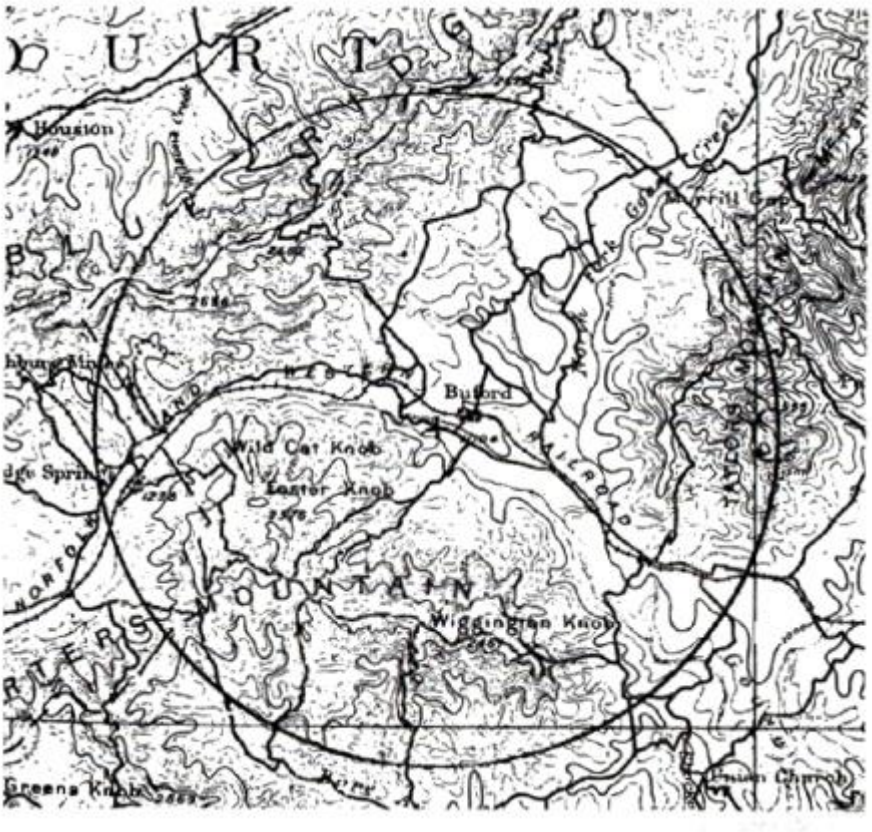


Figura 25. Parte de un mapa de la Inspección Geológica de Estados Unidos realizado en 1891. El círculo tiene un radio de cuatro millas y su centro se halla en la taberna Buford's, un lugar al que se alude en la segunda cifra.

Después de leer la historia de las cifras Beale, puede que usted se anime a tomar el desafío. El aliciente de una cifra del siglo XIX aún sin descifrar, junto a un tesoro

valorado en 20 millones de dólares, puede resultar irresistible. Sin embargo, antes de ponerse a seguir el rastro del tesoro, preste atención al consejo ofrecido por el autor del folleto:

> *Antes de entregar los papeles al público, me gustaría decir unas palabras a los que pueden interesarse en ellos y darles un pequeño consejo, adquirido por amarga experiencia Es que dediquen a la tarea sólo el tiempo que les reste de sus ocupaciones legítimas, y si no les queda nada de tiempo, que se olviden del asunto... De nuevo, nunca sacrifique, como he hecho yo, sus propios intereses y los de su familia por lo que podría resultar ser una ilusión; pero, como ya he dicho, cuando ya haya hecho su trabajo del día y esté cómodamente sentado junto a un buen fuego, un poco de tiempo dedicado al tema no hará daño a nadie y puede verse bien recompensado.*

Capítulo 3
La mecanización del secreto

Contenido:

1. El Santo Grial de la criptografía

2. El desarrollo de las máquinas de cifras. De los discos de cifras a la Enigma

Al final del siglo XIX, la criptografía estaba en desorden. Desde que Babbage y Kasiski acabaron con la seguridad de la cifra Vigenére, los criptógrafos habían estado buscando una nueva cifra, algo que lograra restablecer la comunicación secreta, permitiendo de esta forma a los hombres de negocios y a los militares sacar provecho a la inmediación del telégrafo sin que sus comunicaciones fueran robadas y descifradas. Además, hacia finales de siglo, el físico italiano Guglielmo Marconi inventó una forma de telecomunicación todavía más poderosa, que hizo aún más apremiante la necesidad de una codificación segura.

En 1894 Marconi empezó a experimentar con una curiosa propiedad de los circuitos eléctricos. Bajo ciertas condiciones, si un circuito llevaba una corriente eléctrica, esto podía inducir una corriente en otro circuito aislado situado a cierta distancia. Mejorando el diseño de los dos circuitos, aumentando su potencia y añadiendo antenas, Marconi no tardó en transmitir y recibir pulsaciones de información entre distancias de hasta 2,5 km Había inventado la radio. El telégrafo ya llevaba establecido medio siglo, pero requería un cable para transportar un mensaje entre el emisor y el receptor. El sistema de Marconi tenía la gran ventaja de no necesitar cables; la señal viajaba, como por arte de magia, por el aire.

En 1896, buscando respaldo económico para su idea, Marconi emigró a Gran Bretaña, donde obtuvo su primera patente. Continuando con sus experimentos, aumentó el alcance de sus comunicaciones por radio, transmitiendo primero un mensaje a través de los 15 km del canal de Bristol, y luego los 53 km del canal de la Mancha hasta Francia. Al mismo tiempo comenzó a buscar aplicaciones comerciales para su invento, señalando a los patrocinadores potenciales las dos ventajas principales de la radio: no requería la construcción de costosas líneas de telégrafo y tenía el potencial de enviar mensajes entre lugares que de otra forma

permanecerían aislados. En 1899 llevó a cabo una magnífica maniobra publicitaria, equipando dos barcos con radios para que los periodistas que cubrían la Copa América, la carrera de vela más importante del mundo, pudieran enviar reportajes a Nueva York para que aparecieran en los periódicos del día siguiente.

El interés creció aún más cuando Marconi echó por tierra el mito de que la comunicación por radio quedaba limitada por el horizonte. Los detractores habían alegado que como las ondas de radio no podían curvarse y seguir la curvatura de la Tierra, la comunicación por radio quedaría limitada a unos cien kilómetros. Marconi trató de demostrar que se equivocaban enviando un mensaje desde Poldhu, en Cornualles, a St. John's, en Terranova, a 3500 km de distancia. En diciembre de 1901, durante tres horas cada día, el transmisor de Poldhu envió la letra S (punto-punto-punto) una y otra vez, mientras Marconi se hallaba en los acantilados de Terranova, siempre expuestos al viento, tratando de detectar las ondas de radio. Día tras día, luchó por hacer subir una cometa gigante, que a su vez izaba su antena a gran altura. El 12 de diciembre, un poco después de mediodía, Marconi detectó tres puntos remotos, el primer mensaje de radio transatlántico. La explicación del logro de Marconi siguió siendo un misterio hasta 1942, cuando los físicos descubrieron la ionosfera, una capa de la atmósfera cuyo límite inferior está a unos 60 km sobre la Tierra. La ionosfera actúa como un espejo, permitiendo que las ondas de radio reboten en ella. Las ondas de radio también rebotan en la superficie de la Tierra, por lo que, de hecho, los mensajes por radio pueden llegar a cualquier parte del mundo tras una serie de rebotes entre la ionosfera y la Tierra.

El invento de Marconi sedujo a los militares, que lo vieron con una mezcla de deseo y agitación. Las ventajas tácticas de la radio eran obvias: permite la comunicación directa entre dos puntos sin necesidad de un cable entre los emplazamientos. Tender esos cables es a menudo muy poco práctico, y a veces imposible. Anteriormente, un capitán naval estacionado en un puerto no tenía ninguna manera de comunicarse con sus naves, que podían desaparecer durante meses seguidos, pero la radio le permitiría coordinar una flota sin importar dónde se hallasen los barcos. De manera similar, la radio permitiría que los generales dirigiesen sus campañas, manteniéndolos en contacto continuo con los batallones, a pesar de sus movimientos. Todo esto lo hace posible la naturaleza de las ondas de radio, que

emanan en todas las direcciones, y llegan a los receptores no importa dónde estén. Sin embargo, esta propiedad penetrante de la radio es también su mayor debilidad militar, porque los mensajes llegarán inevitablemente tanto al enemigo como al receptor a quien van dirigidos. Por consiguiente, la codificación fiable se convirtió en algo muy necesario. Si el enemigo iba a poder interceptar todo mensaje de radio, los criptógrafos tenían que encontrar una manera de impedir que descifraran estos mensajes.

Las ventajas e inconvenientes de la radio —facilidad de comunicación y facilidad de interceptación— se pusieron claramente de manifiesto al estallar la primera guerra mundial. Todas las partes estaban deseosas de sacar partido al poder de la radio, pero también se sentían inseguras respecto a cómo garantizar la seguridad. La unión de ambas circunstancias —la llegada de la radio y la guerra mundial— intensificó la necesidad de la codificación efectiva. Había la esperanza de que se produciría un gran avance, alguna nueva cifra que restablecería el secreto para los mandos militares. Sin embargo, entre 1914 y 1918 no iba a surgir ningún gran descubrimiento, solamente un catálogo de fracasos criptográficos. Los creadores de códigos produjeron varias cifras nuevas, pero una a una fueron descifradas.

Una de las cifras más famosas de los tiempos de guerra fue la *cifra ADFGVX* alemana, introducida el 5 de marzo de 1918, justo antes de la gran ofensiva alemana que comenzó el 21 de marzo. Como cualquier ataque, el empuje alemán se beneficiaría del factor sorpresa, y un comité de criptógrafos había seleccionado la cifra ADFGVX entre una variedad de candidatas, creyendo que ofrecía la mejor seguridad. De hecho, confiaban en que era indescifrable. La fortaleza de la cifra radicaba en su naturaleza enrevesada, una mezcla de sustitución y trasposición (véase el Apéndice D).

A principios de junio de 1918, la artillería alemana se encontraba a sólo 100 km de París y se estaba preparando para una ofensiva final. La única esperanza de los aliados era descifrar la cifra ADFGVX para descubrir el lugar exacto en que los alemanes planeaban romper sus defensas. Afortunadamente, tenían un arma secreta, un criptoanalista llamado Georges Painvin. Este francés moreno y esbelto, con una mente penetrante, sólo había reconocido su talento para los enigmas criptográficos tras un encuentro fortuito con un miembro del Bureau du Chiffre

(Oficina de Cifras) poco después del estallido de la guerra. Después de eso, dedicó su valiosísima habilidad a determinar los puntos débiles de las cifras alemanas. Luchó noche y día con la cifra ADFGVX, perdiendo 15 kilos en el proceso.

Finalmente, la noche del 2 de junio descifró un mensaje ADFGVX. El gran avance de Painvin condujo a una serie de nuevos desciframientos, incluido un mensaje que contenía la orden «Envíen municiones rápidamente. Incluso durante el día si no os ven». En el preámbulo se indicaba que había sido enviado desde algún lugar situado entre Montdidier y Compiégne, a unos 80 km al norte de París. La necesidad urgente de municiones implicaba que ése iba a ser el lugar de la inminente ofensiva alemana. El reconocimiento aéreo confirmó que ése era efectivamente el caso. Se enviaron soldados aliados para reforzar este tramo del frente y una semana después comenzó el ataque alemán. Al haber perdido el factor sorpresa, el ejército alemán fue derrotado en una batalla infernal que duró cinco días.

Figura 26. El teniente Georges Painvin.

El desciframiento de la cifra ADFGVX tipificó la criptografía durante la primera guerra mundial. Aunque había una ráfaga de nuevas cifras, todas ellas eran variaciones o combinaciones de cifras decimonónicas que ya habían sido descifradas. Mientras algunas de ellas ofrecían seguridad inicialmente, nunca pasaba mucho tiempo antes de que los criptoanalistas fueran más fuertes que ellas. El mayor problema para los criptoanalistas era enfrentarse al volumen mismo del tráfico. Antes de la llegada de la radio, los mensajes interceptados eran artículos infrecuentes y preciosos, y los criptoanalistas valoraban cada uno de ellos. Sin embargo, en la primera guerra mundial la cantidad de tráfico de radio era enorme, y se podía interceptar cada uno de los mensajes, generando un flujo continuo de textos cifrados para ocupar las mentes de los criptoanalistas. Se estima que los franceses interceptaron mil millones de palabras de comunicaciones alemanas durante el curso de la primera guerra mundial.

De todos los criptoanalistas de los tiempos de la guerra, los franceses fueron los más eficaces. Cuando entraron en la guerra ya contaban con el equipo de descifradores más fuerte de Europa, como consecuencia de la humillante derrota francesa en la guerra franco-prusiana. Napoleón III, deseoso de restaurar su deteriorada popularidad, había invadido Prusia en 1870, pero no había previsto la alianza entre Prusia al norte y los estados alemanes del sur. Conducidos por Otto von Bismarck, los prusianos aplastaron al ejército francés, anexionando las provincias de Alsacia y Lorena y poniendo fin al dominio francés de Europa. Después de eso, la continua amenaza de la Alemania recién unificada parece haber sido el acicate para que los criptoanalistas franceses llegaran a dominar las técnicas necesarias para proporcionar a Francia una inteligencia detallada sobre los planes de su enemigo.

Fue en este clima en el que Auguste Kerckhoffs escribió su tratado *La cryptographie militaire.* Aunque Kerckhoffs era holandés, pasó la mayor parte de su vida en Francia, y sus escritos proporcionaron a los franceses una guía excepcional de los principios del criptoanálisis. Para cuando empezó la primera guerra mundial, tres décadas después, los militares franceses habían puesto en práctica las ideas de Kerckhoffs a escala industrial. Mientras genios solitarios como Painvin trataban de

descifrar las nuevas cifras, equipos de expertos, cada uno con habilidades especialmente desarrolladas para abordar una cifra particular, se concentraban en los desciframientos cotidianos. El tiempo era esencial, y este «criptoanálisis de cinta- transportadora» proporcionaba información —inteligencia— rápida y eficazmente.

Sun-Tzu, autor de *El arte de la guerra*, un texto de estrategia militar que se remonta al siglo IV a. C., afirmó que: «Nada debería considerarse más favorablemente que la inteligencia[8]; nada debería ser tan confidencial como el trabajo de inteligencia». Los franceses eran fervientes creyentes en las palabras de Sun-Tzu, y además de afilar sus habilidades criptoanalíticas, desarrollaron también varias técnicas auxiliares para recoger inteligencia por radio, métodos que no tenían que ver con el desciframiento en sí.

Por ejemplo, los puestos de escucha franceses aprendieron a reconocer el *puño* de los operadores de radio. Una vez codificado, un mensaje se envía en código Morse, como una serie de puntos y rayas, y cada operador puede ser identificado por sus pausas, la velocidad de transmisión y la longitud relativa de los puntos y las rayas. Un *puño* es el equivalente de un estilo reconocible de letra. Además de puestos de escucha operativos, los franceses establecieron seis estaciones para descubrir la dirección, que podían detectar de dónde procedía cada mensaje.

Cada estación movía su antena hasta que la señal entrante alcanzaba su máxima potencia, lo que identificaba una dirección como el origen del mensaje. Combinando la información sobre la dirección ofrecida por dos o más estaciones, era posible localizar el origen exacto de un mensaje. Combinando la información del *puño* con la de la dirección, era posible establecer tanto la identidad como el emplazamiento de, por ejemplo, un batallón en particular. La inteligencia francesa podía entonces seguirle la pista a lo largo de varios días, y deducir potencialmente su destino y objetivo.

Esta forma de recoger inteligencia, conocida como análisis de tráfico, era especialmente valiosa tras la introducción de una cifra nueva. Cada nueva cifra volvía temporalmente impotentes a los criptoanalistas, pero incluso si un mensaje era indescifrable, aún podía proporcionar información mediante el análisis de tráfico.

[8] Se refiere, por supuesto, a la inteligencia en cuanto acumulación de información sobre personas y actividades, especialmente de las enemigas. (N. del T.)

La vigilancia de los franceses contrastaba fuertemente con la actitud de los alemanes, que entraron en la guerra sin contar con una oficina criptográfica militar. Hasta 1916 no se creó el Abhorchdienst, una organización dedicada a interceptar mensajes de los aliados. Parte de la razón de este retraso en establecer el Abhorchdienst era que el ejército alemán se había adentrado en territorio francés en la fase inicial de la guerra. Los franceses, según retrocedían, iban destruyendo las líneas terrestres, obligando a los alemanes a depender de las radios para las comunicaciones. Mientras esto dio a los franceses un suministro continuo de mensajes alemanes interceptados, no sucedía lo mismo en la otra dirección. Según los franceses iban retrocediendo en su propio territorio, tenían todavía acceso a sus propias líneas terrestres y no necesitaban comunicarse por radio. Con la ausencia de comunicaciones francesas por radio, los alemanes no podían realizar interceptaciones, por lo que no se molestaron en desarrollar su departamento criptoanalítico hasta dos años después de comenzar la guerra.

Los británicos y los americanos también hicieron contribuciones importantes al criptoanálisis aliado. La supremacía de los descifradores aliados y su influencia en la primera guerra mundial quedan perfectamente ilustrados en el desciframiento de un telegrama alemán que fue interceptado por los británicos el 17 de enero de 1917. La historia de este desciframiento muestra cómo el criptoanálisis puede afectar el curso de la guerra al más alto nivel y demuestra las repercusiones potencialmente devastadoras de utilizar una codificación inadecuada. En cuestión de semanas, el telegrama descifrado obligaría a Estados Unidos a replantearse su política de neutralidad, cambiando por ello el equilibrio de la guerra.

A pesar de las demandas de políticos ingleses y norteamericanos, el presidente Woodrow Wilson había pasado los dos primeros años de la guerra negándose categóricamente a enviar tropas estadounidenses para apoyar a los aliados. Además de no querer sacrificar a la juventud de su nación en los sangrientos campos de batalla de Europa, estaba convencido de que sólo se podría finalizar la guerra mediante un acuerdo negociado, y creía que podía servir mejor al mundo si permanecía neutral y actuaba como mediador. En noviembre de 1916, Wilson vio la esperanza de un acuerdo cuando Alemania nombró un nuevo ministro de Asuntos Exteriores, Arthur Zimmermann, un hombre gigantesco y jovial que parecía

anunciar una nueva era de diplomacia progresista alemana. Los periódicos americanos lanzaron titulares como NUESTRO AMIGO ZIMMERMANN y LIBERALIZACIÓN DE ALEMANIA, y un artículo lo proclamó como «uno de los augurios más prometedores para el futuro de las relaciones germano-norteamericanas». Sin embargo, lo que los estadounidenses desconocían era que Zimmermann no tenía ninguna intención de perseguir la paz. Por el contrario, estaba tramando extender la agresión militar alemana.

Allá por 1915, un submarino alemán sumergido había sido el responsable del hundimiento del transatlántico *Lusitania,* ahogando a 1198 pasajeros, incluidos 128 civiles norteamericanos. La pérdida del *Lusitania* habría arrastrado a Estados Unidos a la guerra si no hubiera sido por las promesas alemanas que de ahora en adelante los submarinos saldrían a la superficie antes de atacar, una restricción pensada con la intención de evitar ataques accidentales contra barcos civiles.

Figura 27. Arthur Zimraermann.

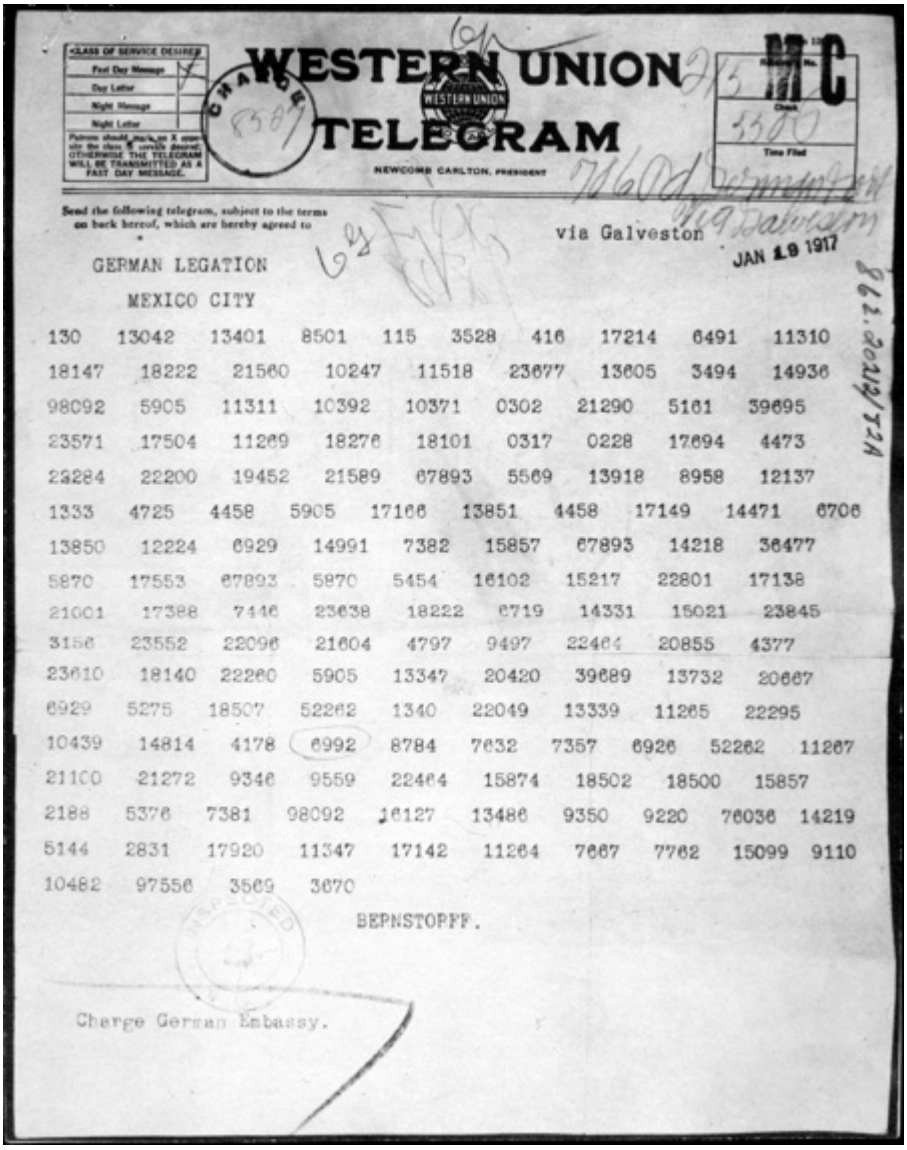
Sin embargo, el 9 de enero de 1917, Zimmermann participó en una reunión transcendental en el castillo alemán de Pless, en la que el Alto Mando Supremo trataba de persuadir al káiser de que había llegado el momento de volverse atrás en su promesa y emprender una guerra submarina sin restricción. Los altos mandos alemanes sabían que sus submarinos eran casi invulnerables si lanzaban sus torpedos mientras permanecían sumergidos, y creían que éste resultaría ser el factor decisivo para determinar el desenlace de la guerra. Alemania había estado construyendo una flota de doscientos submarinos, y el Alto Mando Supremo alegó que la agresión submarina sin restricciones cortaría las líneas de suministro británicas y haría que el hambre la obligara a someterse en menos de seis meses.

Una victoria rápida era esencial. La guerra submarina sin restricciones y el inevitable hundimiento de barcos civiles norteamericanos provocaría casi indudablemente que Estados Unidos declararía la guerra a Alemania. Teniendo esto en cuenta, Alemania necesitaba forzar una rendición aliada antes de que Estados Unidos pudiera movilizar sus tropas y producir un impacto en Europa. Para el final de la reunión de Pless, el káiser estaba convencido de que se podía conseguir una victoria rápida y firmó una orden para proceder con la guerra submarina sin restricción, que entraría en vigor el 1 de febrero.

En las tres semanas que quedaban, Zimmermann urdió una especie de póliza de seguros. Si la guerra submarina sin restricciones aumentaba las probabilidades de que Estados Unidos entrase en la guerra, Zimmermann tenía un plan que retrasaría y debilitaría la implicación norteamericana en Europa, y que incluso podría desalentarla completamente. La idea de Zimmermann era proponer una alianza con México y persuadir al presidente mexicano de que invadiera Estados Unidos y reclamara territorios como Texas, Nuevo México y Arizona. Alemania apoyaría a México en su batalla contra el enemigo común, ayudándole económica y militarmente.

Además, Zimmermann quería que el presidente de México actuara como mediador y persuadiera a Japón de que también debía atacar a Estados Unidos. De esta manera, Alemania amenazaría la costa este de Estados Unidos, Japón atacaría desde el oeste, mientras que México invadiría desde el sur. El principal móvil de

Zimmermann era crear tales problemas a Estados Unidos en su propio territorio que no pudiera permitirse enviar tropas a Europa. Así, Alemania ganaría la batalla en el mar, ganaría la guerra en Europa y luego se retiraría de la campaña americana. El 16 de enero, Zimmermann compendió su propuesta en un telegrama dirigido al embajador alemán en Washington, que debía transmitirlo al embajador alemán en México, que finalmente lo entregaría al presidente mexicano.



WESTERN UNION

TELEGRAM

NEWCOMB CARLTON, PRESIDENT

Send the following telegram, subject to the terms on back hereof, which are hereby agreed to

via Galveston

JAN 19 1917

GERMAN LEGATION

MEXICO CITY

130 13042 13401 8501 115 3528 416 17214 6491 11310
18147 18222 21560 10247 11518 23677 13605 3494 14936
98092 5905 11311 10392 10371 0302 21290 5161 39695
23571 17504 11269 18276 18101 0317 0228 17694 4473
23284 22200 19452 21589 67893 5569 13918 8958 12137
1333 4725 4458 5905 17166 13851 4458 17149 14471 6706
13850 12224 6929 14991 7382 15857 67893 14218 36477
5870 17553 67893 5870 5454 16102 15217 22801 17138
21001 17388 7446 23638 18222 6719 14331 15021 23845
3156 23552 22096 21604 4797 9497 22464 20855 4377
23610 18140 22260 5905 13347 20420 39689 13732 20667
6929 5275 18507 52262 1340 22049 13339 11265 22295
10439 14814 4178 6992 8784 7632 7357 6926 52262 11267
21100 21272 9346 9559 22464 15874 18502 18500 15857
2188 5376 7381 98092 16127 13486 9350 9220 76036 14219
5144 2831 17920 11347 17142 11264 7667 7762 15099 9110
10482 97556 3569 3670

BERNSTORFF.

Charge German Embassy.

Figura 28. El telegrama de Zimmermann, tal como lo remitió Von Bernstorff. el embajador alemán en Washington, a Eckhardt, el embajador alemán en Ciudad de México.

La Figura 28 muestra el telegrama cifrado; el mensaje era el siguiente:

> *Nos proponemos comenzar la guerra submarina sin restricción el 1 de febrero. A pesar de ello, procuraremos mantener neutral a Estados Unidos. En caso de que esto no tenga éxito, hacemos a México una propuesta de alianza con la siguiente base: hacer la guerra juntos, hacer la paz juntos, ayuda económica generosa y el entendimiento por nuestra parte de que México reconquistará los territorios perdidos de Texas, Nuevo México y Arizona. El acuerdo detallado se lo dejamos a usted.*
>
> *Usted informará al presidente [de México] sobre esto en el mayor de los secretos, en cuanto el estallido de la guerra con Estados Unidos sea seguro, y añadirá la sugerencia de que él podría, por iniciativa propia, invitar a Japón a adherirse inmediatamente y, al mismo tiempo, de mediar entre Japón y nosotros.*
>
> *Por favor, señale al presidente el hecho de que el uso sin restricción de nuestros submarinos ofrece ahora la perspectiva de obligar a Inglaterra a firmar la paz en pocos meses. Acuse recibo.*
>
> *Zimmermann*

Zimmermann tuvo que codificar su telegrama porque Alemania era consciente de que los aliados interceptaban todas sus comunicaciones transatlánticas como consecuencia de la primera acción ofensiva británica de la guerra. Antes del amanecer del primer día de la primera guerra mundial, el barco inglés *Telconia* se aproximó a la costa alemana resguardado por la oscuridad, soltó el ancla e izó un conjunto de cables submarinos. Eran los cables transatlánticos de Alemania, sus nexos de conexión con el resto del mundo. A la salida del sol, ya habían sido cortados. Este acto de sabotaje pretendía destruir los medios de comunicación más seguros de Alemania, obligando con ello a que los mensajes alemanes fueran enviados a través de las inseguras conexiones por radio o a través de cables pertenecientes a otros países. Zimmermann se vio obligado a enviar su telegrama cifrado a través de Suecia y, como respaldo de seguridad, también a través del cable más directo, que pertenecía a Estados Unidos. Ambas rutas tocaban

Inglaterra, lo que significó que el texto del *telegrama Zimmermann*, como llegaría a ser conocido, no tardó en caer en manos británicas.

El telegrama interceptado fue enviado inmediatamente a la Sala 40, la agencia de cifras del Ministerio de Marina, que llevaba ese nombre por la oficina en la que se alojaba inicialmente. La Sala 40 era una extraña mezcla de lingüistas, eruditos clásicos y adictos a los crucigramas, capaces de las proezas más ingeniosas en el área del criptoanálisis. Por ejemplo, el reverendo Montgomery, un dotado traductor de obras teológicas alemanas, había descifrado un mensaje secreto oculto en una postal dirigida a *sir* Henry Jones, calle del Rey, 184, Tighnabruaich, Escocia.

La postal había sido enviada desde Turquía, de manera que *sir* Henry había supuesto que era de su hijo, prisionero de los turcos. Sin embargo, se sentía perplejo porque la postal estaba en blanco, y la dirección era peculiar: el pueblo de Tighnabruaich era tan pequeño que ninguna de sus casas tenía número, y no había ninguna calle del Rey. Finalmente, el reverendo Montgomery descubrió el mensaje críptico de la postal. La dirección aludía a la Biblia, Primer Libro de los Reyes, capítulo 18, verso 4:

«Obadiah tomó a cien profetas,
y los ocultó, cincuenta en cada cueva,
y los alimentó con pan y agua».

El hijo de *sir* Henry estaba simplemente tranquilizando a su familia asegurándoles que sus captores cuidaban bien de él.

Cuando el telegrama cifrado de Zimmermann llegó a la Sala 40 se encargó a Montgomery que lo descifrase, junto a Nigel de Grey, un editor procedente de la empresa de William Heinemann Descubrieron inmediatamente que se trataba de una forma de codificación utilizada sólo para comunicaciones diplomáticas de alto nivel y abordaron el telegrama con bastante urgencia. El desciframiento estaba lejos de ser fácil, pero pudieron servirse de análisis previos de otros telegramas codificados de manera similar.

En unas pocas horas, el dúo de descifradores había conseguido recuperar varios trozos de texto, lo suficiente para ver que estaban descubriendo un mensaje de suma importancia. Montgomery y De Grey perseveraron en su tarea, y antes de que

acabara el día pudieron discernir el esbozo de los terribles planes de Zimmermann. Se dieron cuenta de las atroces consecuencias de la guerra submarina sin restricción, pero, al mismo tiempo, podían ver que el ministro alemán de Asuntos Exteriores estaba alentando un ataque contra Estados Unidos, lo que probablemente provocaría al presidente Wilson a abandonar la neutralidad norteamericana. El telegrama contenía la más mortal de las amenazas, pero también la posibilidad de que Estados Unidos se uniera a los aliados.

Montgomery y De Grey llevaron el telegrama parcialmente descifrado al almirante *sir* William Hall, director de la Inteligencia Naval, esperando que pasaría la información a los norteamericanos, arrastrándolos así a la guerra. Sin embargo, el almirante Hall se limitó a colocar el desciframiento parcial en su caja fuerte, alentando a sus criptoanalistas a continuar rellenando los espacios en blanco. Se sentía reacio a pasar a los norteamericanos un desciframiento incompleto, en caso de que hubiera una advertencia vital que todavía no había sido descifrada. También había otra preocupación que le rondaba por la cabeza. Si los británicos entregaban a los norteamericanos el telegrama de Zimmermann descifrado, y éstos reaccionaban condenando públicamente la propuesta agresión alemana, los alemanes conprenderían que su método de codificación había sido adivinado. Esto los empujaría a desarrollar un nuevo sistema de codificación más fuerte, ahogando así un canal vital de inteligencia. En cualquier caso, Hall era consciente de que el ataque submarino total comenzaría en tan sólo dos semanas, lo que podría ser suficiente en sí mismo para incitar al presidente Wilson a declarar la guerra a Alemania. No tenía sentido poner en peligro una valiosa fuente de inteligencia cuando el resultado deseado podía suceder de todos modos.

El 1 de febrero, tal como había ordenado el káiser, Alemania inició la guerra naval sin restricción. El 2 de febrero, Woodrow Wilson mantuvo un consejo de ministros para decidir la respuesta norteamericana. El 3 de febrero habló al Congreso y anunció que Estados Unidos continuaría permaneciendo neutral, actuando como pacificadores, no como combatientes. Esto iba en contra de las expectativas aliadas y alemanas. La reticencia norteamericana a unirse a los aliados no dejó al almirante Hall otra opción que sacar partido al telegrama Zimmermann.

En las dos semanas transcurridas desde que Montgomery y De Grey se habían puesto en contacto con Hall por vez primera habían completado el desciframiento. Además, Hall había encontrado una manera de evitar que Alemania sospechara que su seguridad había sido violada. Se dio cuenta de que Von Bemstorff, el embajador alemán en Washington, habría remitido el mensaje a Von Eckhardt, el embajador alemán en México, tras haber realizado algunos pequeños cambios. Por ejemplo, Von Bernstorff habría suprimido las instrucciones dirigidas a él mismo, y también habría cambiado la dirección Von Eckhardt habría entregado entonces esta versión revisada del telegrama, sin codificar, al presidente de México. Si Hall pudiera obtener de algún modo esta versión mexicana del telegrama de Zimmermann, entonces podría publicarlo en los periódicos y los alemanes supondrían que había sido robado al gobierno mexicano, no interceptado y descifrado por los británicos cuando iba de camino a América. Hall se puso en contacto con un agente británico en México, conocido tan sólo como Mister H, que a su vez se infiltró en la oficina de telégrafos mexicana. Mister H. logró obtener exactamente lo que necesitaba, la versión mexicana del telegrama Zimmermann.

Fue esta versión del telegrama la que Hall entregó a Arthur Balfour, el secretario de Estado de Asuntos Exteriores británico. El 23 de febrero, Balfour convocó al embajador norteamericano, Walter Page, y le entregó el telegrama de Zimmermann. Posteriormente diría que ése fue «el momento más dramático de toda mi vida». Cuatro días después, el presidente Wilson vio por sí mismo la «elocuente evidencia», como él la llamó, que probaba que Alemania había fomentado la agresión directa contra Estados Unidos.

El telegrama fue publicado en la prensa y, por fin, la nación norteamericana se vio enfrentada a la realidad de las intenciones de Alemania. Aunque no había muchas dudas entre la gente estadounidense de que deberían tomar represalias, entre los miembros del gobierno existía la preocupación de que el telegrama pudiera ser un engaño, fabricado por los británicos para garantizar la implicación de Estados Unidos en la guerra. Sin embargo, la cuestión de la autenticidad se disipó muy pronto, cuando Zimmermann admitió públicamente ser su autor. En una rueda de prensa celebrada en Berlín, sin ser acuciado, afirmó simplemente:

«No puedo negarlo. Es verdad».

En Alemania, el Ministerio de Asuntos Exteriores inició una investigación sobre cómo habían obtenido los norteamericanos el telegrama Zimmermann. Se tragaron el ardid de Hall y llegaron a la conclusión de que «varios indicios sugieren que la traición se cometió en México». Mientras tanto, Hall continuó maniobrando para evitar que la atención recayera sobre el trabajo de los criptoanalistas británicos. Insertó una noticia en la prensa británica criticando a su propia organización por no haber interceptado el telegrama Zimmermann, lo que, a su vez, dio lugar a una avalancha de artículos que atacaban al servicio secreto británico y alababan a los norteamericanos.

Figura 29. «Le explota en las manos», una viñeta de Rollin Kirby publicada el 3 de marzo de 1917 en The World.

Al comienzo del año, Wilson había dicho que sería un «crimen contra la civilización» llevar a la nación a la guerra, pero el 2 de abril de 1917 había cambiado de opinión:

«Recomiendo al Congreso que declare que el reciente curso del Gobierno Imperial no es en realidad otra cosa que la guerra contra el gobierno y la población de los Estados Unidos y que acepte formalmente la condición de beligerante a la que se ve enpujado». Un solo logro de los criptoanalistas de la Sala 40 había conseguido lo que tres años de diplomacia intensiva no habían podido lograr. Barbara Tuchman, historiadora estadounidense y autora de *El telegrama Zimmermann*, ofreció el siguiente análisis:

> *Si el telegrama nunca hubiera sido interceptado o publicado, inevitablemente los alemanes habrían hecho algo que habría terminado por meternos en la guerra. Pero era ya muy tarde y, si nos hubiéramos demorado mucho más tiempo, puede que los aliados se habrían visto obligados a negociar. Hasta tal punto alteró el telegrama Zimmermann el curso de la Historia...*
>
> *En sí mismo, el telegrama Zimmermann era sólo un guijarro en el largo camino de la Historia. Pero un guijarro puede matar a un Goliat, y éste mató la ilusión norteamericana de que podíamos seguir con nuestros asuntos alegremente, separados de las demás naciones. En el ámbito de los asuntos del mundo, se trató de una pequeña conspiración de un ministro alemán. En la vida de la gente norteamericana, fue el final de la inocencia.*

1. El Santo Grial de la criptografía

La primera guerra mundial vio una serie de victorias de los criptoanalistas, que culminaron con el desciframiento del telegrama Zimmermann. Desde que resolvieran la cifra Vigenére en el siglo xix, los descifradores habían mantenido la ventaja sobre los codificadores. Hasta que, hacia el final de la guerra, cuando los criptógrafos estaban completamente desesperados, unos científicos estadounidenses realizaron un avance extraordinario. Descubrieron que la cifra Vigenére podía utilizarse como base para una forma nueva y más formidable de codificación. De hecho, esta nueva cifra podía ofrecer una seguridad perfecta.

La debilidad fundamental de la cifra Vigenére es su naturaleza cíclica. Si la clave tiene cinco letras, entonces cada quinta letra del texto llano está codificada según el

mismo alfabeto cifra. Si el criptoanalista puede identificar la longitud de la clave, el texto cifrado puede ser tratado como una serie de cinco cifras monoalfabéticas, y cada una de ellas se puede descifrar con el análisis de frecuencia. Sin embargo, considere qué ocurre si la clave se hace más larga.

Imagine un texto llano de 1000 palabras codificadas según la cifra Vigenére e imagine que estamos tratando de criptoanalizar el texto cifrado resultante. Si la clave utilizada para codificar el texto llano sólo tuviera 5 letras, la fase final del criptoanálisis requeriría aplicar el análisis de frecuencia a 5 series de 200 letras, lo que es fácil de hacer. Pero si la clave hubiese tenido 20 letras, la fase final sería un análisis de frecuencia de 20 series de 50 letras, lo que es considerablemente más difícil. Y si la clave hubiera tenido 1000 letras, nos enfrentaríamos a un análisis de frecuencia de 1000 series de 1 letra cada una, lo que es completamente imposible. En otras palabras, si la clave es tan larga como el mensaje, la técnica criptoanalítica desarrollada por Babbage y Kasiski no funcionará.

Utilizar una clave tan larga como el mensaje está muy bien, pero requiere que el criptógrafo cree una clave muy larga. Si el mensaje tiene cientos de letras, la clave también necesita tener cientos de letras. Más que inventar una clave larga desde cero, sería tentador basarla en, por ejemplo, la letra de una canción. Como alternativa, el criptógrafo podría elegir un libro sobre ornitología y basar la clave en una serie de nombres de pájaros elegidos al azar. Sin embargo, semejantes claves son fundamentalmente defectuosas.

En el siguiente ejemplo, he codificado un trozo de texto cifrado utilizando la cifra Vigenére, y usando una frase clave tan larga como el mensaje. Todas las técnicas criptoanalíticas que he descrito anteriormente fracasarán. No obstante, el mensaje se puede descifrar.

Clave	? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ?
Texto llano	? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ?
Texto cifrado	**V H R M H E U Z N F Q D E Z R W X F I D K**

Este nuevo sistema de criptoanalisis comienza con la suposición de que el texto cifrado contiene algunas palabras corrientes como the[9]. A continuación, colocamos the al azar en varios lugares del texto llano, tal como se muestra más abajo, y deducimos qué tipo de letras- clave serían necesarias para que the se convirtiera en el texto cifrado correcto. Por ejemplo, si suponemos que the es la primera palabra del texto llano, ¿qué implicaría esto para las tres primeras letras de la clave? La primera letra de la clave codificaría la t como V. Para calcular la primera letra de la clave, tomamos un cuadro Vígenére, miramos la columna encabezada por la t hasta llegar a la V y vemos que la letra que comienza esa línea es la C. Repetimos este proceso con la h y la e, que estarían codificadas como H y R, respectivamente, y por fin tenemos candidatas para las tres primeras letras de la clave, CAN. Todo esto resulta de la suposición que the es la primera palabra del texto llano. Colocamos the en unas otras pocas posiciones y, de nuevo, deducimos las letras-clave correspondientes. (Si lo desea, puede comprobar la relación entre cada letra del texto llano y cada letra de texto cifrado consultando el cuadro Vigenére de la Tabla 9.

Clave	C A N ? ? ? B S J ? ? ? ? ? Y P T ? ? ? ?
Texto llano	t h e ? ? ? t h e ? ? ? ? ? t h e ? ? ? ?
Texto cifrado	V H R M H E U Z N F Q D E Z R W X F I D K

Hemos probado tres the en tres posiciones arbitrarias del texto cifrado, y de este modo hemos generado tres conjeturas sobre los componentes de ciertas partes de la clave. ¿Cómo podemos saber si los the están en la posición correcta? Suponemos que la clave consta de palabras con sentido, y es a esto a lo que sacamos partido. Si un the no está en la posición correcta, probablemente resultará en una selección fortuita de letras-clave. Sin embargo, si está en la posición correcta, las letras-clave deberían tener algún sentido. Por ejemplo, el primer the produce las letras-clave CAN, lo que es alentador, ya que ésta es una sílaba inglesa perfectamente razonable. Es posible que este the esté en la posición correcta. El segundo the produce BSJ, que es una combinación muy peculiar de consonantes, dando a

[9] The: artículo determinado inglés. Sirve para todos los géneros y números, siendo, por tanto, el equivalente de los artículos castellanos el, la, lo, los y las. (N. del T.)

entender que probablemente el segundo the es un error. El tercer the produce YPT, una sílaba poco corriente pero que merece la pena seguir investigando. Si YPT fuera realmente parte de la clave, sería parte de una palabra más larga, y las únicas posibilidades (en inglés) son APOCALYPTIC (apocalíptico),
CRYPT (cripta) y EGYPT (Egipto), y los derivados de estas palabras. ¿Cómo podemos descubrir si estas palabras son parte de la clave? Podemos poner a prueba cada hipótesis insertando las tres palabras candidatas en la clave, sobre la sección apropiada del texto cifrado, y calculamos el correspondiente texto llano:

Clave	C A N ? ? ? ? ? A P O C A L Y P T I C ? ?
Texto llano	t h e ? ? ? ? ? n q c b e o t h e x g ? ?
Texto cifrado	V H R M H E U Z N F Q D E Z R W X F I D K

Clave	C A N ? ? ? ? ? ? ? ? C R Y P T ? ? ? ?
Texto llano	t h e ? ? ? ? ? ? ? ? c i t h e ? ? ? ?
Texto cifrado	V H R M H E U Z N F Q D E Z R W X F I D K

Clave	C A N ? ? ? ? ? ? ? ? E G Y P T ? ? ? ?
Texto llano	t h e ? ? ? ? ? ? ? ? a t t h e ? ? ? ?
Texto cifrado	V H R M H E U Z N F Q D E Z R W X F I D K

Si la palabra candidata no forma parte de la clave, probablemente dará como resultado un trozo incoherente de texto llano, pero si forma parte de la clave, el texto llano resultante debería tener algún sentido. Con APOCALYPTIC como parte de la clave, el texto llano resultante es un galimatías de primera calidad. Con CRYPT, el texto llano resultante es cithe, lo que no es un trozo de texto llano inconcebible. Sin embargo, si
EGYPT fuera parte de la clave, generaría atthe, una combinación de letras más prometedora en inglés, que probablemente representa las palabras at the (en el, o en la...).
Por ahora, supongamos que la posibilidad más probable es que EGYPT sea parte de la clave. Quizá la clave sea una lista de países. Esto sugeriría que CAN, la parte de la clave que se corresponde con el primer the, es el comienzo de CANADA.

Podemos poner a prueba esta hipótesis calculando más letras del texto llano basándonos en la suposición que CANADA, como EGYPT, forma parte de la clave:

Clave	C A N A D A ? ? ? ? ? ? E G Y P T ? ? ? ?
Texto llano	t h e m e e ? ? ? ? ? ? a t t h e ? ? ? ?
Texto cifrado	V H R M H E U Z N F Q D E Z R W X F I D K

Nuestra suposición parece tener sentido. CANADA implica que el texto llano comienza con themee, que quizá sea el comienzo de the meeting (la reunión). Ahora que hemos deducido algunas letras más del texto llano, ting, podemos deducir la parte correspondiente de la clave, que resulta ser BRAZ. Seguramente esto sea el principio de BRAZIL (Brasil). Utilizando la combinación CANADABRAZILEGYPT como principio de la clave, obtenemos la siguiente decodificación:

the meeting is at the ???? (la reunión es en el ????).

Para encontrar la palabra final del texto llano —el lugar donde se celebrará la reunión— la mejor estrategia sería completar la clave probando uno a uno los nombres de todos los países posibles y deduciendo el texto llano resultante. El único texto llano con sentido resulta de utilizar CUBA como la última parte de la clave:

Clave	C A N A D A B R A Z I L E G Y P T C U B A
Texto llano	t h e m e e t i n g i s a t t h e d o c k
Texto cifrado	V H R M H E U Z N F Q D E Z R W X F I D K

The meeting is at the dock[10]

De modo que una clave tan larga como el mensaje no es suficiente para garantizar la seguridad. La inseguridad en el ejemplo anterior surge porque la clave estaba formada por palabras con sentido. Comenzamos insertando the al azar por todo el texto llano y calculando las letras-clave correspondientes. Pudimos saber cuándo

[10] «La reunión es en el muelle». (N. del T.)

habíamos puesto un the en el lugar correcto porque las letras-clave resultantes podían ser parte de palabras con sentido. Después de eso, usamos estas porciones de la clave para deducir palabras enteras en la clave.

A su vez, esto nos dio más porciones del mensaje, que pudimos expandir hasta completar palabras enteras, y así sucesivamente. Este proceso de ir y venir entre el mensaje y la clave fue posible tan sólo porque la clave tenía una estructura inherente y constaba de palabras reconocibles. Sin embargo, en 1918 los criptógrafos comenzaron a experimentar con claves que carecían de estructura. El resultado fue una cifra indescifrable.

Tabla 9. Cuadro Vigenére.

Llano	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
1	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R

19	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
26	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Cuando finalizó la primera guerra mundial, el comandante Joseph Mauborgne, jefe de la investigación criptográfica del ejército de Estados Unidos, introdujo el concepto de la clave aleatoria, una clave que no constaba de una serie de palabras reconocibles, sino de una serie de letras mezcladas al azar. Abogó el uso de estas claves aleatorias como parte de la cifra Vigenére para proporcionar un nivel de seguridad sin precedentes. La primera fase del sistema de Mauborgne era compilar un gran cuaderno consistente en cientos de hojas de papel, conteniendo cada una ellas una clave única formada de líneas de letras reunidas al azar. Habría dos copias del cuaderno, una para el emisor y la otra para el receptor. Para codificar un mensaje, el emisor aplicaría la cifra Vigenére utilizando la primera hoja de papel del cuaderno como clave. La Figura 30 muestra tres hojas de un cuaderno semejante (en realidad, cada hoja contendría cientos de letras), seguidas de un mensaje codificado usando la clave aleatoria de la primera hoja. El receptor puede descifrar fácilmente el texto cifrado usando la clave idéntica e invirtiendo la cifra Vigenére. Una vez que el mensaje ha sido enviado, recibido y descifrado con éxito, tanto el emisor como el receptor destruyen la hoja que ha servido como clave, para que no vuelva a ser utilizada. Cuando se codifica el siguiente mensaje se usa la siguiente clave aleatoria del cuaderno, que también será posteriormente destruida, y así sucesivamente. Como cada clave se utiliza sólo una vez, una única vez, el sistema se conoce como la *cifra de* cuaderno de uso único.

La cifra de cuaderno de uso único vence todas las debilidades previas. Imagine que el mensaje attack the valley at dawn («ataquen el valle al amanecer») ha sido codificado como en la Figura 30, enviado por un transmisor de radio e interceptado

por el enemigo. El texto cifrado es entregado a un criptoanalista enemigo, que procede a intentar descifrarlo. El primer obstáculo es que, por definición, en una clave aleatoria no hay repetición, de modo que el método de Babbage y Kasiski no puede penetrar en la cifra de cuaderno de uso único. Como alternativa, el criptoanalista enemigo podría colocar la palabra the en varios lugares y tratar de deducir el trozo correspondiente de la clave, como hicimos cuando tratamos de descifrar el mensaje previo. Si el criptoanalista pone the al principio del mensaje, lo que es incorrecto, el correspondiente fragmentó de la clave que surgiría sería WXB, que es una serie de letras al azar. Si el criptoanalista coloca the para que comience en la séptima letra, que da la casualidad de que es correcto, el correspondiente trozo de clave que surgiría sería QKJ, que también es una serie de letras al azar. En otras palabras, el criptoanalista no puede saber si la palabra de prueba está o no en el lugar correcto.

Desesperado, el criptoanalista podría considerar una búsqueda exhaustiva de todas las claves posibles. El texto cifrado consta de 21 letras, de modo que el criptoanalista sabe que la clave consta de 21 letras.

Esto significa que hay aproximadamente

500.000.000.000.000.000.000.000.000.000

claves posibles que probar, lo que está totalmente fuera de las posibilidades humanas o mecánicas.

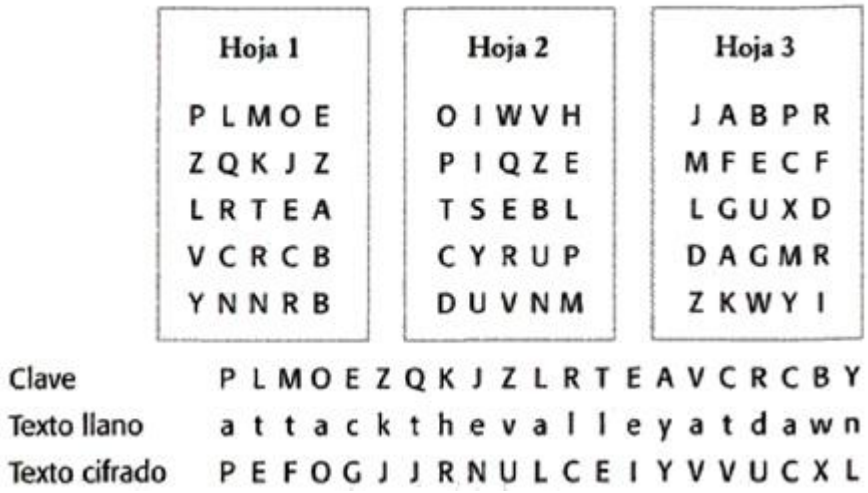


Figura 30. Tres hojas, cada una de ellas una clave potencial para una cifra de cuaderno de uso único. El mensaje está codificado utilizando la Hoja 1.

Sin embargo, incluso si el criptoanalista pudiera poner a prueba todas estas claves, queda un obstáculo aún mayor que tiene que superar. Probando todas las claves posibles, el criptoanalista encontraría indudablemente el mensaje correcto, pero también surgirían todos los mensajes incorrectos. Por ejemplo, la siguiente clave aplicada al mismo texto cifrado genera un mensaje completamente diferente:

Clave	M A A K T G Q K J N D R T I F D B H K T S
Texto llano	d e f e n d t h e h i l l a t s u n s e t
Texto cifrado	P E F O G J J R N U L C E I Y V V U C X L

Defend the hill at sunset[11]

Si se pudieran probar todas las claves diferentes se generarían todos los mensajes de 21 letras concebibles, y el criptoanalista sería incapaz de distinguir entre el correcto y todos los demás. Esta dificultad no habría surgido si la clave hubiera sido una serie de palabras o una frase, porque, casi con toda seguridad, los mensajes incorrectos hubieran quedado asociados con una clave sin sentido, mientras que el mensaje correcto quedaría asociado con una clave con sentido.

[11] «Defiendan la colina al atardecer». (N. del T.)

La seguridad de la cifra de cuaderno de uso único se debe enteramente a que la secuencia de las letras de la clave es por completo aleatoria. La clave inyecta esta naturaleza aleatoria al texto cifrado, y si el texto cifrado es aleatorio entonces no tiene patrones, ni estructura, nada a lo que se pueda agarrar el criptoanalista. De hecho, se puede probar matemáticamente que es imposible que un criptoanalista descifre un mensaje codificado con una cifra de cuaderno de uso único. En otras palabras, la cifra de cuaderno de uso único no es meramente considerada indescifrable, como sucedía con la cifra Vigenére en el siglo XIX, sino que *es en realidad absolutamente segura.* El cuaderno de uso único ofrece garantía de secreto: el Santo Grial de la criptografía.

Por fin, los criptógrafos habían encontrado un sistema de codificación indescifrable. Sin embargo, la perfección de la cifra de cuaderno de uso único no dio fin a la búsqueda de métodos para garantizar el secreto: lo cierto es que casi nunca se ha usado. Aunque en teoría es perfecta, en la práctica tienes fallos, ya que padece de dos dificultades fundamentales. En primer lugar, está el problema práctico de crear grandes cantidades de claves aleatorias. En un solo día, un ejército puede intercambiar cientos de mensajes, con miles de caracteres cada uno, de modo que los operadores de radio requerirían un abastecimiento diario de claves equivalente a millones de letras colocadas al azar. Suministrar tantas secuencias aleatorias de letras constituye una tarea inmensa.

Inicialmente, algunos criptógrafos supusieron que podrían generar cantidades enormes de claves aleatorias tecleando desordenadamente en una máquina de escribir. Sin embargo, siempre que se intentaba esto, la persona que lo hacía tendía a caer en el hábito de escribir un carácter usando la mano izquierda, y luego un carácter con la mano derecha, para después ir alternado entre los dos lados. Esto podía constituir una forma rápida de generar una clave, pero la secuencia resultante tiene estructura, y ya no es aleatoria: si quien escribe teclea la letra D, al lado izquierdo del teclado, entonces la letra siguiente es predecible en tanto que es probable que proceda de la parte derecha del teclado. Si una cifra de cuaderno de uso único va a ser verdaderamente aleatoria, a una letra del lado izquierdo del teclado debería seguirle otra letra del mismo lado izquierdo del teclado en aproximadamente la mitad de las veces.

Los criptógrafos se han dado cuenta de que se requiere muchísimo tiempo, esfuerzo y dinero para crear una clave aleatoria. Las mejores claves aleatorias se crean utilizando procesos físicos naturales, como la radioactividad, que se sabe que exhibe una conducta verdaderamente aleatoria. El criptógrafo podría colocar algo de material radioactivo en una banqueta y detectar su emisión con un contador Geiger. A veces, las emisiones se sucederían rápidamente, a veces habría largas pausas: el tiempo entre las emisiones es impredecible y aleatorio. El criptógrafo podría conectar un dispositivo al contador Geiger que iría pasando rápidamente por el alfabeto a un ritmo fijo, pero que se detendría momentáneamente en cuanto se detectase una emisión. La letra que apareciera en el momento de la pausa sería utilizada como la letra siguiente de la clave aleatoria. El dispositivo vuelve a ponerse en movimiento y recorre de nuevo el alfabeto hasta que se detiene al azar debido a la siguiente emisión: la letra que aparece se añade a la clave, y así sucesivamente. Este sistema garantizaría la creación de una clave verdaderamente aleatoria, pero no resulta práctico para la criptografía cotidiana.

Incluso si se pudieran crear suficientes claves aleatorias, queda un segundo problema, concretamente la dificultad de distribuirlas. Imagine la posibilidad de un campo de batalla en el que cientos de operadores de radio forman parte de la misma red de comunicaciones. Para empezar, todas y cada una de las personas deben tener copias idénticas del cuaderno de uso único. Además, cada vez que se emitan nuevos cuadernos deben ser distribuidos a todo el mundo simultáneamente. Finalmente, todo el mundo tiene que permanecer al día, asegurándose de que están utilizando la hoja apropiada del cuaderno de uso único en el momento apropiado. El uso generalizado del cuaderno de uso único llenaría el campo de batalla de mensajeros y contables. Además, si el enemigo captura un solo juego de claves, todo el sistema de comunicaciones se ve comprometido.

Podría resultar tentador tratar de reducir la creación y distribución de claves volviendo a usar los cuadernos de uso único, pero esto constituye un pecado cardinal criptográfico. Volver a utilizar un cuaderno de uso único permitiría a un criptoanalista enemigo descifrar mensajes con relativa facilidad. La técnica empleada para desentrañar dos textos cifrados codificados con la misma clave de cuaderno de uso único se explica en el Apéndice E, pero por ahora lo importante es

que no puede haber atajos al usar la cifra de cuaderno de uso único. El emisor y el receptor deben usar una clave nueva para cada mensaje.

Un cuaderno de uso único es factible para personas que necesitan una comunicación ultrasegura y que pueden permitirse mantener los enormes costes de creación y distribución segura de las claves. Por ejemplo, la línea directa entre los presidentes de Rusia y de Estados Unidos está protegida por una cifra de cuaderno de uso único.

Los defectos prácticos del teóricamente perfecto cuaderno de uso único tuvieron como consecuencia que la idea de Mauborgne nunca se pudo utilizar en el calor de la batalla. En el período que siguió a la primera guerra mundial y todos sus fracasos criptográficos, continuó la búsqueda de un sistema práctico que pudiera ser utilizado en el siguiente conflicto. Afortunadamente para los criptógrafos, no transcurrió mucho tiempo antes de que realizaran un gran avance, algo que restablecería la comunicación secreta en el campo de batalla. Para fortalecer sus cifras, los criptógrafos se vieron obligados a abandonar el lápiz y el papel, y a sacar partido de la tecnología más avanzada para codificar mensajes.

2. El desarrollo de las máquinas de cifras. De los discos de cifras a la Enigma

La primera máquina criptográfica es el disco de cifras, inventado en el siglo XV por el arquitecto italiano León Alberti, uno de los padres de la cifra poli alfabética. Tomó dos discos de cobre, uno ligeramente mayor que el otro, e inscribió el alfabeto al borde de ambos. Colocando el disco pequeño sobre el grande y fijándolos con una aguja que sirviera de eje construyó algo similar al disco de cifras que se muestra en la Figura 31. Los dos discos pueden hacerse girar independientemente, de modo que los dos alfabetos pueden tener diferentes posiciones relativas y, por tanto, se puede utilizar para codificar un mensaje con un simple cambio del César. Por ejemplo, para codificar un mensaje con un cambio del César de una posición, se coloca la A externa junto a la B interna; el disco externo es el alfabeto llano, y el disco interno representa el alfabeto cifrado. Se busca cada letra del mensaje de texto llano en el disco externo, y la correspondiente letra del disco interno se escribe como parte del texto cifrado. Para enviar un mensaje con un cambio del

César de cinco posiciones simplemente hay que girar los discos de modo que la A externa esté junto a la F interna, y luego usar el disco de cifras en esta nueva posición

Figura 31. Un disco de cifras de la Confederación estadounidense utilizado en la guerra civil norteamericana

A pesar de que el disco de cifras es un aparato muy básico no hay duda de que facilita la codificación y ha perdurado durante cinco siglos. La versión mostrada en la Figura 31 fue utilizada en la guerra civil norteamericana.

La Figura 32 muestra un codeógrafo, un disco de cifras usado por el epónimo héroe de *Capitán Medianoche*, uno de los primeros programas dramáticos de la radio estadounidense. Los oyentes podían obtener su propio codeógrafo escribiendo a la compañía patrocinadora del programa, Ovaltine[12], y adjuntando una etiqueta de uno de sus envases. De vez en cuando, el programa finalizaba con un mensaje secreto del Capitán Medianoche, que los oyentes leales podían descifrar utilizando el

[12] Ovaltine: popular sucedáneo del café a base, principalmente, de malta. (N. del T.)

codeógrafo.

Figura 32. Codeógrafo del Capitán Medianoche que codifica cada letra de texto llano (disco externo) con un número (disco interno) en vez de cómo una letra.

El disco de cifras puede ser considerado un «modificador», que toma cada letra de texto llano y la transforma en otra cosa. El modo de operación descrito hasta ahora es sencillo, y la cifra resultante es muy fácil de descifrar, pero el disco de cifras puede ser utilizado de manera más compleja. Su inventor, Alberti, sugirió cambiar la posición del disco durante el mensaje, lo que de hecho genera una cifra polialfabética en vez de monoalfabética. Por ejemplo, Alberti podría haber usado su disco para cifrar la palabra goodbye (adiós), empleando la clave LEON. Comenzaría situando su disco según la primera letra de la clave, poniendo la A externa junto a la L interna. Luego codificaría la primera letra del mensaje, g, buscándola en el disco externo y anotando la letra correspondiente del disco interno, que es la R.

Para codificar la segunda letra del mensaje resituaría su disco según la segunda letra de la clave, poniendo la A externa junto a la E interna. Luego codificaría la o buscándola en el disco externo y anotando la letra correspondiente del disco interno, que es la S. El proceso de codificación continúa colocando el disco de cifras según la letra O de la clave, luego la N, luego de vuelta a la L, y así sucesivamente. Alberti ha codificado eficazmente un mensaje usando la cifra Vigenére, con su nombre de pila actuando como clave. El disco de cifras acelera la codificación y reduce los errores comparado con realizar la codificación mediante un cuadro Vigenére.

La característica principal de utilizar el disco de cifras de esta manera es el hecho de que el disco cambia su modo de cifrar durante la codificación. Aunque este nivel extra de complicación hace que la cifra sea más difícil de descifrar, no la hace indescifrable, porque estamos simplemente ante una versión mecanizada de la cifra Vigenére, la cual fue desentrañada por Babbage y Kasiski. Sin embargo, quinientos años después de Alberti, una reencarnación más compleja de su disco de cifras conduciría a una nueva generación de cifras, una índole de magnitud más difícil de descifrar que nada de lo usado previamente.

En 1918 el inventor alemán Arthur Scherbius y su íntimo amigo Richard Ritter fundaron la compañía Scherbius y Ritter, una innovadora empresa de ingeniería que lo cubría todo, desde turbinas a almohadas eléctricas. Scherbius estaba a cargo de la investigación y el desarrollo, y buscaba continuamente nuevas oportunidades. Uno de sus proyectos preferidos era sustituir los inadecuados sistemas de criptografía empleados en la primera guerra mundial cambiando las cifras de «lápiz y papel» por una forma de codificación que sacara partido a la tecnología del siglo XX. Había estudiado ingeniería eléctrica en Hannover y en Munich, y desarrolló una pieza de maquinaria criptográfica que era esencialmente una versión eléctrica del disco de cifras de Alberti. El invento de Scherbius, denominado Enigma, se convertiría en el más temible sistema de codificación de la Historia.

La máquina Enigma de Scherbius constaba de una serie de ingeniosos componentes, que combinó para formar una formidable y compleja máquina de cifras. Sin embargo, si descomponemos la máquina en sus partes constituyentes y la reconstruimos en fases quedarán claros sus principios fundamentales. La forma

básica del invento de Scherbius consiste en tres elementos conectados por cables: un teclado para escribir cada letra de texto llano, una unidad modificadora que codifica cada letra de texto llano en una correspondiente letra de texto cifrado y un tablero expositor consistente de varias lámparas para indicar la letra de texto cifrado. La Figura 33 muestra un esquema estilizado de la máquina, limitado a un alfabeto de seis letras para mayor simplicidad. Para codificar una letra de texto llano, el operador pulsa la letra apropiada de texto llano en el teclado, lo que envía una pulsación eléctrica a través de la unidad modificadora central, y llega al otro lado, donde ilumina la correspondiente letra de texto cifrado en el tablero.

El modificador, un grueso disco de goma plagado de cables, es la parte más importante de la máquina. Desde el teclado, los cables entran en el modificador por seis puntos y luego hacen una serie de giros y rodeos dentro del modificador antes de salir por seis puntos al otro lado. El cableado interno del modificador determina cómo serán codificadas las letras del texto llano. Por ejemplo, en la Figura 33 el cableado dicta que:

- *teclear la a iluminará la letra B, lo que significa que la a es codificada como B,*
- *teclear la b iluminará la letra A, lo que significa que la b es codificada como A,*
- *teclear la c iluminará la letra D, lo que significa que la c es codificada como D,*
- *teclear la d iluminará la letra F, lo que significa que la d es codificada como F,*
- *teclear la e iluminará la letra E, lo que significa que la e es codificada como E,*
- *teclear la f iluminará la letra C, lo que significa que la f es codificada como C.*

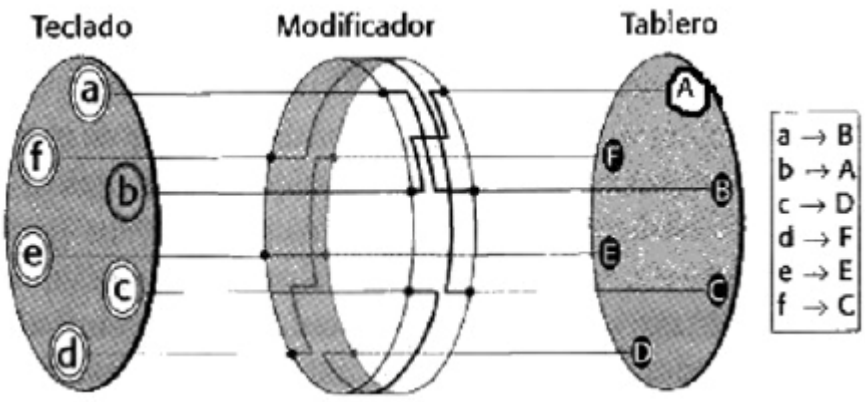


Figura 33. Una versión simplificada de la máquina Enigma con un alfabeto de sólo seis letras. El elemento más impórtame de la máquina es el modificador. Al pul sar la b en el teclado, una corriente pasa al modificador, sigue el sendero del cableado interno y finalmente sale iluminando la lámpara A en el tablero. Resumiendo, la b es codificada como A. El recuadro de la derecha indica cómo se codifica cada una de las seis letras.*

El mensaje café sería codificado como DBCE. Con esta disposición básica, el modificador define esencialmente un alfabeto cifrado y la máquina puede ser utilizada para llevar a cabo una cifra de sustitución monoalfabética simple.

Sin embargo, la idea de Scherbius era que el modificador girase automáticamente un sexto de revolución cada vez que se codificara una letra (o, más bien, un veintiseisavo de revolución para un alfabeto completo de 26 letras). La Figura 34(a) muestra la misma disposición que la Figura 33; de nuevo, teclear la b iluminará la letra A. Sin embargo, esta vez, inmediatamente después de teclear una letra y de que se ilumine el tablero, el modificador gira un sexto de revolución y alcanza la posición que se muestra en la Figura 34(b). Teclear de nuevo la letra b iluminará ahora una letra diferente, concretamente la C. Inmediatamente después, el modificador gira una vez más, hasta llegar a la posición mostrada en la Figura 34(c). Esta vez, teclear la letra b iluminará la E. Teclear la letra b seis veces seguidas generaría el texto cifrado ACEBDC. En otras palabras, el alfabeto cifrado cambia tras cada codificación y la codificación de la letra b está cambiando continuamente. Con esta disposición giratoria, el modificador define esencialmente

seis alfabetos cifrados, y la máquina se puede utilizar para llevar a cabo una cifra polialfabética.

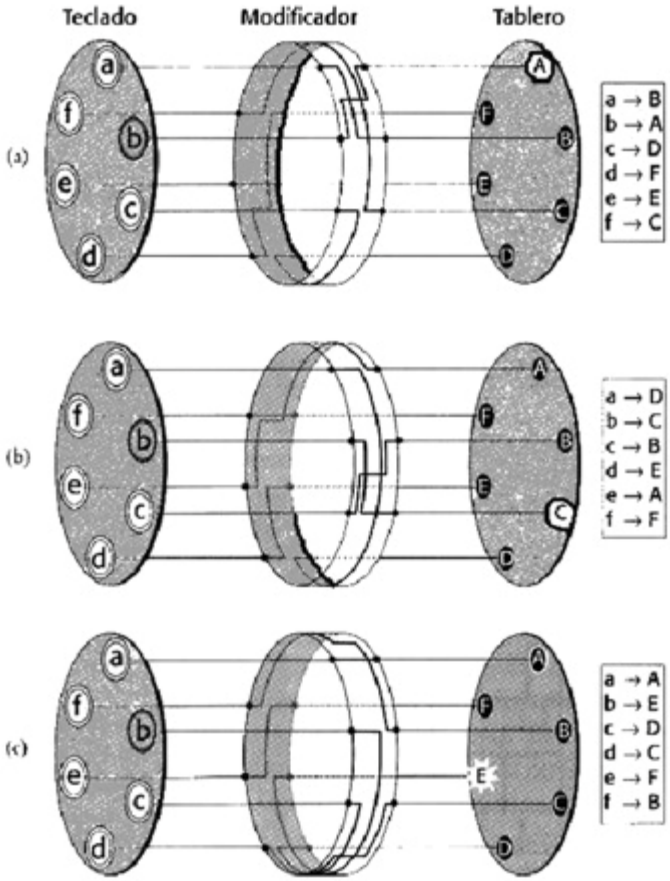


Figura 34. Cada vez que se pulsa una letra en el teclado y se codifica, el modificador gira una posición, cambiando así como se codifica potencialmente cada letra. En (a) el modificador codifica la b como A; pero en (b) la nueva orientación del modificador codifica la b como C. En (c), tras girar una posición más, el modificador codifica la b como E, Después de codificar cuatro letras más y girar cuatro posiciones más, el modificador vuelve a su orientación original.

La rotación del modificador es la característica más inportante del diseño de Scherbius. Sin embargo, la máquina, tal como se presenta, tiene una debilidad obvia. Teclear la b seis veces hará que el modificador vuelva a su posición original y teclear la b una y otra vez repetirá el mismo patrón de codificación. En general, los criptógrafos se han mostrado deseosos de evitar la repetición, porque conduce a la

regularidad y la estructura en el texto cifrado, que son los síntomas de una cifra débil. Este problema se puede mitigar introduciendo un segundo disco modificador.

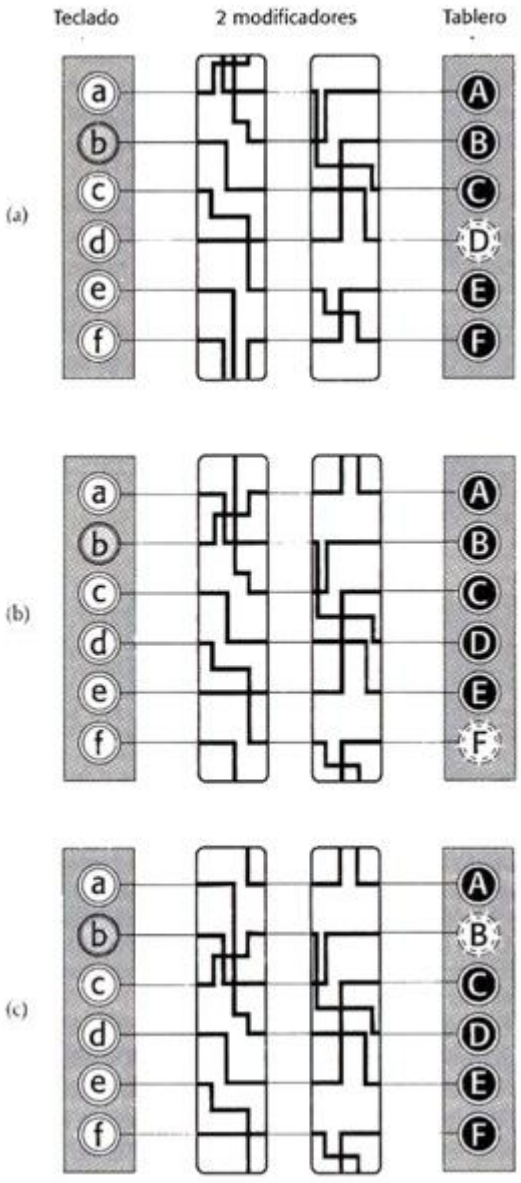


Figura 35. Al añadir un segundo modificador, el patrón de codificación no se repite hasta que se han codificado 36 letras, y ambos modificadores han vuelto a sus posiciones originales. Para simplificar el diagrama, los modificadores están representados en dos dimensiones: en vez de girar una posición, los cableados descienden una posición. Si un cable parece dejar la parte superior o interior de un modificador, su sendero se puede seguir continuando desde el cable correspondiente de la parte inferior o superior del mismo modificador, en (a), b se codifica como D. Después de la codificación, el primer modificador gira una posición, haciendo que también el segundo modificador se mueva una posición —esto sucede sólo una vez durante cada revolución completa de la primera rueda—. Esta nueva disposición se muestra en (b), en la que b se codifica como F. Después de la codificación, el primer modificador gira una posición, pero esta vez el segundo modificador permanece fijo. Esta nueva disposición se muestra en (c) en la que b se codifica como B.

La Figura 35 es un esquema de una máquina de cifras con dos modificadores. A causa de la dificultad de dibujar un modificador tridimensional con cableados internos tridimensionales, la Figura 35 muestra sólo una representación en dos dimensiones. Cada vez que se codifica una letra, el primer modificador gira un espacio, o desde el punto de vista del diagrama en dos dimensiones, cada cableado desciende una posición El segundo disco modificador, por el contrario, permanece inmóvil la mayor parte del tiempo. Sólo se mueve después de que el primer modificador ha realizado una revolución completa. El primer modificador cuenta con un diente y sólo cuando este diente llega a un cierto punto hace que el segundo modificador se mueva una posición.

En la Figura 35(a), el primer modificador se encuentra en una posición en la que está a punto de hacer que avance el segundo modificador. Teclear y codificar una letra mueve el mecanismo a la configuración mostrada en la Figura 35(b), en la que el primer modificador se ha movido una posición y el segundo modificador también ha sido movido una posición. Teclear y codificar otra letra mueve de nuevo el primer modificador una posición, como se ve en la Figura 35(c), pero esta vez el segundo modificador ha permanecido inmóvil. El segundo modificador no volverá a moverse hasta que el primer modificador complete una revolución, lo que le llevará otras cinco codificaciones. Este sistema es similar al cuentakilómetros de un coche: el rotor que representa los kilómetros individuales gira bastante rápido, y cuando completa una revolución llegando a «9», hace que el rotor que representa la decena de kilómetros avance una posición.

La ventaja de añadir un segundo modificador es que el patrón de codificación no se repite hasta que el segundo modificador vuelve a estar como al principio, lo que requiere seis revoluciones completas del primer modificador, o la codificación de 6 x 6, es decir, de 36 letras en total. En otras palabras, hay 36 disposiciones de los modificadores distintas, lo que equivale a cambiar entre 36 alfabetos cifrados. Con un alfabeto completo de 26 letras, la máquina de cifras cambiaría entre 26 x 26, es decir, 676 alfabetos cifrados.

De modo que combinando los modificadores (a veces llamados rotores), es posible construir una máquina de codificación que cambia continuamente entre diferentes alfabetos cifrados. El operador teclea una letra particular y, dependiendo de la

disposición del modificador, puede ser codificada según cualquiera de los cientos de alfabetos cifrados. Luego, la disposición del modificador cambia, de modo que cuando se teclea la siguiente letra es codificada según un alfabeto cifrado diferente. Además, todo esto se lleva a cabo con gran eficiencia y exactitud, gracias al movimiento automático de los modificadores y a la velocidad de la electricidad.

Antes de explicar con detalle cómo quería Scherbius que se utilizara su máquina de codificación, es necesario describir otros dos elementos de la Enigma, que se muestran en la Figura 36. Primero, la máquina de codificación de Scherbius estándar usaba un tercer modificador para obtener aún más complejidad: para un alfabeto completo, estos tres modificadores proveerían 26 x 26 x 26, es decir, 17.576 disposiciones diferentes de los modificadores. Segundo, Scherbius añadió un *reflector.* El reflector se parece un poco a un modificador, en cuanto es un disco de goma con cableados internos, pero es diferente porque no gira, y los cables entran por un lado y vuelven a salir por el mismo lado. Con el reflector colocado, el operador teclea una letra, lo que envía una señal eléctrica a través de los tres modificadores. Cuando el reflector recibe la señal entrante la devuelve a través de los tres mismos modificadores, pero por una ruta diferente. Por ejemplo, con la disposición de la Figura 36 teclear la letra b enviaría una señal a través de los tres modificadores y en el reflector, tras lo cual la señal volvería a través de los cableados para llegar a la letra D. La señal no surge realmente a través del teclado, como podría parecer en la Figura 36, sino que es desviada al tablero. A primera vista, el reflector parece ser un añadido inútil en la máquina, porque al ser estático no aumenta el número de alfabetos cifrados. Sin embargo, su beneficio resulta obvio cuando se ve cómo la máquina codificaba y descodificaba realmente un mensaje.

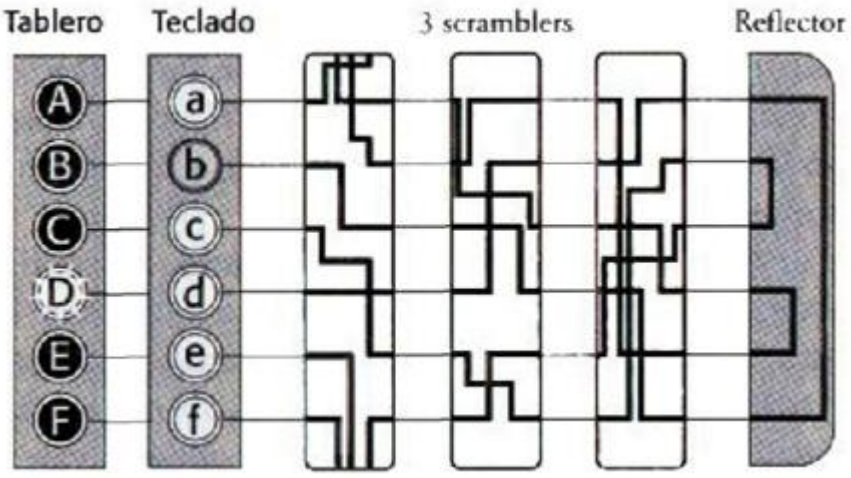


Figura 36. El diseño de la Enigma de Scherbius incluía un tercer modificador y un reflector que devuelve la corriente a través de los modificadores. En esta posición particular, teclear la b iluminará la D en el tablero, que aquí se muestra contiguo al teclado.

Un operador desea enviar un mensaje secreto. Antes de comenzar la codificación, el operador debe hacer girar los modificadores para situarlos en una posición particular. Hay 17.576 disposiciones posibles, y, por tanto, 17.576 posiciones de partida posibles. La disposición inicial de los modificadores determinará cómo se codifica el mensaje. Podemos considerar la máquina Enigma desde el punto de vista de un sistema general de cifras, y las posiciones iniciales son lo que determina los detalles exactos de la codificación. En otras palabras, las posiciones iniciales proporcionan la clave. Generalmente, las posiciones iniciales vienen dictadas por un libro de códigos, que enumera la clave para cada día y que está disponible para todos los que forman parte de la red de comunicaciones.

Distribuir el libro de códigos requiere tiempo y esfuerzo, pero como sólo se necesita una clave para cada día, se podría acordar enviar un libro de códigos que contenga 28 claves una vez cada cuatro semanas. En cambio, si un ejército decidiera usar una cifra de cuaderno de uso único requeriría una cifra nueva para cada mensaje y la distribución de la clave constituiría una tarea mucho más ardua. Una vez que los modificadores se han colocado de acuerdo a lo estipulado en el libro de códigos para ese día, el emisor puede comenzar a codificar.

Teclea la primera letra del mensaje, ve qué letra se ilumina en el tablero y la anota como primera letra del texto cifrado. Luego, como el primer modificador ha avanzado una posición automáticamente, el emisor teclea la segunda letra del mensaje, y así sucesivamente. Una vez que ha generado el texto cifrado completo se lo pasa a un operador de radio que lo transmite al receptor a quien va dirigido.

Para descifrar el mensaje, el receptor necesita tener otra máquina Enigma y una copia del libro de códigos que contenga la posición inicial de los modificadores para ese día. Dispone la máquina de acuerdo al libro, teclea el texto cifrado letra a letra y el tablero muestra el texto llano.

En otras palabras, el emisor tecleó el texto llano para generar el texto cifrado y ahora el receptor teclea el texto cifrado para generar el texto llano, la codificación y la descodificación son procesos que se reflejan mutuamente. La facilidad de la descodificación es una consecuencia del reflector. Con la Figura 36 podemos ver que si tecleamos b y seguimos la trayectoria eléctrica volvemos a D. De manera similar, si tecleamos d y seguimos la trayectoria volvemos a B. La máquina codifica una letra de texto llano en una letra de texto cifrado, y, mientras la máquina esté en la misma posición, descodificará la misma letra de texto cifrado en la misma letra original de texto llano.

Es obvio que nunca se debe permitir que la clave y el libro de códigos que la contiene caigan en manos del enemigo. Es bastante posible que el enemigo pueda hacerse con una máquina Enigma, pero sin conocer las posiciones iniciales utilizadas para la codificación no puede descifrar fácilmente un mensaje interceptado. Sin el libro de códigos, el criptoanalista enemigo debe recurrir a probar todas las claves posibles, lo que significa que tiene que probar las 17.576 posiciones iniciales posibles de los modificadores.

El desesperado criptoanalista colocaría los modificadores de la máquina Enigma capturada en una disposición particular, tecletearía un breve fragmento del texto cifrado y vería si las letras resultantes tenían algún sentido. Si no, cambiaría a una disposición diferente de los modificadores y lo intentaría de nuevo.

Si pudiera probar una disposición de los modificadores por minuto y trabajar día y noche, le llevaría casi dos semanas examinar todas las disposiciones posibles. Esto es un nivel de seguridad moderado, pero si el enemigo pone una docena de

personas a realizar la tarea, entonces se podrían probar todas las disposiciones en un día. Debido a ello, Scherbius decidió mejorar la seguridad de su invento aumentando el número de disposiciones iniciales y, de esta manera, el número de claves posibles.

Podría haber aumentado la seguridad añadiendo más modificadores (cada nuevo modificador aumenta el número de claves con un factor de 26), pero esto agrandaría el tamaño de la máquina Enigma. En vez de ello, añadió dos nuevos rasgos. Primero, simplemente hizo que los modificadores se pudieran sacar y fueran intercambiables. Así, por ejemplo, el disco del primer modificador podía ser movido a la tercera posición y el disco del tercer modificador a la primera. La disposición de los modificadores afecta a la codificación, de modo que la disposición exacta es crucial para la codificación y la descodificación. Hay seis maneras diferentes de disponer los tres modificadores, de manera que este rasgo aumenta el número de claves, o el número de posiciones iniciales posibles, con un factor de seis.

El segundo rasgo nuevo fue la inserción de un *clavijero* entre el teclado y el primer modificador. El clavijero permite que el emisor inserte cables que tienen el efecto de intercambiar algunas de las letras antes de que entren en el modificador. Por ejemplo, se podría usar un cable para conectar las tomas del clavijero, es decir, las conexiones, de la a y de la b, de modo que cuando el criptógrafo quiere codificar la letra b, la señal eléctrica sigue en realidad la trayectoria a través de los modificadores que previamente era la trayectoria para la letra a, y viceversa. El operador de la Enigma tenía seis cables, lo que significaba que se podían intercambiar seis pares de letras, dejando catorce letras sin conectar y sin modificar. Las letras intercambiadas por el clavijero forman parte de la disposición de la máquina, de modo que se deben especificar en el libro de códigos. La Figura 37 muestra el esquema de la máquina con el clavijero colocado. Como este diagrama sólo muestra un alfabeto de seis letras, sólo se ha intercambiado un par de letras, la a y la b.

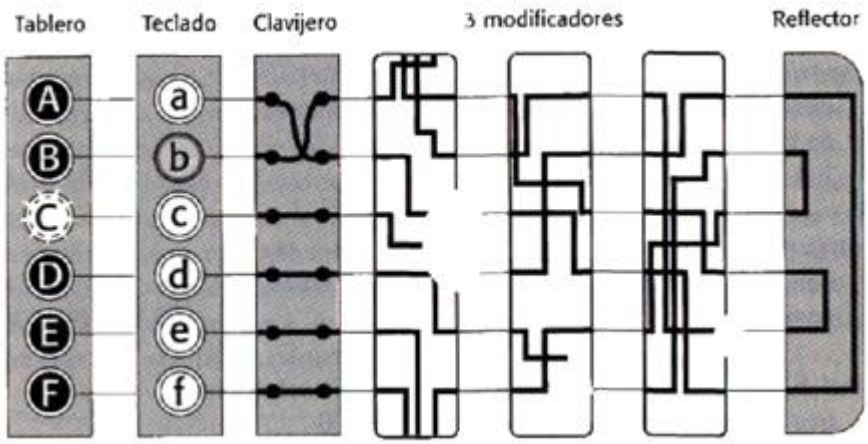


Figura 37. El clavijero está colocado cutre el teclado y e! primer modificador. Insertando cables, es posible intercambiar pares de letras, tic modo que en este caso la b se cambia con la a Ahora, la b es codificada siguiendo la trayectoria que previamente se asociaba con Ja codificación de La a. En la Enigma real de 26 letras, el usuario tendría seis cables para intercambiar seis pares de letras.

Hay otro rasgo más del diseño de Scherbius, conocido como el *anillo*, que aún no ha sido mencionado. Aunque el anillo tiene un cierto efecto en la codificación, es la parte menos significativa de toda la máquina Enigma, y he decidido ignorarlo por lo que respecta a esta exposición. (Los lectores que deseen conocer el papel exacto del anillo deberían consultar alguno de los libros indicados en la lista de lecturas adicionales, como, por ejemplo, *Seizing the Enigma* [«Venciendo la Enigma»], de David Kahn. Esta lista incluye también dos páginas de Internet que contienen excelentes emuladores de la Enigma, que le permitirán operar una máquina Enigma virtual).

Ahora que conocemos todos los elementos principales de la máquina Enigma de Scherbius podemos calcular el número de claves, combinando el número de las posiciones posibles de los cables del clavijero con el número de disposiciones y orientaciones posibles de los modificadores. La lista siguiente muestra cada variable de la máquina y el número correspondiente de posibilidades para cada una:

> *Orientaciones de los modificadores. Cada uno de los tres modificadores se puede situar en 26 orientaciones diferentes. Por tanto, hay 26 x 26 x 26 disposiciones: 17.576*

Disposiciones de los modificadores.
Los tres modificadores (1, 2 y 3) se pueden colocar en cualquier de las disposiciones siguientes: 12-3, 1-3-2, 2-1-3, 2-3-1, 3-1-2, 3-2-1: 6

Clavijero. El número de maneras de conectar, y con ello intercambiar, seis pares de letras entre 26 es enorme: 100.391.791.500

Total. El número total de claves es el múltiplo de estos tres números: 17.576 x 6 x 100.391.791.500 = 10.000.000.000.000.000

Mientras el emisor y el receptor estén de acuerdo sobre la posición de los cables del clavijero, el orden de los modificadores y sus respectivas orientaciones, todo lo cual lo especifica la clave, podrán codificar y descodificar mensajes muy fácilmente. Sin embargo, un interceptador enemigo que no conozca la clave tendrá que probar cada una de las 10.000.000.000.000.000 claves posibles para descifrar el texto cifrado. Poniendo esto en contexto, un criptoanalista persistente que fuera capaz de probar una disposición por minuto necesitaría más tiempo que la edad del universo para probar todas las disposiciones. (De hecho, como he ignorado el efecto del anillo en estos cálculos, el número de claves posibles es aún mayor, así como el tiempo necesario para desentrañar la Enigma).

Como la mayor contribución al número de claves proviene con gran diferencia del clavijero podría usted preguntarse por qué Scherbius se molestó en poner modificadores. Por sí mismo, el clavijero proporcionaría una cifra insignificante, porque no haría otra cosa que actuar como una cifra de sustitución monoalfabética, cambiando entre sólo 12 letras. El problema con el clavijero es que los cambios no se producen una vez que comienza la codificación, de modo que por sí mismo generaría un texto cifrado que no sería difícil de descifrar mediante el análisis de frecuencia. Los modificadores aportan un número menor de claves, pero su

disposición está continuamente cambiando, lo que significa que el texto cifrado resultante no puede ser descifrado con el análisis de frecuencia. Combinando los modificadores con el clavijero, Scherbius protegió su máquina contra el análisis de frecuencia y al mismo tiempo la dotó de un número enorme de claves posibles.

Figura 38, Arthur Scherbius.

Scherbius obtuvo su primera patente en 1918. Su máquina de cifras venía en una caja compacta que sólo medía 34 x 28 x 15 cm, pero que pesaba nada menos que 12 kg. La Figura 39 muestra una máquina Enigma con la cubierta externa abierta, lista para ser usada. Es posible ver el teclado en que se escriben las letras de texto llano y en su parte superior el tablero que muestra la letra de texto cifrado resultante. Debajo del teclado está el clavijero; hay más de seis pares de letras intercambiadas por el clavijero, porque esta máquina Enigma en particular es una

modificación, ligeramente posterior, del modelo original, que es la versión que he venido describiendo hasta ahora.

Figura 39. Una máquina Enigma del Ejército, lista para ser usada

La Figura 40 muestra una Enigma con la cubierta interna abierta para mostrar más rasgos, en particular los tres modificadores.

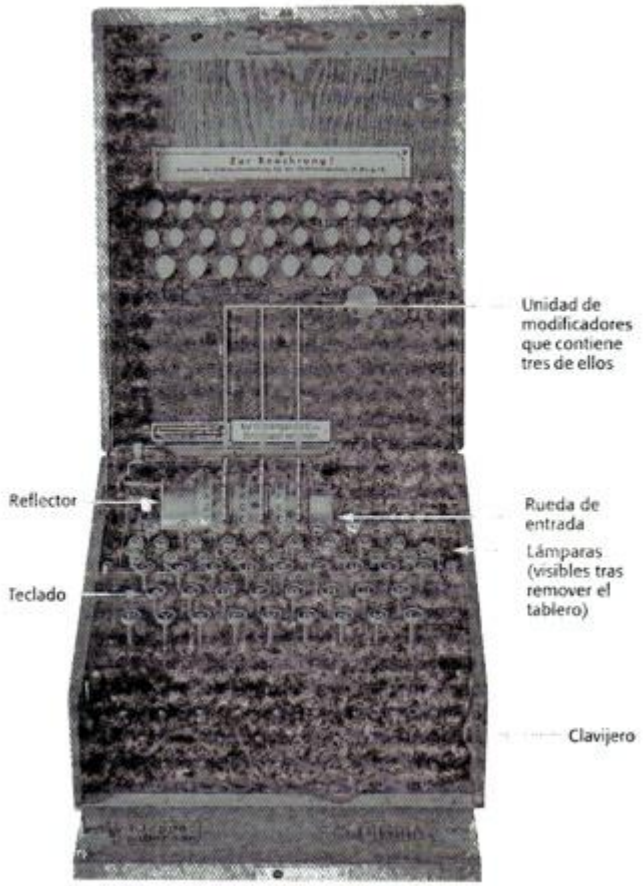


Figura 40. Una máquina Enigma con la cubierta interior abierta, revelando los tres modificadores.

Scherbius creía que la Enigma era inexpugnable y que su fortaleza criptográfica crearía una gran demanda de ella. Intentó promocionar la máquina de cifras tanto para el ejército como para el mundo de los negocios ofreciendo diferentes versiones para cada mercado. Por ejemplo, ofreció una versión básica de la Enigma para los negocios y una versión diplomática de lujo, con impresora en vez de tablero, para el Ministerio de Asuntos Exteriores. El precio de una unidad individual se elevaba al equivalente de más de cinco millones de pesetas en precios de ahora.

Por desgracia, el elevado coste de la máquina desalentó a los compradores potenciales. Las empresas dijeron que no se podían permitir la seguridad de la Enigma, pero Scherbius creía que lo que no podían permitirse era pasar sin ella. Alegó que un mensaje vital interceptado por una empresa rival podía costarle una fortuna a una compañía, pero fueron pocos los hombres de negocios que le hicieron

caso. El ejército alemán mostró la misma ausencia de entusiasmo, porque no era consciente del daño causado por sus cifras poco seguras durante la primera guerra mundial. Por ejemplo, le habían hecho creer que el telegrama Zimmermann había sido robado por espías estadounidenses en México, de modo que culpaban de ese fracaso a la seguridad mexicana. No se daban cuenta de que en realidad el telegrama había sido interceptado y descifrado por los británicos, y que el desastre resultante era realmente un fracaso de la criptografía alemana.

Scherbius no era el único que veía crecer su frustración Otros tres inventores en otros tres países habían tenido, de manera independiente y casi simultáneamente, la idea de crear una máquina de cifras basada en modificadores giratorios. En Holanda, Alexander Koch obtuvo la patente N.° 10.700 en 1919, pero no logró que su máquina de rotores tuviera éxito comercial, y finalmente vendió los derechos de la patente en 1927. En Suecia, Arvid Damm obtuvo una patente similar, pero cuando murió en 1927 aún no había conseguido tampoco encontrar un mercado. En Estados Unidos, el inventor Edward Hebern tenía una fe absoluta en su invento, la denominada Esfinge de la Radio, pero su fracaso fue el mayor de todos.

A mediados de los años veinte, Hebern comenzó a construir una fábrica de 380.000 dólares, pero, desgraciadamente para él, aquél era un período en el que la atmósfera estaba cambiando en Estados Unidos de la paranoia a la apertura. La década anterior, en las secuelas de la primera guerra mundial, el gobierno norteamericano había establecido la Cámara Negra estadounidense, una oficina de cifras altamente eficaz en la que prestaba su servicio un equipo de veinte criptoanalistas, encabezados por el extravagante y brillante Herbert Yardley. Más adelante, Yardley escribiría que «la Cámara Negra, hermética, oculta, resguardada, lo ve todo, lo oye todo. Aunque las persianas están cerradas y las ventanas cuentan también con pesadas cortinas, sus acechantes ojos penetran en las salas de conferencias secretas de Washington, Tokio, Londres, París, Ginebra, Roma.

Sus sensibles oídos captan los susurros más tenues en las capitales extranjeras del mundo». La Cámara Negra estadounidense resolvió 45.000 criptogramas en una década, pero cuando Hebern construyó su fábrica, Herbert Hoover había sido elegido presidente y estaba tratando de entrar en una nueva era de confianza en los asuntos internacionales. Disolvió la Cámara Negra, y su secretario de Estado, Henry

Stimson, declaró que «los caballeros no deberían leer el correo de los demás». Si una nación cree que no está bien leer los mensajes de los demás empieza a creer también que los demás no leerán sus propios mensajes y no ve la necesidad de contar con máquinas de cifras de lujo. Hebern vendió tan sólo doce máquinas a un precio total de unos 1200 dólares, y en 1926 los insatisfechos accionistas lo llevaron a los tribunales, donde fue declarado culpable de acuerdo con la Ley de Garantías Corporativas de California.

Afortunadamente para Scherbius, sin embargo, el ejército alemán llegó a asustarse lo suficiente como para apreciar el valor de la máquina Enigma, gracias a dos documentos británicos. El primero fue *The World Crisis* («La crisis mundial») de Winston Churchill, publicado en 1923, que incluía un dramático relato de cómo los británicos habían obtenido valioso material criptográfico alemán:

A comienzos de septiembre de 1914, el crucero ligero alemán *Magdeburg* naufragó en el Báltico. El cuerpo de un oficial alemán ahogado fue recogido por los rusos algunas horas después y, apretado contra su pecho por los brazos enrigidecidos por la muerte, tenía los libros de claves y señales de la marina alemana, así como mapas minuciosamente milimetrados del mar del Norte y de la ensenada de la isla de Heligoland. El 6 de septiembre, el agregado naval ruso vino a verme. Había recibido un mensaje de Petrogrado diciéndole lo que había sucedido y que el Ministerio de Marina ruso, con la ayuda de los libros de claves y señales, había podido descodificar al menos fragmentos de mensajes navales alemanes. Los rusos pensaron que, siendo el poder naval más importante, el Ministerio de Marina británico debería tener estos libros y mapas. Si enviábamos un navio a Alexandrov, los oficiales rusos a cargo de los libros los enviarían a Inglaterra.

Este material había ayudado a los criptoanalistas de la Sala 40 a descifrar mensajes codificados alemanes regularmente. Finalmente, casi una década después, los alemanes tomaron consciencia de este fracaso en la seguridad de sus comunicaciones. También en 1923, la Marina Real británica publicó su historia oficial de la primera guerra mundial, que reiteraba el hecho de que la interceptación y el criptoanálisis de las comunicaciones alemanas habían dado una clara ventaja a los aliados. Estos espléndidos logros de la Inteligencia británica suponían una marcada condena de los responsables de la seguridad alemana, que tuvieron que admitir

entonces en su propio informe que, «el mando de la flota alemana, cuyos mensajes de radio eran interceptados y descifrados por los ingleses, jugó, como quien dice, con las cartas boca arriba contra el mando británico».

El ejército alemán inició una investigación sobre cómo evitar los fiascos criptográficos de la primera guerra mundial y concluyó que la máquina Enigma ofrecía la mejor solución En 1925 Scherbius comenzó la fabricación en serie de Enigmas, que entraron al servicio del ejército al año siguiente, y que posteriormente fueron utilizadas por organizaciones gubernamentales y estatales como, por ejemplo, los ferrocarriles. Estas Enigmas eran distintas de las pocas máquinas que Scherbius había vendido anteriormente al mundo de los negocios, porque los modificadores tenían cableados internos diferentes. Los dueños de una máquina Enigma comercial, por tanto, no sabían exactamente cómo eran las versiones gubernamentales y militares.

Durante las dos décadas siguientes, el ejército alemán compraría más de 30.000 máquinas Enigma. El invento de Scherbius proporcionó al ejército alemán el sistema de criptografía más seguro del mundo y al estallar la segunda guerra mundial sus comunicaciones estaban protegidas por un nivel de codificación sin precedentes. A veces, pareció que la máquina Enigma tendría un papel vital para asegurar la victoria nazi, pero, en vez de ello, al final formó parte de la perdición de Hitler. Scherbius no vivió lo suficiente para ver los éxitos y los fracasos de su sistema de cifras. En 1929, cuando conducía un equipo de caballos, perdió el control de su carruaje y se estrelló contra una pared, muriendo el 13 de mayo como consecuencia de lesiones internas.

Capítulo 4
El desciframiento de la Enigma

Contenido:

En los años siguientes a la primera guerra mundial, los criptoanalistas británicos de la Sala 40 continuaron vigilando las comunicaciones alemanas. En 1926 comenzaron a interceptar mensajes que los desconcertaron completamente. Había llegado la Enigma, y según aumentaba el número de máquinas Enigma, la habilidad de la Sala 40 para acumular inteligencia disminuyó rápidamente. Los estadounidenses y los franceses intentaron también abordar la cifra Enigma, pero sus tentativas resultaron igualmente deprimentes y no tardaron en abandonar la esperanza de descifrarla. Alemania contaba ahora con las comunicaciones más seguras del mundo.

La velocidad con que los aliados abandonaron la esperanza de descifrar la Enigma contrastaba fuertemente con su perseverancia tan sólo una década antes, durante la primera guerra mundial. Ante la perspectiva de la derrota, los criptoanalistas aliados habían trabajado noche y día para desentrañar las cifras alemanas. Parece ser que el miedo era la principal fuerza de empuje, y que la adversidad es uno de los fundamentos del desciframiento eficaz. De manera similar, fueron el miedo y la adversidad los que hicieron reaccionar a los criptoanalistas franceses a finales del siglo XIX, enfrentados al creciente poder de Alemania. Sin embargo, tras la primera guerra mundial, los aliados ya no temían a nadie. Alemania había sido paralizada por la derrota, los aliados ocupaban la posición dominante, y como consecuencia parecía que habían perdido su entusiasmo criptoanalítico. Los criptoanalistas aliados disminuyeron en número y su calidad se deterioró.

Había una nación, sin embargo, que no se podía permitir relajarse. Después de la primera guerra mundial, Polonia se restableció como estado independiente, pero sentía amenazada su recién adquirida soberanía. Al este tenía a la Unión Soviética, una nación deseosa de extender su comunismo, y al oeste tenía a Alemania,

desesperada por recuperar el territorio que había cedido a Polonia después de la guerra. Encajonada entre estos dos enemigos, los polacos estaban desesperados por obtener información y ampliar su inteligencia, y crearon una nueva oficina de cifras, el Biuro Szyfrów. Si la necesidad es la madre de la invención, entonces quizá la adversidad sea la madre del criptoanálisis. El éxito del Biuro Szyfrów lo ilustran sus éxitos durante la guerra entre la URSS y Polonia de 19191920. Sólo en agosto de 1919, cuando el ejército soviético estaba a las puertas de Varsovia, el Biuro descifró 400 mensajes enemigos. Su vigilancia de las comunicaciones alemanas había sido igualmente efectiva, hasta 1926, cuando también ellos se encontraron con los mensajes de la Enigma.

A cargo de descifrar los mensajes alemanes se encontraba el capitán Maksymilian Ciezki, un comprometido patriota que se había criado en la ciudad de Szamotuty, un centro de nacionalismo polaco. Ciezki tenía acceso a una versión comercial de la máquina Enigma, que revelaba todos los principios del invento de Scherbius. Desgraciadamente, la versión comercial era claramente diferente de la versión militar en cuanto a los cableados internos de cada modificador. Sin conocer los cableados de la máquina militar, Ciezki no tenía ninguna posibilidad de descifrar mensajes enviados por el ejército alemán. Estaba tan desalentado que en un momento dado llegó a emplear a un clarividente en una tentativa frenética de sacar algún sentido de los mensajes codificados interceptados. Pero tampoco el clarividente logró realizar el gran avance que el Biuro Szyfrów necesitaba.

En su lugar, corrió a cargo de un alemán desafecto, Hans-Thilo Schmidt, dar el primer paso hacia el desciframiento de la cifra Enigma.

Hans-Thilo Schmidt había nacido en Berlín en 1888. Era el segundo hijo de un distinguido profesor y su aristocrática esposa. Schmidt emprendió una carrera en el ejército alemán y combatió en la primera guerra mundial, pero no fue considerado merecedor de permanecer en el ejército tras los drásticos recortes implementados como consecuencia del tratado de Versalles. Intentó entonces darse a conocer como hombre de negocios, pero su fábrica de jabón se vio forzada a cerrar a causa de la depresión y la altísima inflación de la posguerra, dejándolos a él y a su familia en la miseria.

La humillación de los fracasos de Schmidt se veía agravada por el éxito de su

hermano mayor, Rudolph, que también había combatido en la guerra, y que pudo permanecer en el ejército tras los recortes. Durante la década de los veinte, Rudolph fue ascendiendo de graduación y finalmente fue nombrado jefe de personal del Cuerpo de Señales. Era el responsable de garantizar la seguridad de las comunicaciones, y de hecho, fue Rudolph quien autorizó oficialmente el empleo de la cifra Enigma en el ejército.

Después del fracaso de sus negocios, Hans-Thilo se vio obligado a pedir ayuda a su hermano, y Rudolph le consiguió un empleo en Berlín, en el Chiffrierstelle, la oficina responsable de administrar las comunicaciones cifradas de Alemania.

Figura 41. Hans-Thilo Schmidt

Era el centro de operaciones de la Enigma, un establecimiento de alto secreto que se ocupaba de la información muy delicada. Cuando Hans-Thilo se trasladó a su nuevo empleo dejó a su familia en Baviera, donde el coste de vida era más

tolerable. Vivía solo en el caro Berlín, empobrecido y aislado, celoso de su perfecto hermano y resentido contra una nación que lo había rechazado.

El resultado era inevitable. Vendiendo información secreta sobre la Enigma a las potencias extranjeras, Hans-Thilo Schmidt podía ganar dinero y vengarse, dañando la seguridad de su país y socavando la organización de su hermano.

El 8 de noviembre de 1931, Schmidt llegó al Grand Hotel de Verviers, Bélgica, para entrar en contacto con un agente secreto francés que se hacía llamar Rex. A cambio de 10.000 marcos (equivalentes a unos 5 millones de pesetas actuales), Schmidt permitió que Rex fotografiase dos documentos: «*Gebrauchsanweisung für die Chiffriermaschine Enigma*» y «*Schlüsselanleitung für die Chiffriermaschine Enigma*». Estos documentos eran instrucciones esenciales para utilizar la máquina Enigma, y aunque no había una descripción explícita de los cableados internos de cada modificador, contenían la información necesaria para deducir esos cableados.

Gracias a la traición de Schmidt, ahora los aliados podían crear una réplica exacta de la máquina Enigma militar alemana. Sin embargo, esto no era suficiente para permitirles descifrar mensajes codificados por la Enigma. La fortaleza de la cifra no depende de mantener secreta la máquina, sino de mantener secreta la disposición inicial de la máquina (la clave). Si un criptoanalista quiere descifrar un mensaje interceptado, además de tener una réplica de la máquina Enigma, aún tiene que descubrir cuál de los millones de billones de claves posibles fue utilizada para codificarlo. Un memorándum alemán lo expresa de esta forma: «Al juzgar la seguridad del criptosistema se asume que el enemigo tiene la máquina a su disposición».

Obviamente, el Servicio Secreto francés estaba a la altura de las circunstancias, pues había conseguido que Schmidt fuera su confidente y había obtenido los documentos que sugerían los cableados de la versión militar de la Enigma. En cambio, los criptoanalistas franceses no daban la talla, pues no parecían ni dispuestos ni capaces de sacar partido a esta información recién adquirida. Tras la primera guerra mundial sufrían de un exceso de autoconfianza y de falta de motivación. El Bureau du Chiffre ni siquiera se molestó en construir una réplica de la versión militar de la Enigma, porque estaban convencidos de que el siguiente paso —encontrar la clave requerida para descifrar un mensaje Enigma concreto— era

imposible.

Pero sucedía que diez años antes Francia había firmado un acuerdo de cooperación militar con Polonia. Los polacos se habían mostrado interesados en todo lo referente a la Enigma, de modo que, cumpliendo su acuerdo de hacía una década, los franceses simplemente entregaron las fotografías de los documentos de Schmidt a sus aliados y dejaron la imposible tarea de descifrar la Enigma en manos del Biuro Szyfrów. El Biuro se dio cuenta de que los documentos eran solamente un punto de partida, pero, a diferencia de los franceses, tenían el miedo de una invasión para servirles de acicate. Los polacos se convencieron de que debía haber un atajo para encontrar la clave de un mensaje codificado con la Enigma y de que si ponían el esfuerzo, el ingenio y la agudeza suficientes podrían encontrar ese atajo.

Además de revelar los cableados internos de los modificadores, los documentos de Schmidt también explicaban detalladamente el diseño de los libros de códigos utilizados por los alemanes. Cada mes, los operadores de la Enigma recibían un nuevo libro de códigos que especificaba qué clave debía usarse para cada día. Por ejemplo, para el primer día del mes, el libro de códigos podía especificar la siguiente clave del día:

1. Posiciones del clavijero:

A/L - P/R - T/D - B/W - K/F - O/Y.

2. Disposición de los modificadores:

2-3-1.

3. Orientación de los modificadores:

Q-C-W.

Juntas, la disposición y la orientación de los modificadores se conocen como las posiciones de los modificadores. Para llevar a la práctica esta clave, el operador de la Enigma dispondría su máquina Enigma de la siguiente manera:

1. Posiciones del clavijero: Intercambia las letras A y L conectándolas con un cable en el clavijero, y haz lo mismo con la P y la R, con la T y la D, con la B y la W, con la K y la F, y con la O y la Y.

2. Disposición de los modificadores: Coloca el 2° modificador en la 1ª ranura de la máquina, el 3.er modificador en la 2ª ranura, y el 1er modificador en la 3ª ranura.

3. Orientación de los modificadores: Cada modificador tiene un alfabeto grabado en su borde externo, que permite que el operador lo sitúe en una orientación particular. En este caso, el operador haría girar el modificador de la 1ª ranura de modo que apareciera la Q, haría girar el modificador de la 2ª ranura hasta que apareciera la C, y haría girar el 3er modificador hasta que apareciera la W.

Una manera de codificar mensajes sería que el emisor codificara todo el tráfico del día de acuerdo a la clave del día. Esto significaría que durante todo un día, al comienzo de cada mensaje todos los operadores de las Enigmas dispondrían sus máquinas según la misma clave del día. Luego, cada vez que hubiera que enviar un mensaje, primero lo teclearían en la máquina; se apuntaría el mensaje codificado resultante y se entregaría al operador de radio para su transmisión. Al otro lado, el operador de la radio receptora anotaría el mensaje entrante, se lo entregaría al operador de la Enigma, que lo teclearía en su máquina, la cual ya estaría dispuesta según la misma clave del día. El mensaje resultante sería el mensaje original.

Este proceso es razonablemente seguro, pero lo debilita el uso repetido de una sola clave del día para codificar los cientos de mensajes que podrían ser enviados cada día. En general, es cierto que si se usa una sola clave para codificar una cantidad enorme de material resulta más fácil que un criptoanalista la deduzca. Una gran cantidad de material codificado de manera idéntica proporciona al criptoanalista una posibilidad igualmente grande de identificar la clave. Por ejemplo, volviendo a las cifras más sencillas, es mucho más fácil descifrar una cifra monoalfabética con el análisis de frecuencia si hay varias páginas de material codificado en vez de un par de frases.

Como precaución adicional, los alemanes dieron el inteligente paso de usar las posiciones de la clave del día para transmitir una nueva *clave de mensaje* para cada mensaje. Las claves de mensaje tenían las mismas posiciones del clavijero y disposición de los modificadores que la clave del día, pero tenían una orientación de

los modificadores diferente. Como la nueva orientación de los modificadores no estaba en el libro de códigos, el emisor tenía que transmitirla de manera segura al receptor según el siguiente proceso. Primero, el emisor dispone la máquina según la clave del día acordada, que incluye una determinada orientación de los modificadores, pongamos por caso QCW. A continuación, escoge al azar una nueva orientación de los modificadores para la clave de mensaje, pongamos por caso PGH. Luego, codifica PGH según la clave del día. La clave de mensaje se teclea en la Enigma dos veces, para proporcionar un control doble al receptor. Por ejemplo, el emisor podría codificar la clave de mensaje PGHPGH como KIVBJE. Nótese que las dos PGH son codificadas de manera diferente (la primera como KIV, la segunda como BJE) porque los modificadores de la Enigma giran después de cada letra, cambiando así el modo general de codificación. Entonces, el emisor cambia su máquina a la disposición PGH y codifica el mensaje propiamente dicho según esta clave de mensaje. Inicialmente, el receptor tiene su máquina dispuesta según la clave del día, QCW Teclea las primeras seis letras del mensaje entrante, KIVBJE, y revelan PGHPGH. Entonces, el receptor sabe que tiene que reajustar sus modificadores a la orientación PGH, la clave de mensaje, y luego puede descifrar el mensaje propiamente dicho.

Esto equivale a que el emisor y el receptor se pongan de acuerdo sobre una clave principal. Luego, en vez de usar esta sola clave principal para codificar cada mensaje la usan meramente para codificar una nueva clave para cada mensaje, y luego codifican el mensaje verdadero según la nueva clave. Si los alemanes no hubieran usado claves de mensaje, entonces todo —quizá miles de mensajes que contenían millones de letras— habría sido enviado utilizando la misma clave del día. Sin embargo, si la clave del día sólo se emplea para transmitir las claves de mensaje, entonces sólo codifica una cantidad limitada de texto. Si se envían 1000 claves de mensaje al día, entonces la clave del día sólo codifica 6000 letras. Y como cada clave de mensaje se elige al azar y sólo se usa para codificar un único mensaje, únicamente codifica una cantidad limitada de texto, quizá sólo unos pocos cientos de caracteres.

A primera vista, este sistema parecía inexpugnable, pero los criptoanalistas polacos permanecieron impertérritos.

Estaban dispuestos a explorar todas las posibilidades para encontrar un punto débil en la máquina Enigma y su empleo de claves del día y de mensaje. En primer plano de la batalla contra la Enigma había una nueva generación de criptoanalistas. Durante siglos, se había asumido que los mejores criptoanalistas eran expertos en la estructura del lenguaje, pero la llegada de la Enigma indujo a los polacos a modificar su política de reclutamiento. La Enigma era una cifra matemática, y el Biuro Szyfrów razonó que una mente más científica podría tener más posibilidades de descifrarla. El Biuro organizó un curso de criptografía e invitó a veinte matemáticos, que individualmente prestaron juramento de guardar secreto. Todos los matemáticos provenían de la Universidad de Poznan. Aunque no se trataba de la institución académica más respetada de Polonia, tenía la ventaja de estar situada al oeste del país, en el territorio que había formado parte de Alemania hasta 1918. Estos matemáticos, por tanto, dominaban el alemán.

Tres de los veinte matemáticos demostraron una aptitud para resolver cifras y fueron reclutados para el Biuro. Entre ellos, el que más talento tenía era Marian Rejewski, un muchacho de veintitrés años, tímido y con gafas, que anteriormente había estudiado estadística con la intención de hacer carrera en el campo de los seguros. Aunque era un buen estudiante en la universidad, fue en el seno del Biuro Szyfrów donde encontró su verdadera vocación. Hizo su aprendizaje descifrando una serie de cifras tradicionales antes de pasar al desafío más severo de la Enigma. Trabajando totalmente solo, concentró toda su energía en la complejidad de la máquina de Scherbius. Como matemático, trataba de analizar cada aspecto del funcionamiento de la máquina, investigando el efecto de los modificadores y de los cables del clavijero. Sin embargo, como sucede con todos los matemáticos, su trabajo requería inspiración además de lógica. Como dijo otro criptoanalista matemático del tiempo de la guerra, el descifrador creativo debe «*forzosamente vivir diariamente en íntima comunión con espíritus oscuros para llevar a cabo sus proezas de jiu-jitsu mental*».

La estrategia de Rejewski para atacar la Enigma se centró en el hecho de que la repetición es el enemigo de la seguridad: la repetición conduce a patrones y es el arma favorita de los criptoanalistas. La repetición más obvia de la codificación de la Enigma era la clave de mensaje, que era codificada dos veces al principio de cada

mensaje. Si el operador elegía la clave de mensaje ULJ, la codificaría dos veces, de modo que ULJULJ podría ser codificado como PEFNWZ, que luego enviaría al comienzo, antes del mensaje verdadero. Los alemanes habían exigido la repetición para evitar errores causados por las intermitencias de radio o fallos del operador. Pero no previeron que esto pondría en peligro la seguridad de la máquina.

Cada día, Rejewski se encontraba ante una nueva remesa de mensajes interceptados. Todos ellos comenzaban con las seis letras de la clave de mensaje de tres letras repetida, que estaban codificadas según la clave del día acordada. Por ejemplo, podría recibir cuatro mensajes que comenzaban con las siguientes claves de mensaje codificadas:

	1ª	2ª	3ª	4ª	5ª	6ª
1er mensaje	L	O	K	R	G	M
2do mensaje	M	V	T	X	Z	E
3er mensaje	J	K	T	M	P	E
4º mensaje	D	V	Y	P	Z	X

En cada caso, las letras 1ª y 4ª son codificaciones de la misma letra, a saber la primera letra de la clave de mensaje. También las letras 2ª y 5ª son codificaciones de la misma letra, a saber la segunda letra de la clave de mensaje, y las letras 3ª y 6ª son codificaciones de la misma letra, a saber la tercera letra de la clave de mensaje. Por ejemplo, en el primer mensaje L y R son codificaciones de la misma letra, la primera letra de la clave de mensaje. La razón por la que la misma letra está codificada de manera diferente, primero como L y luego como R, es que entre las dos codificaciones el primer modificador de la Enigma se ha movido tres veces, cambiando el modo general de codificación.

El hecho de que L y R sean codificaciones de la misma letra permitió a Rejewski deducir una ligera limitación en la disposición inicial de la máquina. La posición inicial de los modificadores, que nos es desconocida, codificó la primera letra de la clave del día, que también nos es desconocida, como L, y luego, otra posición de los modificadores, tres posiciones por delante de la posición inicial, que aún desconocemos, codificó la misma letra de la clave del día, que también seguimos sin

conocer, como R.

La limitación puede parecer vaga, porque está llena de factores desconocidos, pero al menos demuestra que las letras L y R están íntimamente relacionadas por la posición inicial de la máquina Enigma, la clave del día. Según se van interceptando nuevos mensajes, es posible identificar otras relaciones entre las letras 1ª y 4ª de la clave de mensaje repetida. Todas estas relaciones son reflejos de la posición inicial de la máquina Enigma. Por ejemplo, el segundo mensaje del cuadro anterior nos dice que M y X están relacionadas, el tercero nos dice que J y M están relacionadas y el cuarto que D y P están relacionadas.

Figura 42. Marian Rejewski.

Rejewski comenzó a compendiar estas relaciones clasificándolas en tablas. Para los cuatro mensajes que tenemos hasta ahora, la tabla reflejaría las relaciones entre (L-R), (M-X), (J-M) y (D-P)

1.ª letra	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
4.ª letra					P								M					R	X							

Si Rejewski tenía acceso a suficientes mensajes en un solo día podría completar el alfabeto de relaciones. La siguiente tabla muestra semejante juego completo de relaciones:

1.ª letra	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
4.ª letra	F	Q	H	P	L	W	O	G	B	M	V	R	X	U	Y	C	Z	I	T	N	J	E	A	S	D	K

Rejewski no tenía ni idea de la clave del día, así como tampoco de las claves de mensaje elegidas, pero sabía que daban como resultado esta tabla de relaciones. Si la clave del día hubiera sido diferente, la tabla de relaciones también habría sido completamente diferente. La siguiente cuestión era si existía alguna manera de determinar la clave del día observando la tabla de relaciones. Rejewski comenzó a buscar patrones dentro de la tabla, estructuras que pudieran indicar la clave del día. Finalmente, comenzó a estudiar un tipo de patrón en particular, que presentaba cadenas de letras. Por ejemplo, en la tabla anterior, la A de la fila superior está ligada a la F de la fila inferior, de modo que luego buscaríamos la F en la fila superior. Resulta que la F está ligada a la W, de modo que buscaríamos la W en la fila superior. Y resulta que la W está ligada a la A, que es donde empezamos. La cadena se ha completado.

Con las restantes letras del alfabeto, Rejewski generaría más cadenas. Hizo una lista de todas las cadenas y anotó el número de conexiones de cada una:

A → F → W → A ➔3 conexiones

B → Q → Z → K → V → E → L → R → M ➔ 9 conexiones

C → H → G → O → Y → D → P → C ➔ 7 conexiones

J → M → X → S → T → N → U → J ➔ 7 conexiones

Hasta ahora, sólo hemos considerado las conexiones entre las letras 1ª y 4ª de las seis letras de la clave repetida. En realidad, Rejewski repetiría todo este ejercicio con las relaciones entre las letras 2ª y 5ª, y las letras 3ª y 6ª, identificando las cadenas en cada caso y el número de conexiones en cada cadena.

Rejewski se dio cuenta de que las cadenas cambiaban cada día. A veces había muchos tipos de cadenas, y otras sólo unas pocas cadenas largas. Y, por supuesto, las letras de las cadenas cambiaban. Las características de las cadenas eran claramente el resultado de la posición de la clave del día: una compleja secuencia de las posiciones del clavijero, la disposición de los modificadores y la orientación de los modificadores. Sin embargo, permanecía la cuestión de cómo podía Rejewski determinar la clave del día partiendo de estas cadenas. ¿Cuál de las 10.000.000.000.000.000 claves del día posibles se relacionaba con un patrón concreto de las cadenas? El número de posibilidades era sencillamente demasiado grande.

Fue entonces cuando Rejewski tuvo una profunda inspiración Aunque tanto las posiciones del clavijero como las de los modificadores afectan los detalles de las cadenas, sus respectivas contribuciones se pueden distinguir en cierta medida. En particular, hay un aspecto de las cadenas que depende enteramente de la posición de los modificadores y que no tiene nada que ver con las posiciones del clavijero: el número de conexiones de las cadenas es puramente una consecuencia de la posición de los modificadores. Por ejemplo, tomemos el ejemplo anterior y supongamos que la clave del día requería que las letras S y G fueran intercambiadas como parte de las posiciones del clavijero. Si cambiamos este elemento de la clave del día, quitando el cable que intercambia la S y la G, y en vez de ello lo usamos para intercambiar, pongamos por caso, la T y la K, las cadenas se modificarían de la siguiente manera:

A → F → W → A ➔ 3 conexiones

B ➔ Q ➔ Z ➔ T ➔ V ➔ E ➔ L ➔ R ➔ I ➔ E ➔ 9 conexiones

C → H → G → O → Y → D → P → C ➔ 7 conexiones

J → M → X → G → K → N → U → J ➔ 7 conexiones

Algunas de las letras de las cadenas han cambiado, pero, crucialmente, el número de conexiones de cada cadena permanece constante. Rejewski había identificado una faceta de las cadenas que era exclusivamente un reflejo de la posición de los modificadores.

El número total de posiciones de los modificadores es el número de disposiciones de los modificadores (6) multiplicado por el número de orientaciones de los modificadores (17.576), que se eleva a 105.456. De modo que, en vez de tener que preocuparse sobre cuál de las 10.000.000.000.000.00 claves del día se asociaba con un juego de cadenas en particular, Rejewski podía ocuparse de un problema drásticamente más sencillo: ¿cuál de la 105.456 posiciones de los modificadores se asociaba con el número de conexiones en un juego de cadenas? Este número todavía es elevado, pero es aproximadamente cien mil millones de veces menor que el número total de claves del día posibles. Resumiendo, la tarea se había vuelto cien mil millones de veces más fácil, y sin duda estaba dentro del alcance de las posibilidades humanas.

Rejewski procedió de la siguiente manera. Gracias al espionaje de Hans- Thilo Schmidt, tenía acceso a réplicas de la máquina Enigma. Su equipo comenzó la laboriosa tarea de probar cada una de las 105.456 posiciones de los modificadores, catalogando la longitud de las cadenas generadas por cada una de ellas. Les costó un año entero completar el catálogo, pero una vez que el Biuro había acumulado los datos, Rejewski pudo finalmente comenzar desentrañar la cifra Enigma.

Cada día observaba las claves de mensaje codificadas, las seis primeras letras de todos los mensajes interceptados, y usaba la información para desarrollar su tabla de relaciones. Esto le permitía trazar las cadenas y establecer el número de conexiones de cada cadena. Por ejemplo, el análisis de las letras 1ª y 4ª podría resultar en cuatro cadenas con 3, 9, 7 y 7 conexiones. El análisis de las letras 2ª y 5ª podría resultar también en cuatro cadenas, con 2, 3, 9 y 12 conexiones. El análisis de las letras 3ª y 6ª podría resultar en cinco cadenas, con 5, 5, 5, 3 y 8

conexiones. Rejewski aún no tenía ni idea de la clave del día, pero sabía que resultaba en 3 juegos de cadenas con el siguiente número de cadenas y de conexiones en cada uno:

- 4 cadenas de las letras 1ª y 4ª, con 3, 9, 7 y 7 conexiones.
- 4 cadenas de las letras 2ª y 5ª, con 2, 3, 9 y 12 conexiones.
- 5 cadenas de las letras 3ª y 6ª, con 5, 5, 5, 3 y 8 conexiones.

Rejewski podía acudir ahora a su catálogo, que contenía un índice de todas las posiciones de los modificadores según el tipo de cadenas que generaban. Una vez encontrada la entrada del catálogo que contenía el número correcto de cadenas con el número apropiado de conexiones en cada una, Rejewski conocía inmediatamente las posiciones de los modificadores para esa clave del día concreta. Las cadenas funcionaban de hecho como huellas dactilares, la evidencia que delataba las disposiciones y orientaciones iniciales de los modificadores. Rejewski estaba trabajando como un detective que encuentra una huella dactilar en la escena del crimen y utiliza una base de datos para ver a qué sospechoso corresponde.

Aunque había identificado la parte de la clave del día concerniente a los modificadores, Rejewski aún tenía que establecer las posiciones del clavijero. A pesar de que había alrededor de cien mil millones de posibilidades para las posiciones del clavijero, ésta era una tarea relativamente sencilla.

Rejewski empezaba colocando los modificadores de su réplica de la Enigma según la recién establecida parte de la clave del día concerniente a los modificadores. Luego, retiraba todos los cables del clavijero, de modo que el clavijero no tuviera ningún efecto. Finalmente, tomaba un fragmento de texto cifrado interceptado y lo tecleaba en la máquina Enigma. En su mayor parte, esto resultaba un galimatías porque se desconocían y, por tanto, faltaban las posiciones de los cables del clavijero. Sin embargo, alguna que otra vez aparecían frases vagamente reconocibles, como alliveinbelrin, probablemente, esto debía ser *«arrive in Berlín»* («llega a Berlín»), Si esta suposición era correcta, implicaría que las letras R y L deberían estar conectadas e intercambiadas por un cable del clavijero, mientras que A, I, V, E, B y N no deberían estarlo. Analizando otras frases sería posible identificar los otros seis pares de letras que habían sido intercambiadas por el clavijero. Como ya había des

cubierto las posiciones de los modificadores, al establecer las posiciones del clavijero, Rejewski tenía la clave del día completa y podía descifrar cualquier mensaje enviado ese día.

Rejewski había simplificado enormemente la tarea de encontrar la clave del día separando el problema de encontrar las posiciones de los modificadores del problema de encontrar las posiciones del clavijero. Separados, estos problemas eran solubles. Inicialmente, estimamos que costaría más tiempo que la edad del universo probar todas las claves posibles de la Enigma. Sin embargo, Rejewski había pasado sólo un año recopilando su catálogo de longitudes de cadena y después de eso podía encontrar la clave del día antes de que acabara el día. Una vez que tenía la clave del día poseía la misma información que el receptor a quien iba dirigido el mensaje y, por tanto, podía descifrar los mensajes con la misma facilidad.

Después del gran avance de Rejewski, las comunicaciones alemanas se volvieron transparentes. Polonia no estaba en guerra con Alemania, pero existía el peligro de una invasión, y el alivio de los polacos al conquistar la Enigma fue inmenso. Si podían descubrir qué planes tenían los generales alemanes respecto a Polonia, existía una posibilidad de poder defenderse. El destino de la nación polaca había dependido de Rejewski, y él no defraudó a su país. El ataque a la Enigma realizado por Rejewski es uno de los logros verdaderamente grandes del criptoanálisis. He tenido que resumir su trabajo en unas pocas páginas, por lo que he omitido muchos de los detalles técnicos y todos los callejones sin salida. La Enigma es una máquina de cifras complicada, y descifrarla requirió una fuerza intelectual inmensa. Confío que mis simplificaciones no lleven al lector al error de subestimar el extraordinario logro de Rejewski.

El éxito polaco de descifrar la Enigma se puede atribuir a tres factores: el miedo, las matemáticas y el espionaje. Sin el miedo a la invasión, los polacos se habrían desalentado ante la aparente invulnerabilidad de la cifra de la Enigma. Sin las matemáticas, Rejewski no habría sido capaz de analizar las cadenas. Y sin Schmidt, cuyo sobrenombre era «Asche», y sus documentos, no se habrían conocido los cableados de los modificadores, y los criptoanalistas ni siquiera habrían podido empezar. Rejewski no dudó en expresar todo lo que debía a Schmidt: «Los documentos de Asche fueron bienvenidos como maná del cielo, y todas las puertas

se abrieron inmediatamente».

Los polacos utilizaron con éxito la técnica de Rejewski durante varios años. Cuando Hermann Göring visitó Varsovia en 1934, no era en absoluto consciente del hecho de que todas sus comunicaciones estaban siendo interceptadas y descifradas. Mientras él y otros dignatarios alemanes depositaban una corona de flores en la tumba del Soldado Desconocido al lado de las oficinas del Biuro Szyfrów, Rejewski podía verlos desde su ventana, satisfecho de saber que podía leer sus comunicaciones más secretas.

Incluso cuando los alemanes modificaron ligeramente la manera en que transmitían mensajes, Rejewski contraatacó. Su viejo catálogo de longitudes de cadena ya no tenía ninguna utilidad, pero en vez de volver a componer el catálogo inventó una versión mecanizada de su sistema de catalogación, que podía buscar automáticamente las posiciones correctas de los modificadores. El invento de Rejewski era una adaptación de la máquina Enigma, capaz de probar rápidamente cada una de las 17.576 posiciones hasta descubrir la que encaja. A causa de las seis disposiciones posibles de los modificadores era necesario tener seis de las máquinas de Rejewski trabajando en paralelo: cada una de ellas representaba una de las posibles disposiciones. Juntas, formaban una unidad que medía alrededor de un metro de altura, y que era capaz de encontrar la clave del día en unas dos horas. Las unidades se llamaban *bombas,* un nombre que quizá reflejara el tictac que hacían mientras probaban las posiciones de los modificadores. Otra versión afirma que a Rejewski le vino la inspiración de las máquinas cuando estaba en una cafetería comiendo una *bomba*, un helado con forma de hemisferio. Las *bombas* mecanizaron eficazmente el proceso de desciframiento. Era una respuesta natural a la Enigma, que era una mecanización de la codificación.

Durante la mayor parte de la década de los treinta, Rejewski y sus colegas trabajaron infatigablemente para revelar las claves de la Enigma. Mes tras mes, el equipo se enfrentaba al estrés y a la tensión del criptoanálisis, teniendo que solucionar continuamente las averías mecánicas de las *bombas*, enfrentándose constantemente al inacabable suministro de mensajes codificados interceptados. Sus vidas llegaron a estar dominadas por la busca de la clave del día, la pieza vital de información que revelaría el significado de los mensajes cifrados. Sin embargo, lo

que los descifradores polacos desconocían era que gran parte de su trabajo era innecesario. El jefe del Biuro, el comandante Gwido Langer, ya tenía las claves del día de la Enigma, pero las mantenía escondidas, guardadas en su escritorio.

Langer, a través de los franceses, aún recibía información de Schmidt. Las inicuas actividades del espía alemán no finalizaron en 1931 con la entrega de dos documentos sobre el funcionamiento de la Enigma, sino que continuaron durante otros siete años. Se reunió con el agente secreto francés Rex en veinte ocasiones, a menudo en aislados chalés alpinos en los que la privacidad estaba garantizada. En cada reunión, Schmidt entregaba al menos un libro de códigos, cada uno de los cuales contenía las claves del día de todo un mes. Se trataba de los libros de códigos que se distribuían a todos los operadores de la Enigma alemanes y contenían toda la información necesaria para codificar y decodificar mensajes. En total, proporcionó libros de códigos que contenían las claves del día para 38 meses. Las claves le habrían ahorrado a Rejewski una cantidad enorme de tiempo y de esfuerzo, atajando la necesidad de disponer de *bombas*, y ahorrando mano de obra que podía haber sido empleada en otras secciones del Biuro. Sin embargo, el extraordinariamente astuto Langer decidió no decirle a Rejewski que existían las claves. Privando a Rejewski de las claves, Langer creía que lo estaba preparando para el tiempo inevitable en que las claves ya no estuvieran disponibles. Sabía que si estallaba la guerra a Schmidt le resultaría imposible acudir a reuniones secretas, y entonces Rejewski se vería obligado a ser autosuficiente. Lange pensó que Rejewski debía practicar la autosuficiencia en tiempos de paz, como preparación para lo que se avecinaba.

Disposiciones con tres modificadores	Disposiciones adicionales disponibles con dos modificadores extra
123	124 125 134 135 142 143 145 152 153
132	154 214 215 234 235 241 243 245 251
213	253 254 314 315 324 325 341 342 345
231	351 352 354 412 413 415 421 423 425
312	431 432 435 451 452 453 512 513 514
321	521 523 524 531 532 534 541 542 543

Tabla 10. Disposiciones posibles con cinco modificadores.

La habilidad de Rejewski llegó a su límite en diciembre de 1938, cuando los criptógrafos alemanes aumentaron la seguridad de la Enigma. A todos los operadores de la Enigma se les dio dos nuevos modificadores, para que su disposición pudiera afectar a tres cualquiera de los cinco modificadores disponibles. Anteriormente sólo había tres modificadores (llamados 1,2 y 3) entre los que elegir, y sólo seis maneras de disponerlos, pero ahora que había otros dos modificadores (llamados 4 y 5) entre los que elegir, el número de disposiciones aumentó a 60, tal como se muestra en la Tabla 10. El primer desafío de Rejewski era calcular los cableados internos de los dos nuevos modificadores. Lo que era todavía más preocupante era que también tenía que construir diez veces más de *bombas,* para que cada una representara una disposición diferente de los modificadores. El mero coste de construir semejante cantidad de bombas equivalía a quince veces el presupuesto entero anual para equipo del Biuro. El siguiente mes, la situación empeoró cuando el número de cables del clavijero aumentó de seis a diez. En vez de intercambiarse doce letras antes de entrar en los modificadores, ahora había veinte letras intercambiadas. El número de claves posibles ascendió a 159.000.000.000.000.000.000.

En 1938, las interceptaciones y decodificaciones polacas habían estado en su punto álgido, pero para comienzos de 1939 los nuevos modificadores y los cables adicionales del clavijero frenaron el flujo de inteligencia. Rejewski, que había extendido los límites del criptoanálisis en los años anteriores, se sentía contuso. Había demostrado que la Enigma no era una cifra indescifrable, pero sin los medios necesarios para probar cada posición de los modificadores no podía descubrir la clave del día y la decodificación era imposible. En circunstancias tan desesperadas, Langer podría haber sentido la tentación de entregarle las claves que había obtenido Schmidt, pero esas claves no estaban siendo entregadas. Justo antes de la introducción de los nuevos modificadores, Schmidt había roto el contacto con el agente Rex. Durante siete años había proporcionado claves que eran superfluas a causa de la innovación polaca. Ahora, justo cuando los polacos necesitaban las claves, ya no estaban disponibles.

La nueva invulnerabilidad de la Enigma fue un golpe devastador para Polonia,

porque la Enigma no era meramente un medio de comunicación, era el núcleo de la estrategia *blitzkrieg* de Hitler. El concepto de *blitzkrieg* («guerra relámpago») implicaba un ataque rápido, intenso, coordinado, lo que significaba que grandes divisiones de tanques tenían que comunicarse entre sí y con la infantería y la artillería. Además, las fuerzas terrestres eran respaldadas por el refuerzo aéreo de los aviones Stuka de bombardeo en picado, lo que dependía de la comunicación efectiva y segura entre las tropas en primera línea de combate y los campos de aviación.

Figura 43. El vehículo del puesto de mando del general Heinz Guderian. En la parte inferior izquierda se puede ver una máquina Enigma en acción.

El carácter distintivo del *blitzkrieg* era «velocidad del ataque mediante la velocidad de las comunicaciones». Si los polacos no podían descifrar la Enigma, no tenían ninguna esperanza de detener el violento ataque alemán, que obviamente iba a

producirse en cuestión de unos pocos meses. Alemania ya había ocupado los Sudetes, y el 27 de abril de 1939 se desdijo de su tratado de no agresión con Polonia.

La retórica antipolaca de Hitler fue volviéndose cada vez más virulenta. Langer estaba resuelto a que, si Polonia era invadida, sus avances criptoanalíticos, hasta entonces secretos al no haber sido comunicados a los aliados, no deberían perderse. Si Polonia no podía beneficiarse del trabajo de Rejewski, al menos los aliados deberían tener la oportunidad de tratar de usarlos para seguir avanzando. Quizá Inglaterra y Francia, que contaban con más medios, podrían sacar el mayor partido al concepto de la *bomba.*

El 30 de junio, el comandante Langer telegrafió a sus homólogos franceses y británicos invitándolos a Varsovia para tratar asuntos urgentes referentes a la Enigma. El 24 de julio, un grupo de experimentados criptoanalistas franceses y británicos llegó a la sede del Biuro, sin saber realmente qué esperar. Langer los hizo pasar a una habitación en la que había un objeto cubierto con una tela negra. Retiró la tela, revelando de esta manera tan espectacular una de las *bombas* de Rejewski. La audiencia quedó atónita al oír cómo Rejewski había estado descifrando la Enigma durante años. Los polacos llevaban una década de ventaja al resto del mundo.

Los franceses quedaron particularmente atónitos, porque el trabajo polaco se había basado en los resultados del espionaje francés. Los franceses habían pasado la información de Schmidt a los polacos porque creían que no tenía ningún valor, pero los polacos les habían probado que no estaban en lo cierto.

Como sorpresa final, Langer ofreció a los británicos y a los franceses dos réplicas de la Enigma de repuesto y planos para construir las *bombas*, que se enviarían a París en valijas diplomáticas. De ahí, el 16 de agosto una de las máquinas Enigma siguió camino a Londres. Fue pasada a escondidas por el canal como parte del equipaje del dramaturgo Sacha Guitry y su esposa, la actriz Yvonne Printemps, para no despertar las sospechas de los espías alemanes que estarían vigilando el puerto. Dos semanas después, el 1 de septiembre, Hitler invadió Polonia y comenzó la guerra.

1. Los gansos que nunca cacareaban

Durante trece años, los británicos y los franceses habían asumido que la cifra Enigma era indescifrable, pero ahora había esperanza. Las revelaciones polacas habían demostrado que esta cifra tenía fallos, lo que levantó la moral de los criptoanalistas aliados. Los progresos polacos se habían interrumpido con la introducción de nuevos modificadores y cables extra del clavijero, pero seguía siendo un hecho que la Enigma ya no era considerada una cifra perfecta.

Los avances polacos habían demostrado a los aliados el valor de emplear a matemáticos como descifradores. En el Reino Unido, la Sala 40 había estado dominada por lingüistas y clasicistas, pero ahora existía un esfuerzo concertado para equilibrar el personal con matemáticos y científicos. Los reclutaron en gran parte a través de la red de antiguos compañeros de la universidad: los que trabajaban en la Sala 40 se pusieron en contacto con sus antiguos *colleges* de Oxford o Cambridge. También había una red de antiguas compañeras que reclutaba estudiantes universitarias de lugares como Newnham College y Girton College, de Cambridge.

Figura 44. En agosto de 1939 los descifradores británicos visitaron Bletchley Park para evaluar su conveniencia como sede de la nueva Escuela Gubernamental de Códigos y Cifras. Para no levantar sospechas entre los vecinos, dijeron que formaban parte de la cacería del capitán Ridley.

A los nuevos miembros no se les llevaba a la Sala 40 de Londres, sino a Bletchley

Park, en Buckinghamshire, la sede de la Government Code and Cypher School (GC&CS, Escuela Gubernamental de Códigos y Cifras), una organización de descodificación recién fundada que estaba sustituyendo a la Sala 40. Bletchley Park podía albergar a mucho más personal, lo que era importante, ya que se esperaba un diluvio de mensajes cifrados interceptados en cuanto empezara la guerra.

Durante la primera guerra mundial, Alemania había transmitido dos millones de palabras al mes, pero se preveía que la mayor disponibilidad de las radios en la segunda guerra mundial podría resultar en la transmisión de dos millones de palabras al día.

En el centro de Bletchley Park había una gran mansión victoriana de estilo gótico-Tudor, construida por el financiero del siglo XIX *sir* Herbert León. La mansión, con su biblioteca, salón comedor y su ornado salón de baile, proporcionó la administración central para toda la operación Bletchley. El comandante Alastair Denniston, el director de la GC&CS, tenía una oficina en la planta baja, que daba a los jardines, una vista que no tardó en ser afeada por la construcción de numerosos cobertizos. Estas improvisadas construcciones de madera albergaron las diversas actividades de descodificación. Por ejemplo, el Cobertizo 6 se especializaba en atacar las comunicaciones por Enigma del ejército alemán, pasando sus desciframientos al Cobertizo 3, donde operarios de inteligencia traducían los mensajes y trataban de sacar partido a la información. El Cobertizo 8 se especializaba en la Enigma naval, y pasaba sus desciframientos al Cobertizo 4 para su traducción y acumulación de inteligencia. Inicialmente, Bletchley Park tenía un personal de sólo doscientas personas, pero en cinco años la mansión y los cobertizos llegarían a albergar a setecientos hombres y mujeres.

Durante el otoño de 1939, los científicos y matemáticos de Bletchley se familiarizaron con las intrincadas características de la cifra Enigma y dominaron rápidamente las técnicas polacas. Bletchley contaba con más personal y más medios que el Biuro Szyfrów polaco y, por tanto, era capaz de hacer frente a un surtido mayor de modificadores y al hecho de que la Enigma fuera ahora diez veces más difícil de descifrar. Cada veinticuatro horas, los descifradores británicos desempeñaban la misma rutina. A medianoche, los operadores alemanes de la Enigma cambiaban a una nueva clave del día. A partir de ese momento,

cualesquiera que fueran los avances que Bletchley hubiera realizado el día anterior ya no se podían utilizar para descifrar mensajes. Los descifradores tenían que empezar ahora la tarea de intentar identificar la nueva clave del día. Podía costar varias horas, pero en cuanto descubrían las disposiciones de la Enigma para ese día, el personal de Bletchley podía empezar a descifrar los mensajes alemanes que ya había acumulado, revelando información sumamente valiosa para el esfuerzo de la guerra.

La sorpresa es un arma valiosísima con la que puede contar un comandante. Pero si Bletchley conseguía descifrar la Enigma, los planes alemanes se volverían transparentes y los británicos podrían leer la mente del Alto Mando alemán. Si los británicos podían recoger noticias de un ataque inminente, enviarían refuerzos o realizarían maniobras evasivas. Si podían descifrar las discusiones alemanas sobre sus propios puntos débiles, los aliados podían enfocar sus ofensivas. Los desciframientos de Bletchley tenían una importancia máxima. Por ejemplo, cuando Alemania invadió Dinamarca y Noruega en abril de 1940, Bletchley proporcionó una imagen detallada de las operaciones alemanas. De manera similar, durante la batalla de Inglaterra, los criptoanalistas fueron capaces de advertir de los bombardeos con antelación, incluyendo las horas y los lugares. También podían dar informes puestos al día del estado de la Luftwaffe (aviación alemana), como el número de aviones que habían perdido y la velocidad con la que estaban siendo reemplazados. Bletchley enviaba toda esta información a la sede central del MI6 (Inteligencia británica), que la remitía a la Oficina de Guerra, el Ministerio del Aire y el Ministerio de Marina.

Además de influir en el curso de la guerra, de vez en cuando los criptoanalistas encontraban ratos para relajarse. Según Malcolm Muggeridge, que trabajaba para el servicio secreto y visitó Bletchley, el rounders[13] era el pasatiempo favorito:

Cada día después de comer, cuando el clima lo permitía, los descifradores jugaban *rounders* en el césped de la casa, adoptando la actitud cuasiseria que los profesores afectan cuando se dedican a actividades que pueden ser consideradas como frívolas o insignificantes en comparación con sus estudios más serios. Así, disputaban algún punto del juego con el mismo fervor con que podrían hacerlo sobre la cuestión del

[13] Rounders: juego parecido al béisbol. (N. del T.)

libre albedrío o el determinismo, o si el mundo comenzó con un big bang o un proceso de creación continua.

Una vez que habían dominado las técnicas polacas, los criptoanalistas de Bletchley comenzaron a inventar sus propios atajos para descubrir las claves de la Enigma. Por ejemplo, se percataron del hecho que los operadores alemanes de la Enigma de vez en cuando elegían claves de mensajes obvias.

Para cada mensaje se suponía que el operador elegía una clave de mensaje diferente, tres letras escogidas al azar. Sin embargo, en el calor de la batalla, en vez de forzar su imaginación para elegir una clave al azar, los agotados operadores a veces tomaban tres letras consecutivas del teclado de la Enigma (Figura 46), como, por ejemplo, QWE o BNM Estas claves de mensaje previsibles empezaron a ser conocidas como *cillis.* Otro tipo de *cilli* era el uso repetido de la misma clave de mensaje, quizá las iniciales de la novia del operador; de hecho, un juego semejante de iniciales, C.I.L., puede haber sido el origen del término. Antes de descifrar la Enigma de la manera difícil se convirtió en rutina que los criptoanalistas probaran los *cillis,* y a veces sus corazonadas valían la pena.

Figura 45. Los descifradores de Bletchley se relajan jugando al rounders.

Los *cillis* no eran puntos débiles de la máquina Enigma, sino más bien se trataba de debilidades en la manera en que se usaba la máquina. El error humano a niveles

superiores también comprometió la seguridad de la cifra Enigma. Los responsables de redactar los libros de códigos tenían que decidir qué modificadores serían usados cada día y en qué posiciones. Trataron de asegurarse que las disposiciones de los modificadores fueran imprevisibles no permitiendo que ningún modificador permaneciera en la misma posición dos días seguidos. Así, si denominamos 1, 2, 3, 4 y 5 a los modificadores, el primer día sería posible tener la disposición 1 - 3 - 4, y el segundo día sería posible tener 2 - 1 - 5, pero no 2 -1 - 4, porque no se permite que el modificador número 4 permanezca en la misma posición dos días seguidos. Esto podría parecer una estrategia sensata, porque los modificadores están continuamente cambiando de posición, pero el cumplimiento de una regla semejante facilita muchísimo la labor del criptoanalista. Excluir ciertas disposiciones para evitar que un modificador permanezca en la misma posición significaba que los redactores del libro de códigos redujeron a la mitad el número de posibles disposiciones de los modificadores. Los criptoanalistas de Bletchley se dieron cuenta de lo que sucedía y le sacaron el mayor partido. En cuanto identificaban la disposición de los modificadores para un día inmediatamente podían descartar la mitad de las disposiciones de los modificadores para el día siguiente. De esta manera, su trabajo se reducía a la mitad.

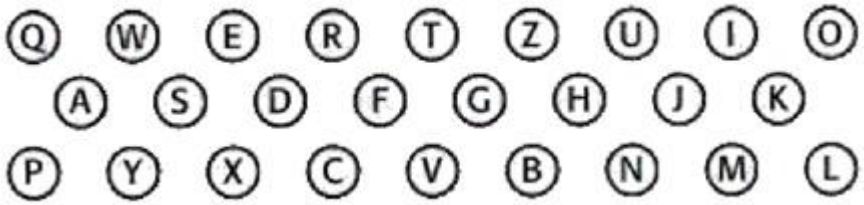


Figura 46. Disposición del teclado de la Enigma

De forma similar, había una regla que impedía que las posiciones del clavijero incluyeran el intercambio entre cualquier letra y su vecina en el alfabeto, lo que significaba que la S podía ser intercambiada con cualquier letra excepto la R y la T. La teoría era que semejantes intercambios obvios debían ser evitados deliberadamente pero, de nuevo, el cumplimiento de una regla redujo drásticamente el número de claves posibles.

Esta búsqueda de nuevos atajos criptoanalíticos era necesaria porque la máquina Enigma continuó evolucionando durante el curso de la guerra. Los criptoanalistas se veían forzados continuamente a innovar, a rediseñar y refinar las *bombas*, y a inventar estrategias completamente nuevas. Parte de la razón de su éxito era la rarísima combinación de matemáticos, científicos, lingüistas, clasicistas, grandes maestros del ajedrez y adictos a los crucigramas dentro de cada cobertizo. Un problema complejo iría pasando por el cobertizo hasta llegar a alguien que tenía las herramientas mentales idóneas para resolverlo, o hasta llegar a alguien que al menos podía resolverlo parcialmente antes de hacerlo pasar de nuevo.

Gordon Welchman, que estaba a cargo del Cobertizo 6, describió a su equipo como «una manada de perros de caza tratando de captar el olor». Hubo muchos grandes criptoanalistas y muchos avances significativos, y se necesitarían varios grandes tomos para describir detalladamente las contribuciones individuales. Sin embargo, si hay una figura que merece una mención particular es Alan Turing, que identificó el punto débil más importante de la Enigma y le sacó partido implacablemente. Gracias a Turing, se hizo posible descifrar la cifra Enigma incluso en las circunstancias más difíciles.

Alan Turing fue concebido en otoño de 1911 en Chatrapur, una ciudad cercana a Madrás, en el sur de India, donde su padre, Julius Turing, era miembro de la administración pública india. Julius y su esposa, Ethel, estaban decididos a que su hijo naciera en Gran Bretaña, y volvieron a Londres, donde Alan nació el 23 de junio de 1912. Su padre regresó a India poco después, y su madre le siguió tan sólo quince meses más tarde, dejando a Alan al cuidado de niñeras y amigos hasta que fue lo suficientemente mayor para ir a un internado.

En 1926, a la edad de catorce años, Turing fue a la Escuela Sherborne, en Dorset. El comienzo de su primer trimestre coincidió con la huelga general, pero Turing estaba decidido a acudir el primer día y recorrió 100 km en bicicleta solo, de Southampton a Sherborne, una proeza que apareció en el periódico local. Para el final de su primer año en la escuela se había ganado una reputación de muchacho tímido y vergonzoso cuyas únicas habilidades eran las relacionadas con la ciencia. La meta de Sherborne era convertir a los niños en hombres bien formados en todos los campos, capacitados para regir el Imperio, pero Turing no compartía esta

ambición y, en términos generales, no fue nada feliz en sus años escolares.

Su único amigo verdadero en Sherborne era Christopher Morcom, que, al igual que Turing, tenía un gran interés por la ciencia. Juntos discutían las últimas noticias científicas y llevaban a cabo sus propios experimentos. La relación alentó la curiosidad intelectual de Turing, pero, aún más, tuvo también un profundo efecto emocional en él. Andrew Hodges, el biógrafo de Turing, escribió que «éste fue su primer amor... Tenía esa sensación de entrega, y una intensificación de la conciencia, como si surgiesen colores brillantes en un mundo en blanco y negro». Su amistad duró cuatro años, pero parece ser que Morcom no llegó a darse cuenta de la profundidad de los sentimientos que Turing albergaba hacia él. Luego, durante su año final en Sherborne, Turing perdió para siempre la posibilidad de decirle lo que sentía. El jueves 13 de febrero de 1930, Christopher Morcom murió repentinamente de tuberculosis.

Figura 47. Alan Turing

Turing quedó destrozado por la pérdida de la única persona a la que amaría verdaderamente. Su manera de afrontar la muerte de Morcom fue concentrarse en sus estudios científicos en una tentativa de realizar el potencial de su amigo. Morcom, que parecía ser el que más talento tenía de los dos, ya había obtenido una beca para la Universidad de Cambridge. Turing creía que era su obligación obtener también una plaza en Cambridge y luego hacer los descubrimientos que de otra forma hubiese hecho su amigo. Pidió una foto a la madre de Christopher y cuando llegó le escribió una carta para darle las gracias: «Ahora la tengo sobre mi mesa, animándome a trabajar duro».

En 1931, Turing fue admitido en el King's College de la Universidad de Cambridge. Llegó allí durante un período de intenso debate sobre la naturaleza de las matemáticas y la lógica, y estuvo rodeado de algunas de las voces más importantes, como Bertrand Russell, Alfred North Whitehead y Ludwig Wittgenstein.

En el centro del debate estaba el tema de la *indecidibilidad,* un polémico concepto desarrollado por el lógico Kurt Gödel. Siempre se había asumido que, al menos en teoría, todas las preguntas matemáticas podían ser respondidas. Sin embargo, Gödel demostró que podría existir una minoría de preguntas que estaba más allá del alcance de la prueba lógica, las denominadas preguntas indecidibles. Los matemáticos se traumatizaron con la noticia de que las matemáticas no eran la disciplina omnipotente que siempre había creído que era.

Trataron de salvar su materia intentando descubrir una manera de identificar las molestas preguntas indecidibles, para poder ponerlas de lado de manera segura. Fue éste el objetivo que inspiraría luego a Turing a escribir su artículo matemático más influyente, «Sobre los números computables», publicado en 1937. En *Breaking the Code* («Descifrando el código»), la obra de teatro de Hugh Whitemore sobre la vida de Turing, uno de los personajes le pregunta a Turing el significado de su artículo. El responde: «Es sobre el bien y el mal. En términos generales. Es un artículo técnico de lógica matemática, pero es también sobre la dificultad de distinguir el bien del mal. La gente piensa —la mayoría de la gente piensa— que en las matemáticas siempre sabemos lo que está bien y lo que está mal. Pero no es así. Ya no».

En su tentativa de identificar las preguntas indecidibles, el artículo de Turing describía una máquina imaginaria diseñada para llevar a cabo una particular operación matemática, o algoritmo. En otras palabras, la máquina sería capaz de realizar una serie de pasos fijos y prescritos que, por ejemplo, multiplicarían dos números. Turing imaginó que los números que debían ser multiplicados serían introducidos en la máquina mediante una cinta de papel, similar a la cinta perforada que se usa para introducir una canción en una pianola. La respuesta de la multiplicación saldría a través de otra cinta. Turing imaginó toda una serie de estos artefactos, denominados *máquinas de Turing*, cada una de ellas diseñada para abordar una tarea particular, como dividir, elevar al cuadrado o convertir en factores. Luego dio un paso más radical.

Imaginó una máquina cuyo funcionamiento interno podía ser modificado para poder realizar todas las funciones de todas las máquinas de Turing imaginables. Las modificaciones se harían insertando cintas cuidadosamente seleccionadas, que transformarían la flexible máquina única en una máquina de dividir, de multiplicar o en cualquier otro tipo de máquina. Turing llamó a este mecanismo hipotético *máquina universal de Turing*, porque sería capaz de responder cualquier pregunta que pudiera ser respondida lógicamente.

Desgraciadamente, resultaba que no es siempre lógicamente posible responder una pregunta sobre la indecidibilidad de otra pregunta, de modo que ni siquiera la máquina universal de Turing podía identificar todas las preguntas indecidibles.

Los matemáticos que leyeron el artículo de Turing se sintieron decepcionados de que el monstruo de Gödel no hubiera sido sometido, pero, como premio de consolación, Turing les había dado el cianotipo del moderno ordenador programable. Turing conocía el trabajo de Babbage, y la máquina universal de Turing puede ser considerada una reencarnación del Motor de Diferencias N°2.

En realidad, Turing había ido mucho más lejos, proporcionando una base sólida para la computación, imbuyendo al ordenador un potencial hasta entonces inimaginable. Sin embargo, todavía estaban en los años treinta y no existía la tecnología para convertir en realidad la máquina universal de Turing. Sin embargo, Turing no se sentía consternado por el hecho de que sus teorías estuvieran por delante de lo que era técnicamente factible. Simplemente quería el reconocimiento de la comunidad

matemática, que efectivamente, aplaudió su artículo como uno de los avances más importantes del siglo. Todavía tenía sólo veintiséis años.

Éste fue un período particularmente feliz y lleno de éxito para Turing. Durante los años treinta, fue ascendiendo de categoría hasta llegar a profesor del King's College, el hogar de la elite intelectual del mundo. Llevaba la vida del arquetípico profesor de Cambridge, mezclando la matemática pura con actividades más triviales. En 1938 puso empeño en ver la película *Blancanieves y los siete enanitos,* que contenía la memorable escena en la que la bruja mala moja con veneno una manzana. Después, sus colegas oyeron a Turing repetir continuamente la macabra cantinela: «*Moja la manzana en la poción, que la muerte durmiente penetre en profusión*».

Turing valoraba mucho sus años en Cambridge. Además de su éxito académico, se encontraba en un ambiente tolerante que le apoyaba. La homosexualidad era aceptada en gran medida en la universidad, lo que significaba que era libre de frecuentar una serie de relaciones sin tener que preocuparse de que alguien se enterase o de lo que los demás podrían decir. Aunque no tuvo ninguna relación seria larga, parecía estar satisfecho con su vida. Entonces, en 1939, la carrera académica de Turing fue detenida abruptamente. La Escuela Gubernamental de Códigos y Cifras lo invitó a convertirse en criptoanalista en Bletchley, y el 4 de septiembre de 1939, el día después de que Neville Chamberlain declarase la guerra a Alemania, Turing se trasladó de la opulencia del patio interior de Cambridge a la posada Crown, en Shentley Brook End.

Cada día recorría en bicicleta 5 km de Shentley Brook End a Bletchley Park, donde pasaba parte del tiempo en los cobertizos contribuyendo al rutinario esfuerzo de desciframiento, y parte del tiempo en el centro de reflexión del grupo de expertos de Bletchley, que previamente había sido la tienda de manzanas, peras y ciruelas de *sir* Herbert León. El centro de reflexión era donde los criptoanalistas barajaban ideas sobre nuevos problemas o preveían cómo abordar problemas que pudieran surgir en el futuro. Turing se concentró en lo que podría suceder si los militares alemanes cambiaban su sistema de intercambiar claves de mensaje. Los éxitos anteriores de Bletchley se apoyaban en el trabajo de Rejewski, que sacaba partido al hecho de que los operadores de la Enigma codificaban cada clave de mensaje dos veces (por

ejemplo, si la clave de mensaje era YGB, el operador codificaría YGBYGB). Se suponía que esta repetición aseguraba que el receptor no cometiera un error, pero creó una grieta en la seguridad de la Enigma. Los criptoanalistas británicos supusieron que los alemanes no tardarían en darse cuenta de que la clave repetida estaba comprometiendo la seguridad de la cifra Enigma; entonces, se ordenaría a los operadores de la Enigma que abandonasen la repetición, confundiendo de este modo las actuales técnicas de desciframiento de Bletchley. Era el trabajo de Turing encontrar una manera alternativa de atacar la Enigma, una manera que no dependiera de la repetición de la clave de mensaje.

Según pasaron las semanas, Turing se dio cuenta que Bletchley estaba acumulando una gran biblioteca de mensajes descifrados y notó que muchos de ellos se ajustaban a una estructura rígida. Estudiando los viejos mensajes descifrados, creyó que a veces podría predecir parte del contenido de un mensaje sin descifrar, basándose en cuándo había sido enviado y en su origen Por ejemplo, la experiencia mostraba que los alemanes enviaban un parte meteorológico regular codificado todos los días poco después de las seis de la mañana. Por eso, un mensaje codificado interceptado a las seis y cinco de la mañana contendría casi seguro la palabra wetter, el «tiempo» en alemán. El riguroso protocolo empleado por cualquier organización militar significaba que semejantes mensajes se redactaban en un estilo estrictamente ordenado, de modo que Turing podía incluso tener mucha confianza respecto a la ubicación de la palabra wetter dentro del mensaje cifrado. Por ejemplo, la experiencia podía decirle que las primeras seis letras de un texto cifrado concreto correspondían a las letras de texto llano wetter. Cuando un fragmento de texto llano se puede asociar con un fragmento de texto cifrado, esta combinación se conoce como un *puntal.*

Turing estaba seguro de que podía sacar partido a los *puntales* para descifrar la Enigma. Si tuviera un texto cifrado y supiese que una sección específica, pongamos por caso ETJWPX, representaba wetter, entonces el desafío era identificar las posiciones de la máquina Enigma que transformarían wetter en ETJWPX. La manera directa, pero poco viable, de hacerlo sería que el criptoanalista tomase una máquina Enigma, tecleara wetter y viera si surgía el texto cifrado correcto. Si no, el criptoanalista cambiaría las posiciones de la máquina intercambiando cables del

clavijero e intercambiando o cambiando de orientación los modificadores, y luego tecleará wetter de nuevo. Si no surgía el texto cifrado correcto, el criptoanalista cambiaría las posiciones una y otra y otra y otra vez hasta encontrar la acertada. El único problema con este enfoque de prueba y error radicaba en el hecho de que había 159.000.000.000.000.000.00 posiciones posibles que probar, de modo que encontrar la que transformaba wetter en ETJWPX era una tarea aparentemente imposible.

Para simplificar el problema, Turing trató de seguir la estrategia de Rejewski de separar los efectos de las posiciones de los diferentes componentes de la máquina. Quería separar el problema de descubrir las posiciones de los modificadores (descubrir qué modificador está en qué ranura y cuáles son sus orientaciones respectivas) del problema de descubrir los cableados del clavijero. Por ejemplo, si podía descubrir algo en el *puntal* que no tenía nada que ver con los cableados del clavijero, entonces no le resultaría imposible probar cada una de las restantes 1.054.560 combinaciones posibles de los modificadores (60 disposiciones x 17.576 orientaciones). Si descubría las posiciones correctas de los modificadores, entonces podía deducir los cableados del clavijero.

Finalmente, se decidió por un tipo particular de *puntal* que contenía rizos internos, similares a las cadenas utilizadas por Rejewski. Las cadenas de Rejewski asociaban letras dentro de la clave de mensaje repetida.

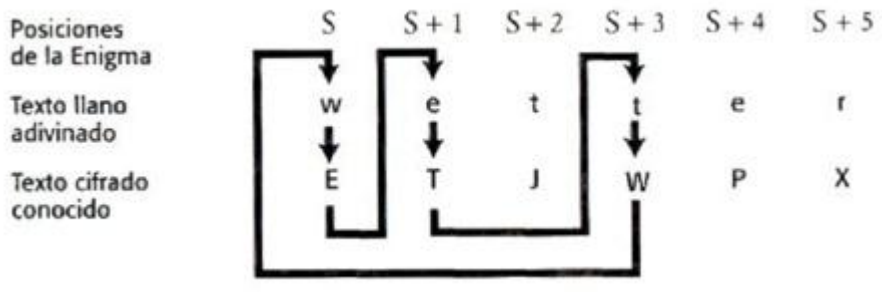


Figura 48. Uno de los puntales *de Turing, mostrando un rizo.*

Sin embargo, los rizos de Turing no tenían nada que ver con la clave de mensaje, porque él trabajaba dando por sentado que los alemanes pronto dejarían de enviar claves de mensaje repetidas. En vez de en esa clave, los rizos de Turing conectaban

letras de texto llano y de texto cifrado en un *puntal.* Por ejemplo, el *puntal* mostrado en la Figura 48 contiene un rizo.

Recuerde, los *puntales* son sólo suposiciones, pero si suponemos que este *puntal* es correcto, podemos asociar las letras w → E, e → T, t → W como parte del rizo. Aunque no conocemos ninguna de las posiciones de la máquina Enigma, podemos llamar a la primera posición, cualquiera que sea, S. En esta primera posición sabemos que la w es codificada como E. Después de esta codificación, el primer modificador gira un lugar hasta la posición S+1 y la letra e es codificada como T. El modificador vuelve a girar un lugar y codifica una letra que no forma parte del rizo, de modo que no tomamos en consideración esta codificación. El modificador avanza un lugar más y, de nuevo, llegamos a una letra que forma parte del rizo. En la posición S+3 sabemos que la letra t es codificada como W. En resumen, sabemos que

En la posición S, la Enigma codifica w como E.
En la posición S + 1, la Enigma codifica e como T.
En la posición S + 3, la Enigma codifica t como W.

Hasta ahora, el rizo no parece más que un curioso patrón, pero Turing siguió rigurosamente las implicaciones de las relaciones dentro del rizo y vio que le proporcionaban el atajo drástico que necesitaba para descifrar la Enigma. En vez de trabajar con sólo una máquina Enigma para probar cada posición, Turing comenzó a imaginar tres máquinas separadas, ocupándose cada una de ellas de la codificación de un elemento del rizo. La primera máquina trataría de codificar w como E, la segunda trataría de codificar e como T y la tercera t como W. Las tres máquinas tendrían posiciones idénticas, excepto que la segunda tendría sus orientaciones de los modificadores un lugar por delante con respecto a las de la primera, por lo que esa posición se llama S+1, y la tercera tendría sus orientaciones de los modificadores tres lugares por delante con respecto a las de la primera, por lo que esa posición se llama S+3. Turing imaginó entonces un criptoanalista frenético, que cambiaba continuamente los cables del clavijero, intercambiaba las disposiciones de los modificadores y cambiaba sus orientaciones para conseguir las codificaciones

correctas. Los cables que se cambiaban en la primera máquina serían también cambiados en las otras dos. Y, lo más importante, cualquiera que fuera la orientación de los modificadores en la primera máquina, la segunda tendría la misma orientación pero avanzada un lugar y la tercera tendría la misma orientación pero avanzada tres lugares.

Turing no parece haber conseguido mucho. El criptoanalista todavía tiene que probar las 159.000.000.000.000.000.000 posiciones posibles y, para empeorar aún las cosas, ahora tiene que hacerlo simultáneamente en las tres máquinas, en vez de sólo en una. Sin embargo, la fase siguiente de la idea de Turing transforma el desafío y lo simplifica considerablemente. Imaginó conectar las tres máquinas haciendo pasar cables eléctricos entre los dispositivos de entrada y de salida de cada máquina, tal como se muestra en la Figura 49.

En realidad, el rizo en el *puntal* tiene su parangón en el rizo del circuito eléctrico. Turing imaginó que las máquinas cambiaban sus posiciones del clavijero y de los modificadores, tal como he descrito, pero el circuito sólo se cerraría cuando todas las posiciones fueran correctas para las tres máquinas, permitiendo entonces que circulase una corriente por las tres máquinas. Si Turing incorporaba una bombilla en el circuito, la corriente la encendería, señalando que las posiciones correctas habían sido encontradas. En esos momentos, las tres máquinas todavía tienen que probar hasta 159.000.000.000.000.000.000 posiciones posibles para encender la bombilla. Sin embargo, todo lo hecho hasta ahora ha sido meramente una preparación para el salto lógico final de Turing, que, de un golpe, haría que la tarea fuese cien millones de millones más fácil.

Turing había construido su circuito eléctrico de manera que anulara el efecto del clavijero, permitiéndole de esta manera ignorar los billones de posiciones del clavijero. La Figura 49 muestra que en la primera Enigma la corriente eléctrica entra en los modificadores y sale por alguna letra desconocida, a la que llamaremos L_1. La corriente pasa entonces por el clavijero, que transforma L_1 en E. Esta letra E se conecta mediante un cable con la letra e de la segunda Enigma y cuando la corriente pasa por el segundo clavijero se vuelve a transformar en L_1. En otras palabras, los dos clavijeros se contrarrestan mutuamente. De manera similar, la corriente que sale de los modificadores de la segunda Enigma entra en el clavijero

en L_2 antes de ser transformada en T. Esta letra T se conecta mediante un cable con la letra t de la tercera Enigma, y cuando la corriente pasa por el tercer clavijero se vuelve a transformar en L_2. Resumiendo, los clavijeros se contrarrestan mutuamente a lo largo de todo el circuito, de modo que Turing podía ignorarlos completamente.

Turing sólo necesitaba conectar el dispositivo de salida del primer juego de modificadores, L_1 directamente al dispositivo de salida del segundo juego de modificadores, también L_1 y así sucesivamente. Desgraciadamente, no sabía el valor de la letra L_1 de modo que tuvo que conectar los 26 dispositivos de salida del primer juego de modificadores a los 26 dispositivos de entrada correspondientes del segundo juego de modificadores, y así sucesivamente.

En realidad, ahora había 26 rizos eléctricos y cada uno de ellos tenía que tener una bombilla para indicar que un circuito eléctrico estaba completo. Los tres juegos de modificadores podían entonces probar simplemente cada una de las 17.576 orientaciones, con el segundo juego de modificadores siempre un lugar por delante del primer juego, y el tercer juego de modificadores dos lugares por delante del segundo juego.

Finalmente, cuando se hubieran encontrado las posiciones correctas de los modificadores, uno de los circuitos se completaría y se encendería la bombilla. Si los modificadores cambiaban de orientación cada segundo sólo se tardaría cinco horas en probar todas las orientaciones.

Sólo quedaban dos problemas. Primero, podría ser que las tres máquinas estuvieran funcionando con una disposición de los modificadores errónea, porque la máquina Enigma opera con tres cualquiera de los cinco modificadores disponibles, situados en cualquier orden, dando sesenta disposiciones posibles. Por tanto, si se han probado todas las 17.576 orientaciones y no se ha encendido la bombilla es necesario probar otra de las sesenta disposiciones de los modificadores y seguir probando otras disposiciones hasta que se complete el circuito. Como alternativa, el criptoanalista podría tener sesenta juegos de tres Enigmas funcionando en paralelo.

El segundo problema es descubrir los cableados del clavijero, una vez que las disposiciones y orientaciones de los modificadores han sido establecidas. Esto es relativamente simple. Utilizando una máquina Enigma con las disposiciones y

orientaciones correctas de los modificadores, el criptoanalista teclea el texto cifrado y observa el texto llano resultante.

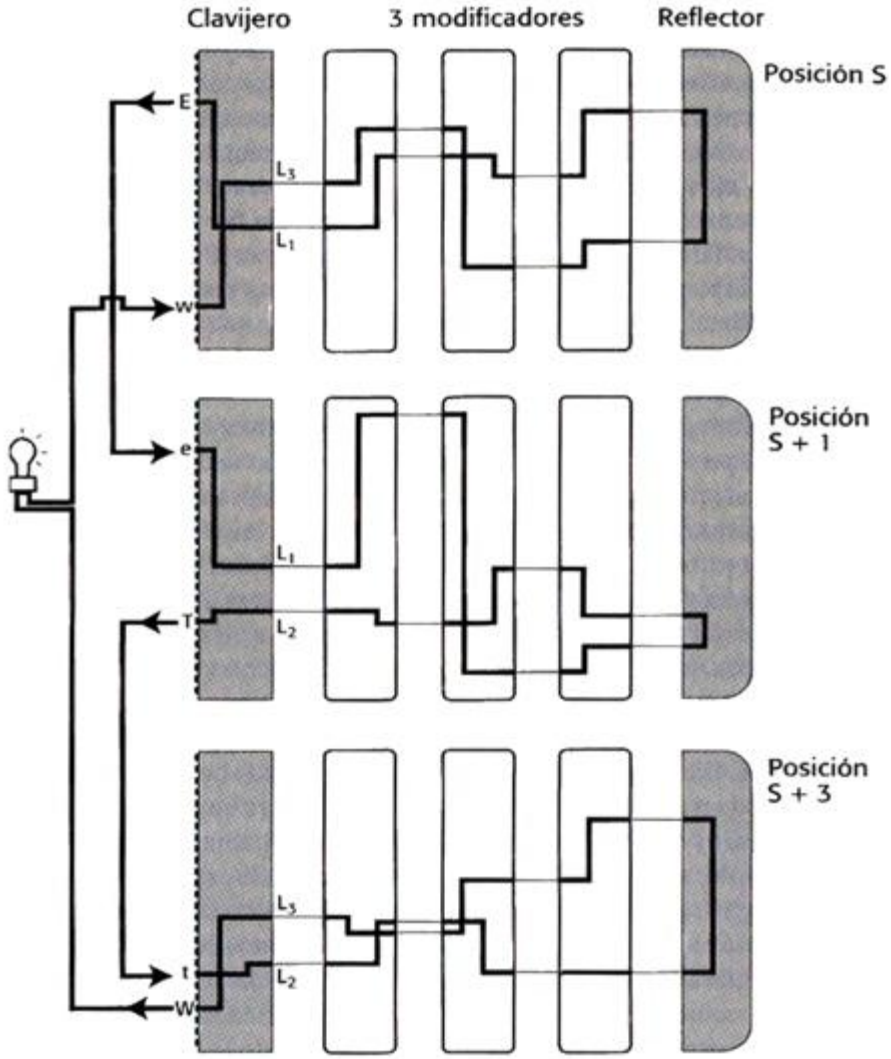


Figura 49. El rizo en el puntal puede tener su paralelo en un rizo eléctrico. Se disponen tres máquinas Enigma de maneras idénticas, excepto que la segunda tiene su primer modificador avanzado un lugar (posición S+1) y la tercera tiene su modificador avanzado otros dos lugares (posición S+3). El dispositivo de salida de cadí Enigma se conecta entonces con el dispositivo de entrada de la siguiente máquina Los tres juegos de modificadores van girando al mismo tiempo hasta que se completa el circuito y se enciende la bombilla. Eso significa que se ha encontrado la posición correcta. En el diagrama de arriba, el circuito está completo, lo que se corresponde con la posición correcta.

Si el resultado es tewwer en vez de wetter, es evidente que hay que insertar cables en el clavijero para intercambiar la w y la t. Teclear otros fragmentos de texto cifrado revelaría otros cableados del clavijero.

La combinación de *puntal*, rizos y máquinas conectadas eléctricamente resultó en una forma extraordinaria de criptoanálisis, y sólo Turing, con sus antecedentes únicos en máquinas matemáticas, podía haber tenido esa idea. Sus reflexiones sobre las imaginarias máquinas de Turing procedían del deseo de responder preguntas esotéricas sobre la indecidibilidad matemática, pero esta investigación puramente académica le había puesto en el estado de ánimo apropiado para diseñar una máquina práctica capaz de resolver problemas muy reales.

Bletchley consiguió obtener 100.000 libras esterlinas para convertir la idea de Turing en máquinas operativas, que recibieron el apodo de *bombas* porque su enfoque mecánico tenía una cierta semejanza con la *bomba* de Rejewski. Cada una de las *bombas* de Turing constaba de doce juegos de modificadores Enigma conectados eléctricamente y, por tanto, era capaz de afrontar rizos de letras mucho más largos. La unidad completa tenía unos dos metros de altura, dos metros de longitud y un metro de anchura. Turing finalizó el diseño a comienzos de 1940, y la labor de construcción fue otorgada a la fábrica de Maquinaria de Tabulación Británica de Letchworth.

Mientras esperaba la entrega de las *bombas*, Turing continuó su trabajo cotidiano en Bletchley. La noticia de su adelanto pronto se extendió entre los demás criptoanalistas, que reconocieron que poseía un talento singular como descifrador. Según Peter Hilton, colega descifrador en Bletchley, «obviamente, Alan Turing era un genio, pero un genio accesible y simpático. Estaba siempre dispuesto a dedicar el tiempo y el esfuerzo necesarios para explicar sus ideas; pero no era un especialista restringido, de manera que su polifacético pensamiento abarcaba un área enorme de las ciencias exactas».

Sin embargo, todo lo relacionado con la Escuela Gubernamental de Códigos y Cifras era de alto secreto, de modo que nadie fuera de Bletchley Park era consciente del extraordinario logro de Turing. Por ejemplo, sus padres no tenían ni idea de que Alan fuera siquiera descifrador, ni mucho menos el principal criptoanalista del Reino

Unido. Una vez le dijo a su madre que su trabajo tenía que ver con algún tipo de investigación militar, pero no le dio ningún detalle. Ella se mostró meramente desilusionada de que esto no hubiera resultado en un corte de pelo más respetable para su desaliñado hijo. Aunque Bletchley dependía del ejército, los militares habían concedido que tendrían que tolerar el desaliño y las excentricidades de estos «tipos profesores». Turing casi nunca se molestaba en afeitarse, sus uñas estaban llenas de suciedad y su ropa estaba siempre arrugada. Lo que no se sabe es si el ejército hubiera tolerado también su homosexualidad. Jack Good, un veterano de Bletchley, comentó: «Afortunadamente, las autoridades no sabían que Turing era homosexual. Si no, podríamos haber perdido la guerra».

La primera *bomba* prototipo, bautizada con el nombre de *Victory*, llegó a Bletchley el 14 de marzo de 1940. La máquina se puso en funcionamiento inmediatamente, pero los resultados iniciales no fueron lo que se dice satisfactorios. La máquina resultó ser mucho más lenta de lo que se esperaba, costándole hasta una semana encontrar una clave concreta. Hubo un esfuerzo conjunto para incrementar la eficacia de la *bomba* y pocas semanas después se presentó un diseño modificado. Costaría cuatro meses más construir la *bomba* mejorada.

Mientras tanto, los criptoanalistas tuvieron que afrontar la calamidad que habían anticipado. El 10 de mayo de 1940, los alemanes cambiaron su protocolo de intercambio de claves. Ya no repetían la clave de mensaje e inmediatamente después el número de desciframientos satisfactorios de la Enigma disminuyó dramáticamente. El apagón de información duró hasta el 8 de agosto, fecha en que llegó la nueva *bomba.* Bautizada como *Agnus Dei*, o *Agnes* para abreviar, esta máquina iba a satisfacer todas las expectativas de Turing.

En menos de dieciocho meses había quince *bombas* más funcionando, sacando partido a los *puntales*, probando posiciones de los modificadores y revelando claves, todas ellas traqueteando como un millón de agujas de hacer punto. Si todo iba bien, una *bomba* podía encontrar una clave de la Enigma en menos de una hora. Una vez que se habían establecido los cableados del clavijero y las posiciones de los modificadores (la clave de mensaje) para un mensaje en particular, era fácil deducir la clave del día. Entonces, todos los demás mensajes enviados ese día también se podían descifrar.

A pesar de que las *bombas* representaron una avance vital en el criptoanálisis, el desciframiento no se había convertido en una mera formalidad. Había que superar muchos obstáculos antes siquiera de que las *bombas* pudieran empezar a buscar una clave. Por ejemplo, para hacer funcionar una *bomba* primero se necesitaba un *puntal.* Los descifradores expertos daban *puntales* a los operadores de las *bombas*, pero no había ninguna garantía de que los descifradores hubiesen adivinado el significado correcto del texto cifrado. E incluso si tenían el *puntal* correcto, podía estar en un lugar erróneo: puede que los criptoanalistas hubieran adivinado que un mensaje codificado contenía cierta frase, pero que hubiesen asociado esa frase con un fragmento equivocado del texto cifrado. Sin embargo, había un truco ingenioso para comprobar si un *puntal* estaba en la posición correcta.

En el siguiente *puntal,* el criptoanalista confía en que el texto llano es correcto, pero no está seguro de si lo ha asociado con las letras apropiadas del texto cifrado.

Texto llano adivinado	w e t t e r n u l l s e c h s
Texto cifrado conocido	I P R E N L W K M J J S X C P L E J W Q

Una de las características de la máquina Enigma era su incapacidad para codificar una letra como sí misma, lo que era una consecuencia del reflector. La letra a nunca podía ser codificada como A, la letra b nunca podía ser codificada como B, y así sucesivamente. Por tanto, este *puntal* anterior en particular debe estar mal alineado, porque la primera e de wetter está asociada con una E del texto cifrado.

Para encontrar la alineación correcta, simplemente deslizamos el texto llano y el texto cifrado correspondientes hasta que ninguna letra esté emparejada consigo misma. Si movemos el texto llano un lugar hacia la izquierda, la combinación aún falla, porque ahora la primera s de sechs está emparejada con una S del texto cifrado. Sin embargo, si movemos el texto llano un lugar hacia la derecha ya no hay codificaciones ilícitas. Por tanto, es probable que este *puntal* esté en la posición correcta y podría usarse como base del desciframiento de una *bomba*:

Texto llano adivinado	w e t t e r n u l l s e c h s
Texto cifrado conocido	I P R E N L W K M J J S X C P L E J W Q

La inteligencia acumulada en Bletchley se pasaba sólo a las figuras militares de más alto rango y a miembros selectos del gabinete de guerra. Winston Churchill era completamente consciente de la importancia de los descifamientos de Bletchley, y el 6 de septiembre de 1941 visitó a los descifradores. Al conocer a algunos de los criptoanalistas, se sorprendió de la extraña mezcla de gente que le estaba proporcionando información tan valiosa; además de matemáticos y lingüistas, había un experto en porcelana, un conservador del Museo de Praga, el campeón británico de ajedrez y numerosos expertos del *bridge.* Churchill murmuró a *sir* Stewart Menzies, jefe del Servicio Secreto de Inteligencia: «Le dije que no dejase piedra sin remover, pero no esperaba que me tomase tan al pie de la letra». A pesar del comentario, sentía mucho afecto por el variopinto equipo y los llamó «los gansos que ponían huevos de oro y nunca cacareaban».

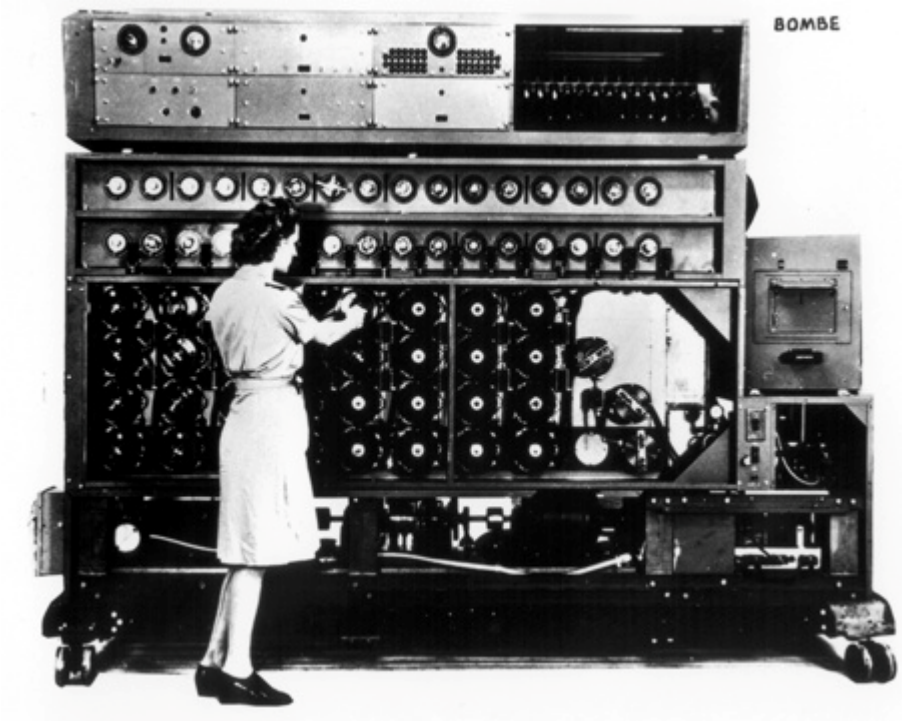


Figura 50. Una bomba de Bletchley Park en acción.

La visita tenía el propósito de levantar la moral de los descifradores mostrándoles que su trabajo era apreciado al más alto nivel. También tuvo el efecto de dar a Turing y sus colegas la confianza necesaria para recurrir directamente a Churchill

cuando surgió una crisis.

Para sacar el mayor partido de las *bombas*, Turing necesitaba más personal, pero sus peticiones habían sido bloqueadas por el comandante Edward Travis, que había tomado el puesto de director de Bletchley, y que pensaba que no podía justificar reclutar más gente. El 21 de octubre de 1941, los criptoanalistas dieron el paso insubordinado de ignorar a Travis y escribir directamente a Churchill.

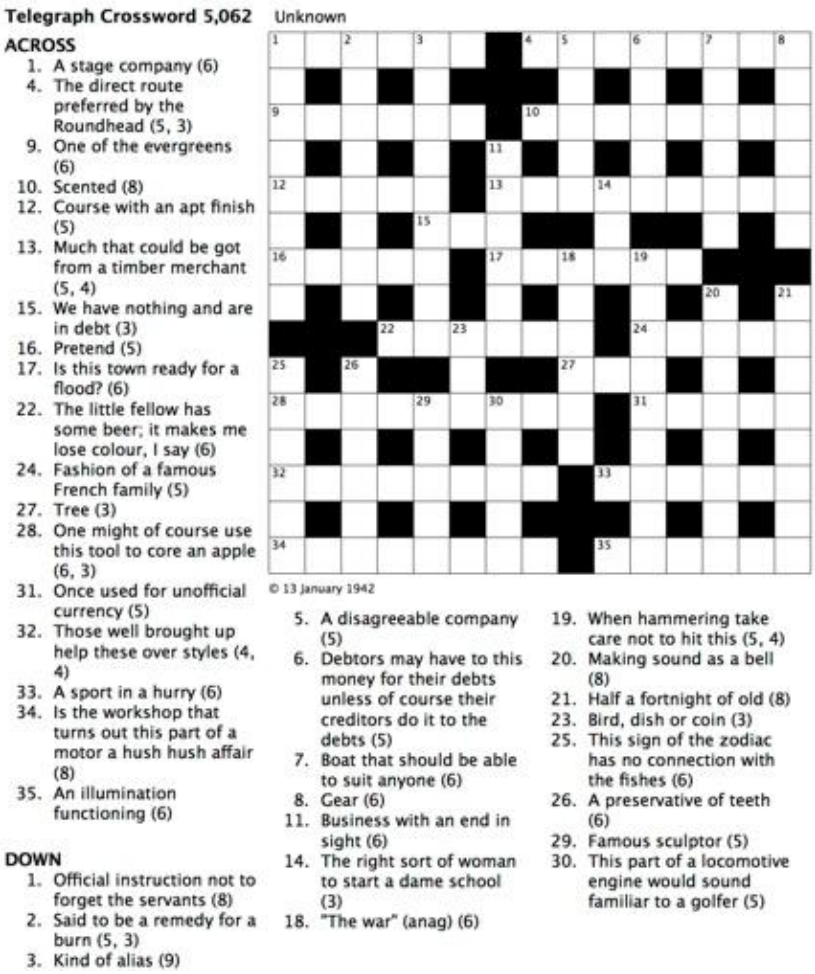
> *Estimado Primer Ministro,*
>
> *Hace algunas semanas nos rindió el honor de una visita, y creemos que considera importante nuestro trabajo. Vería usted que, gracias en gran medida a la energía y previsión del comandante Travis, hemos estado bien equipados de «bombas» para descifrar los códigos de la Enigma alemana. Pensamos, sin embargo, que debería saber que todo este trabajo está siendo retrasado, y en algunos casos no se está realizando en absoluto, principalmente porque no podemos contar con suficiente personal que se ocupe de ello. Nuestra razón para escribirle a usted directamente es que durante meses hemos hecho todo lo posible a través de los canales normales, y que hemos perdido la esperanza de que las cosas mejoren pronto sin su intervención...*
>
> *Somos, Señor, Sus obedientes siervos,*
>
> *A. M. Turing*
> *W. G. Welchman*
> *C. H. O'D Alexander*
> *P. S. Milner-Barry*

La respuesta de Churchill no se hizo esperar. Inmediatamente emitió un memorándum a su principal oficial de personal:

> *ACCIÓN DEL DÍA Asegúrese de que tengan todo lo que quieran con extrema prioridad e infórmeme de que así se ha hecho.*

A partir de entonces ya no hubo barreras para reclutar o para conseguir material. Para finales de 1942 había 49 *bombas*, y se abrió una nueva sede de *bombas* en

Gayhurst Manor, justo al norte de Bletchley. Como parte de la campaña de reclutamiento, la Escuela Gubernamental de Códigos y Cifras publicó una carta en el *Daily Telegraph.*



Telegraph Crossword 5,062 Unknown

ACROSS

1. A stage company (6)
4. The direct route preferred by the Roundhead (5, 3)
9. One of the evergreens (6)
10. Scented (8)
12. Course with an apt finish (5)
13. Much that could be got from a timber merchant (5, 4)
15. We have nothing and are in debt (3)
16. Pretend (5)
17. Is this town ready for a flood? (6)
22. The little fellow has some beer; it makes me lose colour, I say (6)
24. Fashion of a famous French family (5)
27. Tree (3)
28. One might of course use this tool to core an apple (6, 3)
31. Once used for unofficial currency (5)
32. Those well brought up help these over styles (4, 4)
33. A sport in a hurry (6)
34. Is the workshop that turns out this part of a motor a hush hush affair (8)
35. An illumination functioning (6)

DOWN

1. Official instruction not to forget the servants (8)
2. Said to be a remedy for a burn (5, 3)
3. Kind of alias (9)
5. A disagreeable company (5)
6. Debtors may have to this money for their debts unless of course their creditors do it to the debts (5)
7. Boat that should be able to suit anyone (6)
8. Gear (6)
11. Business with an end in sight (6)
14. The right sort of woman to start a dame school (3)
18. "The war" (anag) (6)
19. When hammering take care not to hit this (5, 4)
20. Making sound as a bell (8)
21. Half a fortnight of old (8)
23. Bird, dish or coin (3)
25. This sign of the zodiac has no connection with the fishes (6)
26. A preservative of teeth (6)
29. Famous sculptor (5)
30. This part of a locomotive engine would sound familiar to a golfer (5)

© 13 January 1942

Figura 51. Solución al crucigrama del Daily Telegraph *utilizado como examen para reclutar a nuevos descifradores: HORIZONTALES: (1. Troupe. 4. Short Cut, 9. Privet, 10. Aromatic, 12. Trend, 13. Great deal, 15. Owe, 16. Feign, 17. Newark, 22. Impale, 24. Guise, 27. Ash, 28. Centre bit, 31. Token, 32. Lame dogs, 33. Racing, 34. Silencer, 35. Alight). VERTICALES: (1. Tipstaff, 2. Olive oil, 3. Pseudonym, 5. Hordc, 6. Remit, 7. Cutter, 8. Tackle, 11. Agenda. 14. Ada, 18. Wreath. 19. Right nail, 20. Tinkling, 21. Sennight, 23. Pie, 25. Scales, 26. Enamel, 29. Rodin. 30. Bogie).*

Lanzaron un desafío anónimo a sus lectores, preguntando si alguien podía resolver

el crucigrama del periódico (Figura 51) en menos de 12 minutos. Se tenía la impresión de que los expertos en crucigramas podían ser también buenos descifradores, complementando las mentes científicas que ya había en Bletchley, pero, por supuesto, no se mencionaba nada de esto en el periódico.

Los 25 lectores que contestaron fueron invitados a Fleet Street para realizar un examen consistente en otro crucigrama. Cinco de ellos completaron el crucigrama en el tiempo asignado y a otro sólo le faltaba una palabra cuando acabaron los 12 minutos. Unas pocas semanas después, los seis fueron entrevistados por agentes de la inteligencia militar y reclutados como descifradores de Bletchley Park.

2. El rapto de libros de códigos

En lo que llevamos de capítulo, el tráfico de la Enigma ha sido tratado como un gigantesco sistema de comunicaciones, pero en realidad había varias redes distintas. El ejército alemán en el norte de África, por ejemplo, tenía su propia red separada y sus operadores de la Enigma tenían libros de códigos diferentes a los utilizados en Europa. Por eso, si Bletchley conseguía identificar la clave del día del norte de África podía descifrar todos los mensajes enviados desde el norte de África ese día, pero la clave del día del norte de África no servía para descifrar los mensajes transmitidos en Europa. De manera similar, la Luftwaffe tenía su propia red de comunicaciones, de modo que para descifrar todo el tráfico de la Luftwaffe, Bletchley tenía que desenmarañar su clave del día.

Algunas redes eran más difíciles de descifrar que otras. La red de la Kriegsmarine era la más difícil de todas, porque la marina alemana operaba una versión más sofisticada de la maquina Enigma. Por ejemplo, los operadores de la Enigma naval podían elegir entre ocho modificadores, y no sólo cinco, lo que significaba que había casi seis veces más de posiciones de los modificadores y, por tanto, casi seis veces más de claves que Bletchley tenía que probar. La otra diferencia de la Enigma naval tenía que ver con el reflector, que se ocupaba de devolver la señal eléctrica a través de los modificadores. En la Enigma normal, el reflector estaba siempre fijo en una orientación particular, pero en la Enigma naval, el reflector podía colocarse en veintiséis orientaciones diferentes. Por eso, el número de claves posibles había tenido un incremento adicional de un factor de 26.

Los operadores navales dificultaban aún más el criptoanálisis de la Enigma naval, ya que ponían mucho cuidado en no enviar mensajes estereotipados, por lo que privaban a Bletchley de *puntales.* Además, la Kriegsmarine había introducido también un sistema más seguro para seleccionar y transmitir las claves de mensaje. La combinación de modificadores adicionales, un reflector variable, mensajes no estereotipados y un nuevo sistema para intercambiar claves de mensaje contribuyó a que las comunicaciones navales alemanas fueran impenetrables.

El fracaso de Bletchley ante la Enigma naval tuvo como consecuencia que la Kriegsmarine fuera adquiriendo una clara ventaja en la batalla del Atlántico. El almirante Karl Dönitz había desarrollado una estrategia en dos fases altamente eficaz en la guerra naval. Comenzaba extendiendo sus submarinos y rastreando el Atlántico en búsqueda de convoyes aliados. En cuanto uno de ellos divisaba un objetivo iniciaba la fase siguiente de la estrategia llamando a los demás submarinos para que acudieran a la escena.

El ataque comenzaba sólo cuando ya se había reunido un grupo grande de submarinos. Para que esta estrategia de ataque coordinado tuviera éxito era esencial que la Kriegsmarine tuviese acceso a comunicaciones seguras. La Enigma naval proporcionaba semejantes comunicaciones y los ataques de submarinos tuvieron un impacto devastador en el tráfico marítimo que estaba suministrando al Reino Unido la comida y el armamento que tanto necesitaba.

Mientras las comunicaciones de los submarinos siguieran siendo seguras, los aliados no tendrían ni idea de la ubicación de los submarinos, y no podrían planear rutas seguras para los convoyes. Parecía que la única estrategia del Ministerio de Marina para determinar con precisión la ubicación de los submarinos era observando el emplazamiento de los buques británicos hundidos. Entre junio de 1940 y junio de 1941, los aliados perdieron una media de 50 barcos al mes, y corrían el peligro de no poder construir nuevos buques lo suficientemente rápido para sustituirlos. Además de la intolerable destrucción de los barcos, había también un terrible costo humano: 50.000 marinos aliados murieron durante la guerra.

A no ser que estas pérdidas pudieran ser reducidas drásticamente, el Reino Unido estaba en peligro de perder la batalla del Atlántico, lo que habría significado perder la guerra. Churchill escribiría más tarde: «Entre el torrente de sucesos violentos

había una ansiedad especialmente predominante. Las batallas podían ganarse o perderse, las empresas podían tener éxito o fracasar, podían ganarse o perderse territorios, pero todo nuestro poder para seguir en la guerra, o incluso para seguir con vida, dependía de nuestro dominio de las rutas oceánicas y el libre acceso a nuestros puertos».

La experiencia polaca y el caso de Hans-Thilo Schmidt habían enseñado a Bletchley Park que si el esfuerzo intelectual no lograba descifrar una cifra, entonces era necesario depender del espionaje, la infiltración y el robo para obtener las claves enemigas. De vez en cuando, Bletchley realizaba un avance contra la Enigma naval, gracias a una astuta estratagema de la RAF. Los aviones británicos ponían minas en una ubicación particular, provocando que los navíos alemanes enviasen advertencias a otros barcos. Estas advertencias codificadas con la Enigma contendrían inevitablemente una referencia cartográfica, pero lo importante era que esta referencia criptográfica ya la conocían los británicos, de modo que podía usarse como *puntal.* En otras palabras, Bletchley sabía que un fragmento particular de texto cifrado representaba un conjunto particular de coordenadas. Sembrar minas para obtener *puntales*, actividad conocida como «jardinería», requería que la RAF volase en misiones especiales, de modo que no podía hacerse regularmente. Bletchley tenía que encontrar otra manera de descifrar la Enigma naval.

Una estrategia alternativa para descifrar la Enigma naval dependía de robar las claves. Uno de los planes más intrépidos para robar claves fue ideado por Ian Fleming, creador de James Bond y miembro de la Inteligencia Naval durante la guerra. Fleming sugirió estrellar en el canal de la Mancha, cerca de un barco alemán, un bombardero alemán capturado. Los marineros alemanes se acercarían entonces al avión para rescatar a sus compañeros, tras lo cual la tripulación del avión, pilotos británicos haciéndose pasar por alemanes, entrarían en el barco y capturarían sus libros de códigos. Estos libros de códigos alemanes contenían la información requerida para establecer la clave de codificación, y como los barcos a menudo estaban lejos de la base durante largos períodos, estos libros serían válidos para al menos un mes. Capturando tales libros de códigos, Bletchley podría descifrar la Enigma naval durante todo un mes.

Después de aprobar el plan de Fleming, conocido como Operación Implacable, la

Inteligencia británica comenzó a preparar un bombardero Heinkel para el aterrizaje forzoso y reunió una tripulación de ingleses que hablaban alemán. El plan se programó para principios de mes, para así capturar un libro de códigos nuevo. Fleming fue a Dover para supervisar la operación, pero por desgracia no había ningún barco alemán en el área, por lo que el plan fue pospuesto indefinidamente. Cuatro días después, Frank Birch, jefe de la sección naval de Bletchley, anotó la reacción de Turing y su colega Peter Twinn: «Turing y Twinn se me acercaron como empresarios de pompas fúnebres a los que se les ha estafado un buen cadáver hace un par de días, totalmente alterados por la cancelación de la Operación Implacable».

A su debido tiempo, la Operación Implacable sería cancelada, pero los libros de códigos navales alemanes fueron finalmente capturados durante un cúmulo de audaces ataques a barcos meteorológicos y submarinos. Estas acciones, denominadas «pellizcos», proporcionaron a Bletchley los documentos que necesitaba para poner fin al apagón de inteligencia. Al volver transparente la Enigma naval, Bletchley pudo determinar con precisión la ubicación de los submarinos, y la batalla del Atlántico empezó a dar un giro favorable a los aliados. Los convoyes podían ser llevados por una trayectoria libre de submarinos, y los destructores británicos pudieron incluso comenzar a emprender la ofensiva, encontrando y hundiendo submarinos.

Era vital que el Alto Mando alemán nunca sospechara que los aliados habían «pellizcado» libros de códigos de la Enigma. Si los alemanes descubrían que su seguridad estaba comprometida, mejorarían sus máquinas Enigma y Bletchley volvería a estar en el punto de partida. Igual que habían hecho con el episodio del telegrama Zimmermann, los británicos tomaron varias precauciones para evitar levantar sospechas, como hundir un navío alemán tras robar sus libros de códigos. Esto convencería al almirante Dönitz de que el material referente a la cifra se había ido al fondo del mar, en vez de haber ido a parar a manos británicas.

Una vez que el material se había capturado en secreto se tenían que tomar precauciones adicionales antes de sacar partido a la inteligencia resultante. Por ejemplo, los desciframientos de la Enigma ofrecían el emplazamiento de numerosos submarinos, pero hubiese sido imprudente atacar todos y cada uno de ellos, porque

un inexplicable aumento del éxito británico advertiría a los alemanes de que sus comunicaciones estaban siendo descifradas. Por consiguiente, los aliados permitían escapar a algunos submarinos y sólo atacaban a otros cuando se había enviado previamente un avión de reconocimiento, justificando de este modo que pocas horas después se acercara un destructor. Como alternativa, los aliados podían enviar mensajes falsos que anunciaban haber localizado submarinos, lo que proporcionaba igualmente una explicación suficiente para el ataque que seguía.

A pesar de esta política de minimizar las señales delatoras de que la Enigma había sido descifrada, algunas acciones británicas hicieron despertar las sospechas de ciertos expertos en seguridad alemanes.

En una ocasión, Bletchley descifró un mensaje de la Enigma que daba la ubicación exacta de un grupo de buques cisterna y barcos de suministro alemanes, nueve en total. El Ministerio de Marina decidió no hundir todos los barcos, por si acaso una eliminación completa de los objetivos despertaba las sospechas alemanas. En vez de eso, informaron a los destructores de la ubicación exacta de sólo siete de los buques, lo que habría permitido que el *Gadania* y el *Gonzenheim* escapasen ilesos.

Los siete barcos en cuestión fueron efectivamente hundidos, pero los destructores de la Marina Real encontraron accidentalmente los dos navíos a los que se pensaba perdonar y los hundieron también. Los destructores no sabían nada acerca de la Enigma o de la política de no despertar sospechas, creían simplemente que estaban cumpliendo con su deber. En Berlín, el almirante Kurt Fricke instigó una investigación sobre éste y otros ataques similares, explorando la posibilidad de que Inglaterra hubiera descifrado la Enigma. El informe concluyó que las numerosas pérdidas eran, bien el resultado del infortunio natural, o bien eran causadas por un espía inglés que se había infiltrado en la Kriegsmarine. El desciframiento de la Enigma se consideraba imposible e inconcebible.

3. Los criptoanalistas anónimos

Además de descifrar la cifra de la Enigma alemana, Bletchley Park logró también descifrar mensajes italianos y japoneses. La inteligencia que surgió de estas tres fuentes recibió el nombre de Ultra, y los archivos de Inteligencia Ultra fueron los responsables de dar a los aliados una clara ventaja en todas las áreas principales

del conflicto. En el norte de África, la Ultra ayudó a destruir líneas de suministro alemanas e informó a los aliados de la situación de las fuerzas del general Rommel, permitiendo que el Octavo Ejército se defendiera contra los avances alemanes. La Ultra advirtió también de la invasión alemana de Grecia, lo que permitió que las tropas británicas se retirasen sin pérdidas cuantiosas. De hecho, la Ultra proporcionó informes precisos de la situación del enemigo en todo el Mediterráneo. Esta información resultó particularmente valiosa cuando los aliados desembarcaron en Italia y Sicilia en 1943.

En 1944 la Ultra desempeñó un papel principal en la invasión aliada de Europa. Por ejemplo, en los meses anteriores al día D, los desciframientos de Bletchley proporcionaron una imagen detallada de las concentraciones de tropas alemanas a lo largo de la costa francesa. *Sir* Harry Hinsley, historiador oficial de la Inteligencia británica durante la guerra, escribió:

> *Según se acumulaba la Ultra, producía algunos desagradables sobresaltos. En particular, en la segunda mitad de mayo reveló —después de preocupantes indicios de que los alemanes estaban llegando a la conclusión de que el área entre El Havre y Cherburgo iba a ser un área, y quizá incluso el área principal, de la invasión— que estaban enviando refuerzos a Normandía y la península de Cherburgo. Pero esta prueba llegó a tiempo para permitir que los aliados modificaran sus planes y situasen los desembarcos en la playa Utah y detrás de ella; y es un hecho singular que antes de que zarpase la expedición, el cálculo aliado del número, la identificación y la ubicación de las divisiones enemigas en el oeste, cincuenta y ocho en total, era certero en todos los puntos menos dos de los que iban a tener importancia operativa.*

A lo largo de toda la guerra, los descifradores de Bletchley sabían que sus desciframientos eran vitales, y la visita de Churchill a Bletchley había reforzado este punto. Pero a los criptoanalistas nunca se les dio ningún detalle operacional, ni se les dijo cómo eran usados sus desciframientos. Por ejemplo, no se les dio ninguna información sobre la fecha del día D, y ellos organizaron un baile para la noche

anterior a los desembarcos. Esto preocupó al comandante Travis, el director de Bletchley y la única persona del lugar que conocía los planes para el día D. No podía decir al comité del baile del Cobertizo 6 que cancelara el acto, porque eso hubiera dado una pista clara de que estaba en perspectiva una gran ofensiva, lo que pondría en peligro la seguridad. Permitió que se celebrara el baile.

Dio la casualidad de que, debido al mal tiempo, los desembarcos se aplazaron veinticuatro horas, de modo que los descifradores pudieron recuperarse de las frivolidades. El día de los desembarcos, la resistencia francesa destruyó las líneas terrestres, obligando a los alemanes a comunicarse únicamente por radio, lo que a su vez dio a Bletchley la oportunidad de interceptar y descifrar todavía más mensajes. En el momento decisivo de la guerra, Bletchley pudo proporcionar una imagen aún más detallada de las operaciones militares alemanas.

Stuart Milner-Barry, uno de los criptoanalistas del Cobertizo 6, escribió: «*No creo que haya habido ninguna guerra desde la época clásica, si es que ha habido alguna vez, en la que una de las partes leyó consistentemente la principal inteligencia militar y naval de la otra*».

Un informe norteamericano llegó a la misma conclusión:

> «*La Ultra creó entre el personal de alto rango y la cumbre política un estado de ánimo que transformó la manera en que se tomaban las decisiones. Saber que conoces a tu enemigo es una sensación enormemente alentadora. Va creciendo imperceptiblemente con el tiempo si observas regular e íntimamente sus pensamientos y maneras y hábitos y acciones. Este tipo de conocimiento hace que tu planificación sea menos vacilante y más segura, menos angustiosa y más optimista*».

Se ha afirmado, si bien de forma polémica, que los logros de Bletchley Park fueron el factor decisivo de la victoria aliada. Lo que es seguro es que los descifradores de Bletchley acortaron considerablemente la guerra. Esto resulta evidente si repetimos mentalmente la batalla del Atlántico y especulamos lo que podría haber sucedido sin el beneficio de la inteligencia Ultra. Para empezar, no cabe duda que se hubieran perdido más barcos y suministros debido a la dominante flota de submarinos, lo que

habría comprometido el vital enlace con Estados Unidos y obligado a los aliados a transferir mano de obra y medios económicos a la construcción de nuevos barcos. Los historiadores han estimado que esto habría retrasado varios meses los planes aliados, lo que habría significado posponer la invasión del día D por lo menos hasta el año siguiente. Según *sir* Harry Hinsley, «*la guerra, en vez de acabar en 1945, habría finalizado en 1948 si la Escuela Gubernamental de Códigos y Cifras no hubiera sido capaz de leer las cifras de la Enigma y producir la inteligencia Ultra*».

Durante este período de demora se habrían perdido aún más vidas en Europa, y Hitler habría podido utilizar aún más sus armas Y causando daños por todo el sur de Inglaterra. El historiador David Kahn resume el impacto del desciframiento de la Enigma: «Salvó vidas. No sólo vidas aliadas y rusas, sino, al acortar la guerra, también vidas alemanas, italianas y japonesas. Mucha gente viva tras la segunda guerra mundial no lo estaría si no hubiese sido por estas soluciones. Esa es la deuda que el mundo debe a los descifradores; ése es el valor humano culminante de sus triunfos».

Después de la guerra, las proezas de Bletchley se mantuvieron cautelosamente en secreto. Tras haber descifrado satisfactoriamente tantos mensajes durante la guerra, el Reino Unido quería continuar sus operaciones de inteligencia y no quería divulgar sus habilidades. De hecho, el Reino Unido había capturado miles de máquinas Enigma y las distribuyó entre sus antiguas colonias, que creían que la cifra era tan segura como les había parecido a los alemanes. Los británicos no hicieron nada para desengañarlas de esta creencia y descifraron constantemente sus comunicaciones secretas durante los años siguientes.

Mientras tanto, la Escuela Gubernamental de Códigos y Cifras de Bletchley Park fue cerrada y los miles de hombres y mujeres que habían contribuido a la creación de la Ultra fueron dispersados. Las *bombas* fueron desmanteladas y todo pedazo de papel relacionado con los desciframientos de la época de la guerra fue guardado bajo llave o quemado. Las actividades de desciframiento británicas fueron transferidas oficialmente a la recién fundada *Government Communications Headquarters* (GCHQ, Sede Gubernamental de Comunicaciones) de Londres, que fue trasladada a Cheltenhamen 1952. Aunque algunos de los criptoanalistas fueron a la GCHQ, la mayoría de ellos volvió a la vida civil, bajo juramento de guardar secreto, sin poder

revelar su papel esencial en el esfuerzo de guerra aliado. Mientras que los que habían combatido en batallas convencionales podían hablar de sus heroicas proezas, los que habían luchado batallas intelectuales no menos trascendentes tenían que soportar la vergüenza de tener que eludir las preguntas sobre sus actividades durante la guerra. Gordon Welchman contó cómo uno de los jóvenes criptoanalistas que habían trabajado con él en el Cobertizo 6 había recibido una carta mordaz del que había sido el director de su escuela, acusándole de ser una vergüenza para la escuela por no haber estado en el frente. Derek Taunt, que también trabajó en el Cobertizo 6, resumió la verdadera contribución de sus colegas: «Nuestra banda feliz puede no haber estado con el rey Harry el día de San Crispín, pero desde luego no nos quedamos en la cama y no tenemos ninguna razón por la que sentirnos malditos por haber estado donde estuvimos».

Tras tres décadas de silencio, el secreto en torno a Bletchley Park finalmente llegó a su fin a principios de los años setenta. El capitán F. W. Winterbotham, que había sido el responsable de distribuir la inteligencia Ultra, comenzó a acosar al gobierno británico, alegando que los países de la Commonwealth habían dejado de usar la cifra Enigma y que ya no había nada que conseguir ocultando el hecho de que el Reino Unido la había descifrado. Los Servicios de Inteligencia asintieron de mala gana y le permitieron escribir un libro sobre el trabajo realizado en Bletchley Park. Publicado en el verano de 1974, el libro de Winterbotham, titulado *The Ultra Secret,* fue la señal de que los miembros del personal de Bletchley eran libres, por fin, para hablar de sus actividades de la época de la guerra. Gordon Welchman sintió un alivio enorme: «Después de la guerra aún eludía las discusiones sobre sucesos por miedo de que podría revelar información obtenida de la Ultra en vez de leída en algún relato publicado... Sentí que el nuevo giro de los acontecimientos me liberaba de mi juramento, del tiempo de la guerra, de guardar secreto».

Los que habían contribuido tanto al esfuerzo de la guerra podían ahora recibir el reconocimiento que merecían. Posiblemente, la consecuencia más notable de las revelaciones de Winterbotham fue que Rejewski se dio cuenta de las asombrosas consecuencias de sus avances contra la Enigma, realizados antes de la guerra. Después de la invasión de Polonia, Rejewski había escapado a Francia, y cuando Francia fue invadida huyó a Inglaterra. Parecería natural que hubiera formado parte

del esfuerzo británico contra la Enigma, pero, en vez de ello, fue relegado a abordar cifras de poca categoría en una unidad de inteligencia de poca importancia en Boxmoor, cerca de Hemel Hempstead. No está claro por qué una mente tan brillante fue excluida de Bletchley Park, pero a causa de ello permaneció completamente desconocedor de las actividades de la Escuela Gubernamental de Códigos y Cifras. Hasta la publicación del libro de Winterbotham, Rejewski no tenía ni idea de que sus ideas habían proporcionado la base de los desciframientos diarios de la Enigma a lo largo de toda la guerra.

Para algunos, la publicación del libro de Winterbotham llegó demasiado tarde. Muchos años después de la muerte de Alastair Denniston, el primer director de Bletchley, su hija recibió una carta de uno de sus antiguos colegas: «Su padre fue un gran hombre con el que todas las personas de habla inglesa estarán en deuda durante muchísimo tiempo, si no para siempre. Que sea tan pocos los que sepan exactamente lo que hizo es la parte triste de la historia».

Alan Turing fue otro de los criptoanalistas que no vivió lo suficiente para recibir ningún reconocimiento público. En vez de ser aclamado como un héroe, fue perseguido por su homosexualidad. En 1952, mientras denunciaba un robo a la policía, reveló ingenuamente que mantenía una relación homosexual. La policía pensó que no le quedaba otra opción que detenerlo y acusarlo de «flagrante indecencia contraria a la Sección 11 del Acta de Enmienda de la Ley Penal de 1885». Los periódicos informaron del juicio y la condena subsiguientes y Turing fue humillado públicamente.

El secreto de Turing había sido revelado, y su sexualidad era ahora de dominio público. El gobierno británico le retiró su acreditación de miembro de la seguridad. Se le prohibió trabajar en proyectos de investigación relacionados con el desarrollo del ordenador. Fue obligado a consultar a un psiquiatra y tuvo que someterse a un tratamiento de hormonas, que lo dejó impotente y obeso. Durante los dos años siguientes sufrió una grave depresión, y el 7 de junio de 1954 se fue a su dormitorio con un tarro de solución de cianuro y una manzana. Veinte años antes había coreado la rima de la bruja mala: «*Moja la manzana en la poción, que la muerte durmiente penetre en profusión*». Ahora estaba listo para obedecer su conjuro. Mojó la manzana en el cianuro y dio varios mordiscos. Con sólo cincuenta y dos años,

uno de los genios verdaderos del criptoanálisis se suicidó.

Capítulo 5
La barrera del idioma

Contenido:

Mientras los descifradores británicos estaban descifrando la cifra Enigma alemana y alterando el curso de la guerra en Europa, los descifradores norteamericanos estaban teniendo una influencia igualmente importante en los acontecimientos del área del Pacífico desentrañando la máquina de cifras japonesa conocida como Purple («Púrpura»), Por ejemplo, en junio de 1942, los norteamericanos descifraron un mensaje que esbozaba un plan japonés para atraer las fuerzas navales estadounidenses a las islas Aleutianas simulando un ataque, lo que permitiría que la marina japonesa tomase su objetivo real, la isla Midway. Aunque los barcos norteamericanos siguieron el juego y abandonaron Midway, no se alejaron mucho. Cuando los criptoanalistas estadounidenses interceptaron y descifraron la orden japonesa de atacar Midway, los buques pudieron volver rápidamente y defender la isla en una de las batallas más importantes de toda la guerra del Pacífico. Según el almirante Chester Nimitz, la victoria estadounidense en Midway «fue esencialmente una victoria de inteligencia. Intentando la sorpresa, los japoneses fueron ellos mismos los sorprendidos».

Casi un año después, los criptoanalistas estadounidenses identificaron un mensaje que mostraba el itinerario de una visita a las islas Salomón del norte del almirante Isoruko Yamamoto, comandante en jefe de la flota japonesa. Nimitz decidió enviar aviones de caza para interceptar el avión de Yamamoto y derribarlo. Este almirante, famoso por ser obsesivamente puntual, se aproximó a su destino exactamente a las 8 de la mañana, tal como establecía el programa interceptado. Había dieciocho aviones de caza P-38 norteamericanos listos para recibirle, logrando matar a una de las figuras más influyentes del Alto Mando japonés.

Aunque la Púrpura y la Enigma, las cifras japonesa y alemana, fueron finalmente descifradas, ofrecieron bastante seguridad cuando fueron puestas en práctica inicialmente y supusieron verdaderos desafíos para los criptoanalistas norteamericanos y británicos. De hecho, si las máquinas de cifras hubieran sido utilizadas correctamente —sin claves de mensaje repetidas, sin *cillis,* sin restricciones en las posiciones del clavijero y en las disposiciones de los modificadores, y sin mensajes estereotipados que causaban *puntales*— es bastante posible que nunca habrían sido descifradas en absoluto.

La verdadera fuerza y potencial de las máquinas de cifras la demostraron la máquina de cifras Tipex (o Tipo X) utilizada por el ejército y las fuerzas aéreas británicas, y la máquina de cifras SIGABA (o M-143-C) utilizada por los militares norteamericanos. Estas dos máquinas eran más complejas que la Enigma y las dos fueron usadas correctamente, por lo que permanecieron indescifradas durante toda la guerra. Los criptógrafos aliados tenían confianza en que las complejas máquinas de cifras electromecánicas podían garantizar la comunicación segura. Sin embargo, las complejas máquinas de cifras no son la única manera de enviar mensajes seguros. De hecho, una de las formas de codificación más seguras utilizadas en la segunda guerra mundial era también una de las más simples.

Durante la campaña del Pacífico, los comandantes estadounidenses empezaron a darse cuenta que las máquinas de cifras, como la SIGABA, tenían una desventaja fundamental. Aunque la codificación electromecánica ofrecía niveles relativamente altos de seguridad, eran terriblemente lentas. Los mensajes tenían que ser tecleados en la máquina letra por letra, el resultado había de ser anotado también letra por letra, y luego el texto cifrado completo tenía que ser transmitido por el operador de radio. El operador de radio que recibía el mensaje codificado tenía que pasárselo entonces a un experto en cifras, que seleccionaría cuidadosamente la clave correcta y tecletaría el texto cifrado en una máquina de cifras, para descifrarlo letra por letra. El tiempo y espacio requeridos para esta delicada operación están disponibles en las sedes centrales o a bordo de un navío, pero la codificación por máquina no era la idónea en entornos más hostiles e intensos, como las islas del Pacífico. Un corresponsal de guerra describió las dificultades de la comunicación en plena batalla en la jungla: «Cuando la lucha quedaba limitada a un área pequeña

había que trasladarlo todo en una fracción de segundo. No había tiempo para codificar y descodificar. En épocas semejantes, el "inglés del rey[14]" se convirtió en el último recurso: contra más profano, mejor». Por desgracia para los norteamericanos, muchos soldados japoneses habían asistido a universidades estadounidenses y dominaban el inglés, incluidos los «tacos». Mucha información valiosa acerca de la estrategia y las tácticas norteamericanas estaba cayendo en manos del enemigo.

Uno de los primeros en reaccionar ante este problema fue Philip Johnston, un ingeniero establecido en Los Ángeles, que era demasiado viejo para combatir pero aún quería contribuir al esfuerzo de la guerra. A comienzos de 1942 empezó a formular un sistema de codificación inspirado en sus experiencias infantiles. Hijo de un misionero protestante, Johnston había crecido en las reservas de los indios navajos de Arizona, y como consecuencia de ello se había imbuido totalmente en la cultura navajo. Era una de las pocas personas fuera de la tribu que podía hablar su lengua con fluidez, lo que le permitió actuar de intérprete en las conversaciones entre los navajos y los agentes del gobierno. Su trabajo en esta capacidad culminó en una visita a la Casa Blanca, cuando, a los nueve años, Johnston tradujo para dos navajos que apelaban al presidente Theodore Roosevelt para que se diera un tratamiento más justo a su comunidad. Totalmente consciente de lo impenetrable que resultaba esa lengua para los ajenos a la tribu, a Johnston se le ocurrió la idea de que la lengua navajo, o cualquier otra lengua de los indios nativos americanos, podría servir como código virtualmente indescifrable. Si cada batallón en el Pacífico empleaba a un par de indios americanos como operadores de radio se podría garantizar la comunicación segura.

Ofreció su idea al teniente coronel James E. Jones, el oficial de señales locales de Camp Elliott, a las afueras de San Diego. Simplemente lanzando unas pocas frases en navajo al perplejo oficial, Johnston logró persuadirlo de que la idea merecía ser considerada seriamente. Dos semanas después, volvió con dos navajos, listo para hacer una demostración de prueba ante varios altos oficiales de la marina. Los navajos fueron separados, y uno de ellos recibió seis mensajes típicos en inglés, los tradujo a la lengua navajo y los transmitió por radio a su colega. El receptor navajo

[14] «Inglés del rey» (o «de la reina»). [«King's (Queen's) English»]: la lengua inglesa correctamente escrita o hablada. (N. del T.)

volvió a traducir los mensajes al inglés, los escribió y los entregó a los oficiales, que los compararon con los originales. El juego de los susurros navajos resultó ser perfecto, y los oficiales de la marina autorizaron un proyecto piloto y ordenaron que empezara inmediatamente el reclutamiento.

Sin embargo, antes de reclutar a nadie, el teniente coronel Jones y Philip Johnston tenían que decidir si realizar el estudio piloto con los navajos o elegir otra tribu. Johnston había usado a hombres navajos para su demostración original porque tenía conexiones personales con la tribu, pero esto no significaba necesariamente que constituyeran la elección ideal. El criterio de selección más importante era simplemente una cuestión de números: los marinos necesitaban encontrar una tribu capaz de proveer un gran número de hombres que dominaran el inglés y supieran leer y escribir. La falta de inversión gubernamental tenía como resultado que el índice de alfabetización era muy bajo en la mayoría de las reservas y, por tanto, la atención se concentró en las cuatro tribus más grandes: los navajos, los sioux, los chippewa y los pima-papagos.

Los navajos eran la tribu más grande, pero también la menos alfabetizada, mientras que los pima-papagos eran los más alfabetizados, pero muchos menos en número. Había poco que elegir entre las cuatro tribus, y finalmente la decisión se basó en otro factor crítico. Según el informe oficial sobre la idea de Johnston:

> *Los navajos son la única tribu en Estados Unidos que no ha estado infestada de estudiantes alemanes en los últimos veinte años. Estos alemanes, que estudiaban los diversos dialectos tribales con el pretexto de ser estudiantes de arte, antropólogos, etc., han adquirido indudablemente un buen conocimiento básico de todos los dialectos tribales excepto el navajo. Por esta razón, los navajos son la única tribu disponible que ofrece total seguridad para el tipo de trabajo que se está considerando. Habría que señalar también que el dialecto tribal navajo es completamente ininteligible para todas las demás tribus y todas las demás personas, con la posible excepción de hasta* 28 *americanos que han estudiado el dialecto. Este dialecto es equivalente a un código secreto para el enemigo, y admirablemente idóneo para la comunicación rápida y segura.*

En el momento de la entrada de Estados Unidos en la segunda guerra mundial, los navajos vivían en condiciones muy duras y eran tratados como gente inferior. Sin embargo, su consejo tribal apoyó el esfuerzo de la guerra y declaró su lealtad: «*No existe una concentración más pura de americanismo que entre los Primeros Americanos*». Los navajos estaban tan deseosos de luchar que algunos de ellos mintieron respecto a su edad, o se atiborraron de racimos de plátanos y tragaron grandes cantidades de agua para alcanzar el peso mínimo requerido de 55 kg. De manera similar, no hubo ninguna dificultad para encontrar candidatos idóneos para servir de mensajeros de código navajo, como se les llamaría. En menos de cuatro meses desde el bombardeo de Pearl Harbor, 29 navajos, algunos con sólo quince años, comenzaron un curso de comunicaciones de ocho semanas con la Infantería de Marina.

Antes de poder comenzar el curso de formación, la Infantería de Marina tuvo que solucionar un problema que había acosado al único otro código que se había basado en un idioma de los indios nativos americanos. En el norte de Francia, durante la primera guerra mundial, el capitán E. W. Horner, de la Compañía D, 141ª de Infantería, ordenó que ocho hombres de la tribu choctaw fueran empleados como operadores de radio. Obviamente, nadie en el campo enemigo comprendía su idioma, de modo que los choctaw proporcionaron comunicaciones seguras. Sin embargo, este sistema de codificación era esencialmente defectuoso porque la lengua choctaw no tenía ningún equivalente para la jerga militar moderna. Por tanto, un término técnico específico en un mensaje podría ser traducido como una vaga expresión choctaw, con el riesgo de que esto podía ser mal interpretado por el receptor.

El mismo problema habría surgido con el idioma navajo, pero la Infantería de Marina planeó crear un léxico de términos navajos para sustituir palabras inglesas que de otra forma resultarían imposibles de traducir, eliminando así cualquier ambigüedad. Los aprendices ayudaron a recopilar el léxico, tendiendo a elegir palabras que describían el mundo natural para indicar términos militares específicos. De esta manera, los nombres de pájaros se usaron para los nombres de aviones y los peces para los barcos (Tabla 11). Los comandantes se convirtieron en

«jefes de guerra», los pelotones eran «clanes del barro», las fortificaciones se volvieron «cuevas» y los morteros se conocían como «cañones que se agachan».

Tabla 11

Palabras de código en navajo para referirse a aviones y barcos.

Avión de caza	Hummingbird (colibrí)	Da-he-t¡h-hi
Avión de observación	Owl (búho)	Ne-as-jah
Avión torpedo	Swallow (golondrina)	Tas-chizzie
Bombardero	Buzzard (águila ratonera)	Jay-sho
Avión de bombardeo en picado	Chicken Hawk (halcón comepollos)	Cini
Bombas	Eggs (huevos)	A-ye-shi
Vehículo anfibio	Frog (rana)	Chal
Acorazado	Whale (ballena)	Lo-tso
Destructor	Shark (tiburón)	Calo
Submarino	Iron fish (pez de hierro)	Besh-lo

A pesar de que el léxico completo contenía 274 palabras, todavía quedaba el problema de traducir palabras menos previsibles y los nombres de personas y lugares. La solución fue crear un alfabeto fonético codificado para deletrear las palabras difíciles. Por ejemplo, la palabra Pacific (Pacífico) sería deletreada como «*pig, ant, cat, ice, fox, ice, cat*» («cerdo, hormiga, gato, hielo, zorro, hielo, gato»), lo que luego se traduciría al navajo como bi- sodih, wol-la-chee, moasi, tkin, ma-e, tkin, moasi.

El alfabeto navajo completo se ofrece en la Tabla 12. En seis semanas, los aprendices de mensajeros de código tuvieron que aprender el léxico completo y el alfabeto, evitando así la necesidad de libros de códigos que podían caer en manos del enemigo. Para los navajos, aprender todo esto de memoria resultaba insignificante, porque tradicionalmente su lengua no tenía una forma escrita, de modo que estaban acostumbrados a memorizar sus cuentos populares y las historias de las familias. Como dijo William McCabe, uno de los aprendices, «en navajo todo está en la memoria: canciones, oraciones, todo. Así es como nos criaron».

Tabla 12

El alfabeto de código navajo

A	Ant (hormiga)	Wol-la-chee	N	Nut (fruto seco)	Nesh-chee
B	Bear(oso)	Shush	O	Owl (búho)	Ne-ash-jsh
C	Car (gato)	Moasi	P	Pig (cerdo)	Bi-sodih
D	Deer (ciervo)	Be	Q	Quiver (carcaj)	Ca-yeílth
E	FJk (alce)	Dieh	R	Rabbil (conejo)	Gah
F	Fox (zorro)	Ma-e	S	Sheep (oveja)	Dibeh
C	Goat (cabra)	Klizzie	T	Turkey (pavo)	Tfian-zie
H	Horse (caballo)	Lin	U	Ute (indio Ute)	No-da-ih
I	Ice (hielo)	Tkin	V	Victor (triunfador)	A-keh-di-glini
J	Jackass (burro)	Tkele-cho-g¡	W	Weasel (comadreja)	Gloe-ih
K	Khi (chaval)	Klizzie-yazzi	X	Cross (cruce)	Al-an-as-dzoh
L	Lamb (cordero)	Dibeh-yazzi	Y	Yucca (yuca)	Tsah-as-zih
M	Mouse (ratón)	Na-as-tso-si	Z	Zinc (zinc)	Besh-do-gliz

Al final de su formación se puso a prueba a los navajos. Los emisores tradujeron una serie de mensajes del inglés al navajo, los transmitieron y entonces los receptores los volvieron a traducir al inglés, usando el léxico y el alfabeto memorizados cuando era necesario. Los resultados fueron perfectos. Para probar la solidez del sistema se entregó una grabación de las transmisiones a la Inteligencia Naval, la unidad que había descifrado la Púrpura, la cifra japonesa más difícil. Tras tres semanas de intenso criptoanálisis, los descifradores navales aún estaban desconcertados por los mensajes. Llamaron al idioma navajo una «extraña sucesión de sonidos guturales, nasales, trabalenguas... ni siquiera podemos transcribirlos, y mucho menos descifrarlos». El código navajo fue considerado un éxito. Se pidió a dos soldados navajos, John Benally y Johnny Manuelito, que se quedaran y formasen a la siguiente tanda de reclutas, mientras que los otros 27 mensajeros de código navajo fueron asignados a cuatro regimientos y enviados al Pacífico.

Las fuerzas japonesas habían atacado Pearl Harbor el 7 de diciembre de 1941, y en poco tiempo dominaban gran parte del oeste del Pacífico; después invadieron la

guarnición norteamericana de Guam el 10 de diciembre, tomaron Guadalcanal, una de las islas del archipiélago de Salomón, el 13 de diciembre, Hong Kong capituló el 25 de diciembre, y las tropas estadounidenses de las Filipinas se rindieron el 2 de enero de 1942. Los japoneses planeaban consolidar su control del Pacífico el verano siguiente construyendo un campo de aviación en Guadalcanal, creando así una base para los bombarderos, lo que les permitiría destruir las líneas de suministro aliadas, imposibilitando casi por completo cualquier contraataque aliado. El almirante Ernest King, jefe de las operaciones navales norteamericanas, exhortó un ataque a la isla antes de que se completara el campo de aviación, y el 7 de agosto la 1.ª división de la Marina encabezó una invasión de Guadalcanal. Entre los primeros en desembarcar se encontraba el primer grupo de mensajeros de código que entraba en acción.

Figura 52. Los 29 primeros mensajeros de código navajo posando para la tradicional foto de graduación.

Aunque los navajos estaban seguros de que sus habilidades serían muy beneficiosas para los marinos, sus primeras tentativas generaron tan sólo confusión. Muchos de los operadores de radio habituales no se habían enterado de este nuevo código y enviaron mensajes de pánico por toda la isla, afirmando que los japoneses estaban emitiendo en frecuencias norteamericanas. El coronel al mando detuvo

inmediatamente las comunicaciones en navajo hasta que pudiera convencerse de que merecía la pena poner en práctica el sistema. Uno de los mensajeros de código recordó cómo finalmente se volvió a poner en servicio el código navajo:

> *El coronel tuvo una idea. Dijo que nos permitiría seguir con una condición: que yo pudiera ser más rápido que su «código blanco», un ruidoso objeto mecánico de forma cilíndrica. Los dos enviamos mensajes, con el cilindro blanco y con mi voz. Los dos recibimos respuestas y la carrera era ver quién podía descodificar su respuesta el primero. Me preguntaron: «¿Cuánto tiempo te costará? ¿Dos horas?». «Más bien dos minutos», respondí. El otro estaba aún descodificando cuando obtuve el «¡recibido!» a mi mensaje de respuesta en unos cuatro minutos y medio. Le dije: «Coronel, ¿cuándo va a abandonar esa cosa cilíndrica?». El no dijo nada. Tan sólo encendió su pipa y se alejó.*

Los mensajeros de código pronto demostraron su valía en el campo de batalla. Durante un episodio en la isla de Saipán, un batallón de marinos tomó posiciones que previamente estaban en poder de soldados japoneses, que se habían retirado. De pronto explotó una salva muy cerca. Estaban siendo atacados por sus compañeros norteamericanos, que no se habían enterado de su avance. Los marinos enviaron mensajes de radio en inglés explicando su posición, pero las salvas continuaron porque las tropas estadounidenses que atacaban sospecharon que los mensajes provenían de imitadores japoneses que trataban de engañarlos. Sólo cuando se envió un mensaje en navajo los agresores se dieron cuenta de su error y detuvieron el asalto. Un mensaje navajo nunca podía ser falsificado, por lo que siempre se podía confiar en él.

La reputación de los mensajeros de código no tardó en extenderse, y hacia finales de 1942 se solicitó que enviaran otros 83 hombres. Los navajos prestaron servicio en las seis divisiones de la Infantería de Marina, y a veces fueron tomados prestados por otras fuerzas norteamericanas. Su guerra de palabras no tardó en convertir a los navajos en héroes. Otros soldados se ofrecían a cargar con sus radios y sus rifles, e incluso les pusieron guardaespaldas personales, en parte para

protegerlos de sus propios compañeros. En al menos tres ocasiones, algunos mensajeros de código fueron confundidos con soldados japoneses y capturados por compañeros norteamericanos. Sólo se los liberó cuando sus propios batallones respondieron por ellos.

La impenetrabilidad del código navajo se debía al hecho de que el navajo pertenece a la familia de lenguas na-dené, que no tiene ninguna conexión con ninguna lengua asiática o europea. Por ejemplo, un verbo navajo no se conjuga solamente en concordancia con su sujeto, sino también con su objeto. La terminación verbal depende de la categoría a que pertenece el objeto: largo (p. e., pipa, lápiz), fino y flexible (p. e., serpiente, correa), granulado (p. e., azúcar, sal), atado en haces (p. e., heno), viscoso (p. e., barro, heces) y muchas otras. El verbo también incorpora los adverbios y refleja si el hablante ha experimentado o no lo que está diciendo, o si son rumores. Por consiguiente, un solo verbo puede equivaler a una frase completa, haciendo que resulte virtualmente imposible para los extraños desentrañar su significado.

A pesar de sus puntos fuertes, el código navajo aún tenía dos defectos importantes. Primero, las palabras que ni pertenecían al vocabulario natural navajo ni aparecían en la lista de las 274 palabras codificadas autorizadas tenían que ser deletreadas utilizando el alfabeto especial. Esto requería mucho tiempo, de modo que se decidió añadir otros 234 términos comunes al léxico. Por ejemplo, a las naciones se les dio apodos navajos: «Sombrero Enrollado» para Australia, «Ligada al Agua» para Inglaterra, «Cabello Trenzado» para China, «Sombrero de Hierro» para Alemania, «Tierra Flotante» para las Filipinas, «Dolor de la Oveja» para España[15].

El segundo problema tenía que ver con las palabras que aún tenían que ser deletreadas. Si los japoneses se daban cuenta de que había palabras que se deletreaban comprenderían que podían usar el análisis de frecuencia para identificar las palabras navajo que representaban a cada letra en particular. Pronto les resultaría obvio que la palabra más usada era dzeh, que significa *elk* (alce) y que representa a la e, la letra utilizada con más frecuencia en inglés. Tan sólo deletrear el nombre de la isla de Guadalcanal, repitiendo así la palabra wol-la-chee, que significa *ant* (hormiga), cuatro veces, les daría una gran pista de qué palabra

[15] Este último apodo tiene su origen en la analogía fonética, ya que en inglés Sheep Pain («dolor de la oveja») tiene un sonido que se acerca al de Spain («España»). (N. del T.)

representaba a la letra a. La solución fue añadir más palabras que sirvieran de sustitutas adicionales (homófonas) para las letras usadas frecuentemente. Se introdujeron dos palabras extra como alternativas para cada una de las seis letras más corrientes (e, t, a, o, i, n) y una palabra extra para las seis letras siguientes en frecuencia (s, h, r, d, l, u). La letra a, por ejemplo, ahora podía sustituirse también con las palabras be- la-sana, que significa *apple* (manzana), o tse-nihl, que significa *axe* (hacha). A partir de entonces, Guadalcanal podía deletrearse con sólo una repetición: klizzie, shi-da, wol-la-chee, Iha-cha-eh, be-la-sana, dibeh-yaz-zie, moasi, tse-nihl, nesh-chee, tse-nihl, ah-jad (goat, únele, ant, dog, apple, lamb, cat, axe, nut, axe, leg).[16]

Según se fue intensificando la guerra en el Pacífico, y mientras los norteamericanos avanzaban de las islas Salomón a Okinawa, los mensajeros de código navajo desempeñaron un papel cada vez más vital. Durante los primeros días del ataque a Iwo Jima, se enviaron más de ochocientos mensajes en navajo, todos sin error. Según el comandante general Howard Conner, «*sin los navajos, los marinos nunca habrían tomado Iwo Jima*». La contribución de los mensajeros de código navajo resulta aún más extraordinaria al considerar que, para cumplir con sus obligaciones, a menudo tenían que confrontar y desobedecer a sus propios miedos espirituales, tan profundamente arraigados. Los navajos creen que los espíritus de los muertos, chindi, tratarán de vengarse de los vivos a no ser que se celebren ritos ceremoniales con el cadáver. La guerra del Pacífico fue particularmente sangrienta, con cadáveres esparcidos por los campos de batalla, y, sin embargo, los mensajeros de código se armaron del valor necesario para continuar a pesar de los chindi que los perseguían. En el libro de Doris Paul *The Navajo Code Talkers* («Los mensajeros de código navajo»), uno de los navajos relata un incidente que tipifica su valentía, dedicación y serenidad:

> *Si levantabas la cabeza apenas quince centímetros eras hombre muerto; el fuego era tan intenso. Y luego, de madrugada, sin relevo ni en nuestra parte ni en la suya, había una pausa muerta. Debió pasar que este japonés ya no pudo soportarlo más. Se levantó y gritó y chilló con todas sus fuerzas y salió corriendo hacia nuestra*

[16] Por supuesto, la traducción al castellano no deletrearía la palabra correcta (Guadalcanal), sino sólo un galimatías: cthpmcghfshp (cabra, tío, hormiga, perro, manzana, cordero, gato, hacha, fruto seco, hacha, pierna). (N. del T.)

trinchera, esgrimiendo una larga espada de samurai. Imagino que le dispararon de 25 a 40 veces antes de que cayera.

Había un amigo conmigo en la trinchera. Pero ese japonés le había cortado toda la garganta, limpiamente hasta las cuerdas de la parte trasera del cuello. Todavía jadeaba, por la tráquea. Y el sonido que hacía tratando de respirar era horrible. Murió, por supuesto. Cuando el japonés atacó, salpicó totalmente con sangre caliente mi mano, en la que tenía el micrófono. Estaba llamando en código pidiendo ayuda. Me dicen que a pesar de lo que sucedía, cada una de las sílabas de mi mensaje llegó claramente.

En total, hubo 420 mensajeros de código navajo. Aunque se reconoció su valentía como combatientes, su papel especial en proteger las comunicaciones era información clasificada. El gobierno les prohibió hablar sobre su trabajo, y su contribución única no se hizo pública. Igual que Turing y los criptoanalistas de Bletchley Park, los navajos fueron ignorados durante décadas. Finalmente, en 1968, el código navajo fue desclasificado y al año siguiente los mensajeros de código mantuvieron su primera reunión Luego, en 1982, se les rindió homenaje cuando el gobierno de Estados Unidos declaró el 14 de agosto «Día nacional de los mensajeros de código navajo». Sin embargo, el mayor tributo al trabajo de los navajos es el simple hecho de que su código es uno de los poquísimos de toda la Historia que nunca fue descifrado. El teniente coronel Seizo Arisue, jefe de la Inteligencia japonesa, admitió que, aunque habían descifrado el código de las fuerzas aéreas norteamericanas, no consiguieron tener ningún éxito con el código navajo.

1. El desciframiento de lenguas perdidas y escrituras antiguas

El éxito del código navajo se basó en gran medida en el simple hecho de que la lengua nativa de una persona carece totalmente de sentido para quien no esté familiarizado con ella. En muchos aspectos, la tarea a la que se enfrentaban los criptoanalistas japoneses es similar a la que afrontan los arqueólogos que tratan de descifrar una lengua antigua ya olvidada, escrita quizá en una escritura extinta. En realidad, el desafío arqueológico es mucho más duro. Por ejemplo, mientras que los

japoneses tenían una oleada continua de palabras en navajo que podían tratar de identificar, la información disponible para el arqueólogo a veces puede ser tan sólo una pequeña colección de tablillas de arcilla. Además, el descifrador arqueológico a menudo desconoce por completo el contexto o el contenido de un texto antiguo, que son pistas con las que los descifradores militares pueden contar normalmente para ayudarles a desentrañar una cifra.

Descifrar textos antiguos parece una actividad casi imposible y, sin embargo, muchos hombres y mujeres se han dedicado a esta ardua empresa. Su obsesión procede del deseo de comprender las escrituras de nuestros antepasados, permitiéndonos hablar sus palabras y hacernos una idea de sus pensamientos y sus vidas. Quizá este anhelo de descifrar escrituras antiguas haya sido resumido de la mejor manera por Maurice Pope, el autor de *La historia del desciframiento*: «Los desciframientos son, con diferencia, los logros más atractivos de la investigación académica. Hay algo mágico en las escrituras desconocidas, especialmente cuando proceden de un pasado remoto, y por ello hay una gloria correspondiente que recae sobre la primera persona que consigue resolver su misterio».

El desciframiento de escrituras antiguas no forma parte de la constante batalla evolutiva entre los codificadores y los descifradores, porque, aunque hay arqueólogos que son descifradores, no los hay que sean codificadores. Es decir, en la mayoría de los casos de desciframiento arqueológico, el escriba original del texto no intentó deliberadamente ocultar el significado de éste. El resto de este capítulo, que trata de los desciframientos arqueológicos, se desvía ligeramente, por tanto, del tema principal del libro. Sin embargo, los principios del desciframiento arqueológico son esencialmente los mismos que los del criptoanálisis militar convencional. De hecho, muchos descifradores militares se han sentidos atraídos por el desafío de desenmarañar una escritura antigua. Esto se debe probablemente a que los desciframientos arqueológicos suponen un cambio refrescante con respecto al desciframiento militar, ofreciendo un rompecabezas puramente intelectual en vez de un desafío militar. En otras palabras, la motivación es la curiosidad en vez de la animosidad.

El más famoso, y podría decirse que el más romántico, de todos los desciframientos fue el de los jeroglíficos egipcios. Los jeroglíficos fueron un misterio durante siglos,

y lo único que los arqueólogos podían hacer era especular sobre su significado. Sin embargo, gracias a un caso ya clásico de descodificación, los jeroglíficos fueron finalmente descifrados y desde entonces los arqueólogos han podido leer explicaciones de primera mano acerca de la historia, la cultura y las creencias de los antiguos egipcios. El desciframiento de los jeroglíficos ha conseguido tender un puente entre los milenios que nos separan de la civilización de los faraones.

Los jeroglíficos más antiguos se remontan al año 3000 a. C., y esta forma de escritura ornada perduró durante los siguientes tres mil quinientos años. Aunque los elaborados símbolos de los jeroglíficos resultaban ideales para los muros de los majestuosos templos (la palabra griega *hieroglyphica* significa «tallas sagradas»), eran demasiado complicados para registrar transacciones mundanas. Por eso, paralelamente a los jeroglíficos evolucionaba la *hierática*, una escritura cotidiana en la que cada símbolo jeroglífico era sustituido por una representación estilizada que era más rápida y más fácil de escribir. Alrededor del año 600 a. C., la hierática fue reemplazada por una escritura aún más simple conocida como *demótica,* nombre que procede del griego *demotika* y significa «popular», lo que refleja su función secular. Los jeroglíficos, la hierática y la demótica eran esencialmente la misma escritura: casi podrían ser consideradas simplemente como el equivalente a los diferentes tipos de letra entre los que podemos elegir ahora al escribir en un ordenador.

Las tres formas de escrituras eran fonéticas, es decir, los caracteres representaban en gran medida sonidos distintos, igual que las letras de nuestro alfabeto. Durante más de tres mil años, los antiguos egipcios utilizaron estas escrituras en todos los aspectos de sus vidas, igual que usamos la escritura en la actualidad. Luego, hacia el final del siglo IV de nuestra era, en menos de una generación, las escrituras egipcias desaparecieron. Los últimos ejemplos fechables de escritura egipcia antigua se pueden encontrar en la isla de File. Una inscripción jeroglífica fue tallada en un templo en el año 394, y un fragmento de *graffiti* demótico ha sido datado en el año 450. La expansión de la Iglesia cristiana fue la responsable de la extinción de las escrituras egipcias, ya que fueron prohibidas para erradicar cualquier conexión con el pasado pagano de Egipto. Las antiguas escrituras fueron sustituidas por el copto, una escritura consistente en 24 letras tomadas del alfabeto griego suplementadas

con seis caracteres demóticos utilizados para sonidos egipcios que no se expresaban en griego. El dominio del copto fue tan completo que desapareció la habilidad para leer los jeroglíficos, la demótica y la hierática. La lengua egipcia antigua siguió hablándose y evolucionó hasta convertirse en lo que se vino a denominar lengua copta, pero a su debido tiempo tanto la lengua como la escritura copta fueron desplazadas por la expansión del árabe en el siglo XI. Se había roto la última conexión con los antiguos reinos de Egipto perdiéndose el conocimiento necesario para leer las historias de los faraones.

El interés por los jeroglíficos resurgió en el siglo XVII, cuando el papa Sixto V reorganizó la ciudad de Roma según una nueva red de avenidas, erigiendo en cada intersección obeliscos comprados a Egipto. Los eruditos intentaron descifrar el significado de los jeroglíficos de los obeliscos, pero su labor se vio entorpecida por una falsa suposición; nadie estaba dispuesto a aceptar que los jeroglíficos pudieran representar caracteres fonéticos, o *fonogramas.* La idea de deletrear fonéticamente era considerada demasiado avanzada para una civilización tan antigua. En vez de eso, los eruditos del siglo XVII estaban convencidos de que los jeroglíficos eran *semagramas*: que estos intricados caracteres representaban ideas enteras, y no eran más que una primitiva escritura pictórica. La creencia de que los jeroglíficos eran meramente escritura pictórica era generalmente compartida incluso por los extranjeros que visitaban Egipto en la época en que los jeroglíficos eran todavía una escritura viva. Diodoro Sículo, un historiador griego del siglo la. C., escribió:

> *Sucede ahora que las formas de las letras egipcias toman la forma de todo tipo de criaturas vivientes y de las extremidades del cuerpo humano y de utensilios... Porque su escritura no expresa la idea deseada mediante una combinación de sílabas, una después de la otra, sino por medio de la apariencia externa de lo que se ha copiado y del significado metafórico inculcado en la memoria con la práctica... De modo que el halcón simboliza para ellos todo lo que sucede rápidamente, porque esta criatura es de las más rápidas entre los animales alados. Y la idea se transfiere, mediante la transferencia metafórica adecuada, a todas las cosas rápidas y a las cosas a las que les resulta apropiada la velocidad.*

A la luz de semejantes explicaciones, quizá no resulte sorprendente que los eruditos del siglo XVII tratasen de descifrar los jeroglíficos interpretando cada uno de ellos como una idea completa. Por ejemplo, en 1652 el jesuita alemán Athanasius Kircher publicó un diccionario de interpretaciones alegóricas titulado *Ædipus ægyptiacus,* y lo utilizó para producir una serie de traducciones extrañas y fantásticas. Un puñado de jeroglíficos, que ahora sabemos que representan simplemente el nombre del faraón Apries, fue traducido por Kircher de la siguiente manera: «Los beneficios del divino Osiris se procurarán por medio de ceremonias sagradas y de la cadena de los Genios, para que los beneficios del Nilo puedan ser obtenidos». En la actualidad, las traducciones de Kircher parecen absurdas, pero su impacto en otros aspirantes a descifradores fue inmenso. Kircher no era sólo un egiptólogo: escribió un libro sobre criptografía, construyó una fuente musical, inventó la linterna mágica (un precursor del cine) y descendió por el cráter del Vesubio, ganándose el título de «padre de la vulcanología». El jesuita era ampliamente reconocido como el erudito más respetado de su época y, por consiguiente, sus ideas influyeron a generaciones de egiptólogos futuros.

Un siglo y medio después de Kircher, en el verano de 1798, la antigüedad egipcia volvió a ser sometida a un minucioso análisis cuando Napoleón Bonaparte envió un equipo de historiadores, científicos y dibujantes para seguir los pasos de su ejército invasor. Estos académicos, o «perros pequineses», como los llamaban los soldados, realizaron un magnífico trabajo trazando planos, dibujando, midiendo y anotando todo lo que veían. En 1799, los académicos franceses dieron con la losa de piedra más famosa de la historia de la arqueología, encontrada por una tropa de soldados franceses apostados en el Fuerte Julien, en la ciudad de Rosetta, en el delta del Nilo. Se había encargado a los soldados que derribaran un antiguo muro para abrir paso a una expedición que se dirigía al fuerte. Incrustada en el muro había una piedra que tenía un extraordinario conjunto de inscripciones: el mismo texto había sido inscrito en la piedra tres veces, en griego, demótico y jeroglíficos. La Piedra Rosetta, como sería llamada, parecía ser el equivalente de un *puntal* criptoanalítico, similar a los *puntales* que ayudaron a los criptoanalistas de Bletchley a penetrar en la Enigma. Podría decirse que el griego, que resultaba fácil de leer, era un trozo de

texto llano que se podía comparar con los textos cifrados en demótico y en jeroglíficos. La Piedra Rosetta era potencialmente un medio de desentrañar el significado de los antiguos símbolos egipcios.

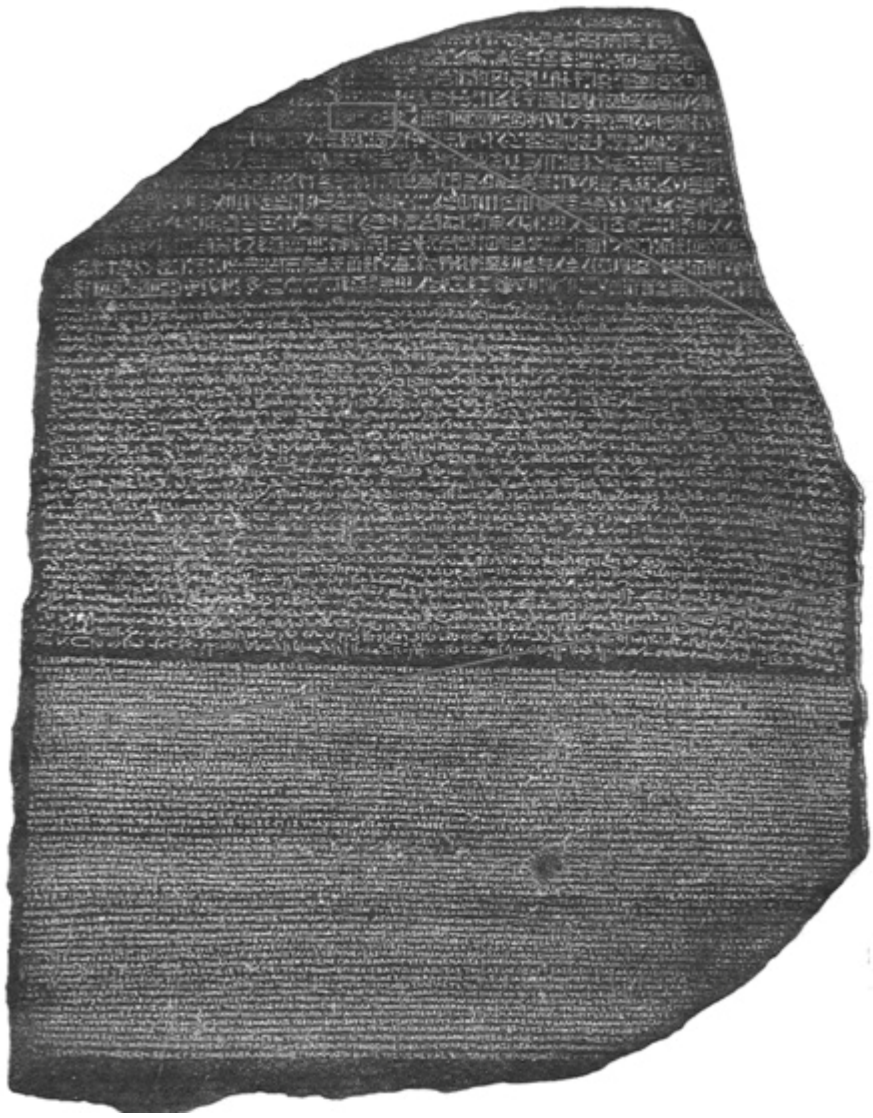


Figura 54. La Piedra Rosetta inscrita en 196 a.C. y redescubierta en 1799, contiene el mismo texto escrito en tres escrituras diferentes jeroglíficos arriba, demótica en el medios griego abajo.

Los académicos reconocieron inmediatamente la importancia de la piedra y la enviaron al Instituto Nacional de El Cairo para un estudio más detallado. Sin embargo, antes de que el instituto pudiera emprender una investigación seria quedó

claro que el ejército francés estaba a punto de ser derrotado por las fuerzas de avance británicas. Los franceses trasladaron la Piedra Rosetta de El Cairo a la seguridad relativa de Alejandría, pero irónicamente, cuando los franceses se rindieron finalmente, el artículo XVI del tratado de Capitulación entregó todas las antigüedades de Alejandría a los británicos, mientras que se permitió que las de El Cairo volvieran a Francia. En 1802, la valiosísima losa de basalto negro (que medía 118 cm de altura, 77 cm de anchura y 30 cm de grosor, y pesaba tres cuartos de tonelada) fue enviada a Portsmouth a bordo del barco de la Armada real *L'Egyptienne*, y después, en ese mismo año, se instaló en el Museo Británico, donde ha permanecido desde entonces.

La traducción del griego pronto reveló que la Piedra Rosetta contenía un decreto del consejo general de sacerdotes egipcios emitido en 196 a. C. El texto registra los beneficios que el faraón Tolomeo había concedido al pueblo egipcio, y detalla los honores que, a cambio, los sacerdotes habían otorgado al faraón. Por ejemplo, declaraban que «se mantendrá un festival en honor del rey Tolomeo, el eterno, el amado de Ptah, el dios Epífanes Eucaristos, anualmente en los templos de toda la nación desde el 1° de Troth durante cinco días, en los que se llevarán guirnaldas y se celebrarán sacrificios y libaciones y los demás honores habituales». Si las otras dos inscripciones contenían el mismo decreto idéntico, el desciframiento de los textos en jeroglíficos y demótica parecería ser sencillo. Sin embargo, quedaban tres obstáculos principales. Primero, la Piedra Rosetta está seriamente dañada, como puede verse en la Figura 54. El texto griego consta de 54 líneas, de las cuales las 26 últimas están dañadas. El texto demótico consta de 32 líneas, de las cuales el principio de las 14 primeras está dañado (obsérvese que la demótica y los jeroglíficos se escriben de derecha a izquierda). El texto jeroglífico es el que está en peores condiciones, ya que faltan completamente la mitad de las líneas, y las 14 líneas restantes (que se corresponden con las últimas 28 líneas del texto griego) faltan parcialmente. La segunda barrera al desciframiento es que las dos escrituras egipcias expresan la antigua lengua egipcia, que nadie había hablado durante al menos ocho siglos. Si bien era posible encontrar una serie de símbolos egipcios que se correspondieran con una serie de palabras griegas, lo que permitiría que los arqueólogos dedujeran el significado de los símbolos egipcios, era imposible

establecer el sonido de las palabras egipcias. A no ser que los arqueólogos conocieran cómo se decían las palabras egipcias, no podrían deducir la fonética de los símbolos.

Figura 55. Thomas Young.

Finalmente, el legado intelectual de Kircher aún alentaba a los arqueólogos a considerar la escritura egipcia en cuanto a semagramas, en vez de fonogramas, y por eso fueron muy pocos los que llegaron incluso a considerar la tentativa de un desciframiento fonético de los jeroglíficos.

Uno de los primeros estudiosos que cuestionó el prejuicio de que los jeroglíficos eran una escritura pictórica fue el prodigioso polifacético inglés Thomas Young. Nacido en 1773 en Milverton, Somerset, Young podía leer con fluidez a los dos años. Al cumplir catorce ya había estudiado griego, latín, francés, italiano, hebreo, caldeo, sirio, samaritano, árabe, persa, turco y etíope, y cuando comenzó a estudiar en el

Emmanuel College, de la Universidad de Cambridge, su brillantez le granjeó el apodo de «el Fenómeno Young». En Cambridge estudió medicina, pero se decía que sólo le interesaban las enfermedades, no los pacientes que las tenían. Gradualmente comenzó a concentrarse más en la investigación y menos en cuidar a los enfermos.

Young llevó a cabo una serie de extraordinarios experimentos médicos, muchos de ellos con el objeto de explicar cómo funciona el ojo humano. Estableció que la percepción del color es el resultado de tres tipos distintos de receptores, cada uno de ellos sensible a uno de los tres colores primarios. Luego, colocando aros de metal alrededor de un ojo ocular viviente, mostró que enfocar no requería la distorsión de todo el ojo y postuló que las lentes internas hacían todo el trabajo. Su interés por la óptica le llevó hacia la física y otra serie de descubrimientos. Publicó «La teoría ondulatoria de la luz», un artículo clásico sobre la naturaleza de la luz; creó una explicación nueva y mejor de las mareas; definió formalmente el concepto de energía y publicó innovadores artículos sobre el tema de la elasticidad. Young parecía capaz de abordar problemas en casi cualquier tema, pero ésta no era su única ventaja. Su mente se fascinaba tan fácilmente que él saltaba de un tema a otro, embarcándose en un nuevo problema antes de finalizar completamente el anterior.

Cuando Young oyó hablar de la Piedra Rosetta, ésta se convirtió en un desafío irresistible. En el verano de 1814 se puso en camino hacia su vacación anual en el pueblo costero de Worthing, llevándose consigo una copia de las tres inscripciones. El gran avance de Young se produjo cuando se centro en un conjunto de jeroglíficos enmarcados en una línea, a los que se denomina un *cartucho.* Su presentimiento fue que estos jeroglíficos estaban rodeados por una línea porque representaban algo muy importante, posiblemente el nombre del faraón Tolomeo, porque su nombre griego, Ptolemaios, se mencionaba en el texto griego. Si esto era así, permitiría a Young descubrir la fonética de los jeroglíficos correspondientes, porque el nombre de un faraón se pronunciaría aproximadamente igual sin importar la lengua. El cartucho de Tolomeo se repite seis veces en la Piedra Rosetta, a veces en una versión que se ha llamado normal, y a veces en una versión más larga y más elaborada. Young asumió que la versión grande era el nombre de Tolomeo con sus

títulos y se concentró en los símbolos que aparecían en la versión normal, adivinando el valor sonoro de cada jeroglífico (Tabla 13).

Tabla 13. El desciframiento de Young de  , el cartucho de Tolomeo (versión normal) de la Piedra Rosetta.

Jeroglífico	Valor sonoro de Young	Valor sonoro verdadero
	p	p
	t	t
	opcional	o
	lo o ole	l
	ma o m	m
	i	i o y
	osh o os	s

Aunque entonces no lo sabía, Young se las arregló para establecer la correlación entre la mayoría de los jeroglíficos y su valor sonoro correcto. Afortunadamente, había situado los dos primeros jeroglíficos (□ ^{Q}), que aparecían uno encima del otro, en su orden fonético correcto. El escriba había colocado los jeroglíficos de esta manera por razones estéticas, a expensas de la claridad fonética. Los escribas tendían a escribir de ese modo para evitar los espacios en blanco y mantener la armonía visual; a veces incluso intercambiaban la posición de las letras contradiciendo cualquier regla de ortografía, simplemente para aumentar la belleza de una inscripción. Después de este desciframiento, Young descubrió un cartucho en una inscripción copiada del templo de Karnak, en Tebas, y sospechó que era el nombre de una reina tolemaica: Berenika (o Berenice).

Repitió la misma estrategia; los resultados se muestran en la Tabla 14.

Tabla 14. El desciframiento de Young de  , el cartucho Berenika del templo de Karnak.

Jeroglífico	Valor sonoro de Young	Valor sonoro verdadero
	bir	b
	e	r
	n	n
	i	i
	opcional	k
	ke o ken	a
	terminación femenina	terminación femenina

De los trece jeroglíficos de ambos cartuchos, Young había descifrado la mitad de ellos perfectamente y un cuarto parcialmente bien. También había identificado correctamente el símbolo de la terminación femenina, colocado tras los nombres de reinas y diosas. Aunque no podía saber el nivel de su éxito, la aparición de M en ambos cartuchos, representando a la i en ambas ocasiones, debió indicar a Young que iba por buen camino y darle la confianza que necesitaba para seguir adelante con los desciframientos. Sin embargo, su trabajo se detuvo de repente. Parece ser que tenía demasiado respeto al argumento de Kircher de que los jeroglíficos eran semagramas, y no estaba dispuesto a echar por tierra ese paradigma. Justificó sus propios descubrimientos fonéticos señalando que la dinastía tolemaica era descendiente de Lagus, un general de Alejandro Magno. En otras palabras, los tolomeos eran extranjeros, y Young propuso la hipótesis de que sus nombres tuvieron que ser deletreados porque no había para ellos un solo semagrama natural en la lista normal de jeroglíficos. Resumió sus ideas comparando los jeroglíficos con los caracteres chinos, que los europeos estaban entonces empezando a comprender:

> *Es sumamente interesante localizar algunos de los pasos mediante los que la escritura alfabética parece haber surgido de la jeroglífica; un proceso que efectivamente podría ser ilustrado en cierta medida por la manera en que los chinos modernos expresan una combinación extranjera de sonidos, convirtiendo simplemente los caracteres en «fonéticos» mediante una señal apropiada, en vez de retener su significado natural, y esta señal, en algunos libros*

impresos modernos, se acerca mucho al aro que rodea los nombres jeroglíficos.

Young llamó a estos logros «*el entretenimiento de unas pocas horas de ocio*». Perdió el interés en los jeroglíficos y concluyó su trabajo resumiéndolo en un artículo para el Suplemento de la Enciclopedia Británica *de 1819.*

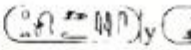
Mientras tanto, en Francia, un joven y prometedor lingüista, Jean-François Champollion, estaba listo para llevar las ideas de Young a su conclusión natural. Aunque aún no había llegado a los treinta años, Champollion llevaba ya casi dos décadas fascinado por los jeroglíficos.

Figura 56. Jean-François Champollion

La obsesión comenzó en 1880, cuando el matemático francés Jean-Baptiste Fourier, que había sido uno de los primeros «perros pequineses» de Napoleón, enseñó a

Champollion, que entonces tenía diez años, su colección de antigüedades egipcias, muchas de las cuales estaban decoradas con extrañas inscripciones. Fourier le explicó que nadie podía interpretar esta escritura críptica y entonces el chico prometió que un día él resolvería el misterio. Sólo siete años después, cuando tenía diecisiete años, presentó un artículo titulado «Egipto bajo los Faraones». Era tan innovador que Champollion fue elegido inmediatamente para la Academia de Grenoble. Cuando se enteró de que se había convertido en un profesor adolescente, Champollion se emocionó tanto que se desmayó en el acto.

Champollion continuó sorprendiendo a sus coetáneos, dominando el latín, el griego, el hebreo, el etíope, el sánscrito, el zendo, el palevi, el árabe, el sirio, el caldeo, el persa y el chino, todo con la intención de armarse para el asalto a los jeroglíficos. Su obsesión la ilustra un incidente de 1808, cuando se encontró en la calle con un viejo amigo. El amigo mencionó casualmente que Alexander Lenoir, un conocido egiptólogo, había publicado un desciframiento completo de los jeroglíficos. Champollion se sintió tan destrozado que perdió el sentido en el acto. (Parece ser que tenía mucho talento para los desmayos). Su única razón para vivir parecía depender de ser el primero en leer la escritura de los antiguos egipcios. Afortunadamente para Champollion, los desciframientos de Lenoir eran tan fantasiosos como las tentativas del siglo XVII de Kircher, y el desafío continuó.

Tabla 15. El desciframiento de Champollion de  y  , los cartuchos de Tolomeo y Cleopatra del obelisco de Bankes.

Jeroglífico	Valor sonoro
	p
	t
	o
	l
	m
	e
	s

Jeroglífico	Valor sonoro
	c
	l
	e
	o
	p
	a
	t
	r
	a

En 1822, Champollion aplicó el enfoque de Young a otros cartuchos. El naturalista británico W. J. Bankes había llevado a Dorset un obelisco con inscripciones griegas y jeroglíficas, y había publicado recientemente una litografía de estos textos bilingües, que incluían cartuchos de Tolomeo y Cleopatra. Champollion consiguió una reproducción y logró asignar valores sonoros a jeroglíficos individuales (Tabla 15). Las letras p, t, o, l y e aparecían en los dos nombres; en cuatro de los casos estaban representadas por el mismo jeroglífico tanto en Tolomeo como en Cleopatra, y en un solo caso, la t, había una discrepancia. Champollion supuso que el sonido t podía ser representado por dos jeroglíficos, de igual manera que en inglés el sonido duro c se puede representar por medio de la c o de la k, como en *cat* (gato) y en *kid* (chaval). Inspirado por su éxito, Champollion comenzó a tratar cartuchos que carecían de traducción bilingüe, sustituyendo siempre que podía los valores sonoros de los jeroglíficos que ya había derivado de los cartuchos de Tolomeo y Cleopatra. Su primer cartucho misterioso (Tabla 16) contenía uno de los nombres más importantes de los tiempos antiguos. A Champollion le resultaba obvio que la tarjeta, que parecía leerse como a-l-?-s-e-?-t-r-?, representaba el nombre alksentrs, Alexandros en griego, o Alejandro en castellano. También le pareció evidente a Champollion que a los escribas no les gustaba utilizar las vocales, y a menudo las omitían; los escribas asumían que los lectores no tendrían problemas para rellenar las vocales que faltaban Con otros dos jeroglíficos en su haber, el joven erudito estudió otras inscripciones y descifró una serie de cartuchos. Sin embargo, todos estos progresos eran meramente una extensión del trabajo de Young. Todos estos nombres, como Alejandro o Cleopatra, todavía eran extranjeros, lo que apoyaba la teoría de que sólo se recurría a la fonética para las palabras que quedaban fuera del léxico egipcio tradicional.

Luego, el 14 de septiembre de 1822, Champollion recibió unos relieves procedentes del templo de Abú Simbel, que contenían cartuchos que precedían al período de la dominación grecorromana. La importancia de estos cartuchos radicaba en que eran lo suficientemente antiguos como para contener nombres egipcios tradicionales y, sin embargo, aún aparecían deletreados: una clara prueba contra la teoría de que

sólo se recurría a deletrear en el caso de los nombres extranjeros. Champollion se centró en un cartucho que sólo contenía cuatro jeroglíficos: 

Los dos primeros símbolos eran desconocidos, pero del par repetido al final, W, se sabía, porque aparecía en el cartucho de Alejandro (alksentrs), que representaba dos veces la letra s. Esto significaba que el cartucho representaba (?-?-s-s). Entonces, Champollion recurrió a sus amplios conocimientos lingüísticos. Aunque el copto, el descendiente directo de la antigua lengua egipcia, había dejado de ser una lengua viva en el siglo XI, todavía existía en forma fosilizada en la liturgia de la Iglesia cristiana copta. Champollion había aprendido el copto cuando aún era un adolescente, y lo dominaba tanto que lo usaba para escribir en su diario. Sin embargo, hasta ese momento, nunca había pensado que el copto podría ser también la lengua de los jeroglíficos.

Champollion se preguntó si el primer signo del cartucho, ©, podría ser un semagrama que representase al sol, esto es, un dibujo del sol sería el símbolo de la palabra «sol». A continuación, en un acto de genio intuitivo, supuso que el valor sonoro del semagrama sería el de la palabra copta para sol, ra. Esto le dio la secuencia (ra- ?-s-s). Sólo un nombre faraónico parecía encajar. Teniendo en cuenta la irritante omisión de vocales, y suponiendo que la letra que faltaba era la m, entonces sin duda tendría que ser el nombre de Ramsés, uno de los faraones más importantes, y uno de los más antiguos. Se había roto el hechizo. Incluso los nombres tradicionales se escribían fonéticamente. Champollion corrió a la oficina de su hermano y proclamó *«Je tiens l'affaire!»*. («¡Ya lo tengo!»), pero, una vez más, su intensa pasión por los jeroglíficos fue más fuerte que él. No tardó en perder el conocimiento y estuvo postrado en cama los cinco días siguientes.

Champollion había demostrado que los escribas a veces sacaban partido al principio de un tipo de adivinanza. En estas adivinanzas, que aún aparecen en los pasatiempos para niños, las palabras largas se descomponen en sus componentes fonéticos, que luego se representan mediante semagramas.

Tabla 16. El desciframiento de Champollion de  , el cartucho de Alksentrs (Alejandro).

Jeroglífico	Valor sonoro
	a
	l
	?
	s
	e
	?
	t
	r
	?

Por ejemplo, la palabra inglesa *belief* (creencia) se puede descomponer en dos sílabas, *be-lief* que entonces se puede reescribir como *bee-leaf* (abeja-hoja[17]). En vez de escribir la palabra fonéticamente, se puede representar con la imagen de una abeja seguida de la imagen de una hoja. En el ejemplo descubierto por Champollion, sólo la primera sílaba ra se representa mediante una imagen de adivinanza, un dibujo del sol, mientras que el resto de la palabra se escribe más convencionalmente.

La trascendencia del semagrama del sol en el cartucho de Ramsés es enorme, porque restringe claramente las posibilidades acerca de la lengua que hablaban los escribas. Por ejemplo, los escribas no podían haber hablado el griego, porque eso

[17] La pronunciación inglesa de la palabra belief (creencia) es identica a la de la combinación de palabras bee-leaf (abeja-hoja). (N. del T.)

habría significado que el cartucho se pronunciaría «helios- mses». El cartucho sólo tiene sentido si los escribas hablaban un tipo de copto, porque entonces el cartucho se pronunciaría «ra-mses».

Aunque éste era un cartucho más, su desciframiento demostró claramente los cuatro principios fundamentales de los jeroglíficos. Primero, la lengua de la escritura por lo menos está relacionada con el copto, y, efectivamente, el examen de otros jeroglíficos mostró que se trataba de copto puro y simple. Segundo, los semagramas se utilizaban para representar algunas palabras, p. e., la palabra «sol» se representa con un simple dibujo del sol. Tercero, para la mayor parte de lo que escribían, los antiguos escribas utilizaban un alfabeto fonético relativamente convencional. Este último punto es el más importante, y Champollion afirmó que la fonética era el «alma» de los jeroglíficos.

Usando su profundo conocimiento del copto, Champollion comenzó un desciframiento sin obstáculos y prolífico de los jeroglíficos que no estaban en las tarjetas. En menos de dos años identificó los valores fonéticos de la mayoría de los jeroglíficos y descubrió que algunos de ellos representaban combinaciones de dos o incluso tres consonantes. Esto a veces ofrecía a los escribas la opción de escribir una palabra usando muchos jeroglíficos simples o sólo unos pocos jeroglíficos multiconsonánticos.

Champollion envió sus resultados iniciales al señor Dacier, secretario permanente de la Academia Francesa de Inscripciones. Después, en 1824, a la edad de treinta y cuatro años, Champollion publicó todos sus logros en un libro titulado *Précis du systéme hiéroglyphique.* Por primera vez en catorce siglos era posible leer la historia de los faraones, tal como la habían escrito los escribas. Para los lingüistas, esto presentaba la oportunidad de estudiar la evolución de una lengua y una escritura a lo largo de un período de más de tres mil años. Los jeroglíficos se podían comprender y trazar desde el tercer milenio a. C. hasta el siglo cuarto de nuestra era. Además, la evolución de los jeroglíficos se podía comparar con las escrituras hierática y demótica, que ahora también podrían ser descifradas.

Durante muchos años, la política y las envidias impidieron que el magnífico logro de Champollion fuera aceptado universalmente. Thomas Young fue un crítico particularmente acerbo. En algunas ocasiones, Young negaba que los jeroglíficos

pudieran ser en su mayor parte fonéticos; otras veces, aceptaba el argumento, pero se quejaba de que había sido él quien había llegado a esa conclusión antes que Champollion y que el francés se había limitado a rellenar las lagunas. Gran parte de la hostilidad de Young fue el resultado del hecho que Champollion no le dio ningún crédito, a pesar de que es probable que los logros iniciales de Young le dieran la inspiración para el desciframiento completo.

En julio de 1828 Champollion emprendió su primera expedición a Egipto, que duró dieciocho meses. Era una oportunidad extraordinaria para ver directamente las inscripciones que previamente sólo había visto en dibujos o litografías. Treinta años antes, la expedición de Napoleón había hecho todo tipo de conjeturas sobre el significado de los jeroglíficos que adornaban los templos, pero ahora Champollion podía simplemente leerlos carácter por carácter y reinterpretarlos correctamente. Su visita sucedió justo a tiempo. Tres años después, tras haber redactado sus notas, dibujos y traducciones procedentes de su expedición a Egipto, sufrió un grave derrame cerebral. La racha de desmayos que había sufrido a lo largo de su vida era quizá sintomática de una enfermedad mucho más seria, exacerbada por su obsesivo e intenso estudio. Murió el 4 de marzo de 1832, a los cuarenta y un años.

2. El misterio del Lineal B

Los dos siglos transcurridos desde los logros de Champollion, los egiptólogos han seguido mejorando su comprensión de las complejidades de los jeroglíficos. Su nivel de comprensión es ahora tan alto que los eruditos son capaces de desenmarañar jeroglíficos codificados, que están entre los textos cifrados más antiguos del mundo. Algunas de las inscripciones encontradas en las tumbas de los faraones estaban codificadas utilizando una variedad de técnicas, incluida la cifra de sustitución. A veces se usaban símbolos inventados en vez del jeroglífico establecido y en otras ocasiones se empleaba un jeroglífico fonéticamente diferente pero visualmente similar en vez del correcto. Por ejemplo, el jeroglífico del áspid con cuernos, que normalmente representa a la f, se usaba en vez de la serpiente, que representa a la z. Generalmente, estos epitafios codificados no se hacían con la intención de ser indescifrables, sino que más bien servían como rompecabezas crípticos para

despertar la curiosidad de los transeúntes, a los que se tentaba de esta forma para que permanecieran más tiempo junto a una tumba en vez de pasar de largo.

Tras haber conquistado los jeroglíficos, los arqueólogos pasaron a descifrar muchas otras escrituras antiguas, incluidos los textos cuneiformes de Babilonia, las runas Kók-Turki de Turquía y el alfabeto brahmi de India. Sin embargo, la buena noticia para los Champollion en ciernes es que aún quedan muchas excelentes escrituras por descifrar, como la etrusca y ciertas escrituras indostaníes (véase el Apéndice F). La gran dificultad para descifrar las escrituras que quedan es que no hay *puntales*, ni nada que permita al descifrador desvelar el significado de estos textos antiguos.

Con los jeroglíficos egipcios fueron los cartuchos los que sirvieron de *puntales*, dando a Young y a Champollion la primera pista sobre la base fonética subyacente. Sin *puntales*, el desciframiento de una escritura antigua podría parecer imposible, pero hay un notable ejemplo de una escritura que fue desenmarañada sin la ayuda de un *puntal.* El Lineal B, una escritura cretense que se remonta a la Edad de Bronce, fue descifrado sin ninguna pista de ayuda legada por los antiguos escribas. Fue resuelto mediante una combinación de lógica e inspiración, un potente ejemplo de criptoanálisis puro. De hecho, el desciframiento del Lineal B se considera generalmente como el mayor de los logros arqueológicos.

La historia del Lineal B comienza con las excavaciones de sir Arthur Evans, uno de los arqueólogos más eminentes de principios de siglo. Evans estaba interesado en el período de la historia de Grecia descrito por Homero en sus poemas épicos gemelos, la *Ilíada* y la *Odisea.* Homero relata la historia de la guerra de Troya, la victoria griega en Troya y las proezas subsiguientes del héroe conquistador Ulises, sucesos que supuestamente tuvieron lugar en el siglo XII a. C.

Algunos eruditos del siglo XIX habían considerado los poemas épicos de Homero como meras leyendas, pero en 1872 el arqueólogo alemán Heinrich Schliemann excavó el emplazamiento de la misma Troya, cerca de la costa occidental de Turquía, y de pronto los mitos homéricos se convirtieron en Historia. Entre 1872 y 1900, los arqueólogos descubrieron aún más pruebas que sugieren un rico período de la historia prehelénica, que precedía a la era clásica griega de Pitágoras, Platón y Aristóteles en unos seiscientos años. El período prehelénico duró desde 2800 a 1100 a. C., y fue durante los últimos cuatro siglos de esta etapa cuando la civilización

alcanzó su cima. En la península griega se centraba en torno a Micenas, donde los arqueólogos excavaron una gran variedad de artefactos y tesoros. Sin embargo, a sir Arthur Evans le había dejado perplejo el hecho de que los arqueólogos no descubrieran ninguna forma de escritura. No podía aceptar que una sociedad tan sofisticada hubiera sido totalmente analfabeta, y se decidió a demostrar que la civilización micénica tenía alguna forma de escritura.

Figura 57. Antiguos emplazamientos en torno al mar Egeo. Tras descubrir tesoros en Micenas, en la península griega, sir Arthur Evans emprendió la búsqueda de tablillas inscritas. Las primeras tablillas del Lineal B fueron descubiertas en la isla de Creta, el centro del imperio minoico.

Después de ponerse en contacto con varios comerciantes de antigüedades en Atenas, sir Arthur encontró finalmente algunas piedras grabadas, que parecían ser sellos que se remontaban a la era prehelénica. Los signos que aparecían en los sellos parecían ser emblemáticos en vez de escritura genuina, similares a los símbolos que se usan en heráldica. Sin embargo, este descubrimiento le dio el ímpetu necesario para continuar su búsqueda. Se decía que los sellos procedían de

la isla de Creta, y en particular de Cnosos, donde según la leyenda se encontraba el palacio del rey Minos, el centro de un imperio que dominaba el Egeo. Sir Arthur partió para Creta y comenzó a excavar en marzo de 1900. Los resultados fueron tan espectaculares como rápidos.

Excavó los restos de un lujoso palacio, repleto de una intrincada red de pasadizos y adornado con frescos de muchachos saltando sobre feroces toros. Evans especuló que el deporte del salto de toro estaba ligado de alguna forma con la leyenda del Minotauro, el monstruo con cabeza de toro que se alimentaba de jovencitos, y sugirió que la complejidad de los pasillos del palacio había inspirado la historia del laberinto del Minotauro.

El 31 de marzo, sir Arthur comenzó a desenterrar el tesoro que más había deseado. Inicialmente descubrió una sola tablilla de arcilla con una inscripción y pocos días después un cofre de madera lleno de esas tablillas, y luego reservas de material escrito que superaban todas sus expectativas. Originalmente, todas estas tablillas de arcilla habían sido secadas al sol, en vez de ser cocidas, para poder reciclarse simplemente añadiendo agua. A lo largo de los siglos, la lluvia debería haber disuelto las tablillas, que se habrían perdido para siempre. Sin embargo, parece ser que el palacio de Cnosos había sido destruido por un incendio, que coció las tablillas y contribuyó a preservarlas durante tres mil años. Estaban en tan buen estado que aún era posible distinguir las huellas digitales de los escribas.

Las tablillas comprendían tres categorías. La primera serie de tablillas, que databan desde 2000 a 1650 a. C., consistía meramente en dibujos, probablemente semagramas, aparentemente relacionados con los símbolos de los sellos que sir Arthur Evans había comprado a los comerciantes de Atenas. La segunda serie de tablillas, que databa desde 1750 a 1450 a. C., estaban inscritas con caracteres que consistían en simples líneas, por lo que esa escritura recibió el nombre de Lineal A. La tercera serie de tablillas, que databa desde 1450 a 1375 a. C., tenía una escritura que parecía ser un Lineal A perfeccionado, por lo que fue llamada Lineal B. Como la mayoría de las tablillas eran Lineal B, y como era la escritura más reciente, sir Arthur y otros arqueólogos creían que el Lineal B ofrecía la mejor posibilidad de desciframiento.

Muchas de las tablillas parecían contener inventarios. Con tantas columnas de caracteres numéricos era relativamente fácil deducir el sistema numeral, pero los caracteres fonéticos eran muchísimo más desconcertantes. Parecían una colección sin sentido de garabatos arbitrarios. El historiador David Kahn describió algunos de los caracteres individuales como «*un arco gótico rodeando una línea vertical, una escalera, un corazón atravesado por una raíz, un tridente doblado con una lengüeta, un dinosaurio de tres patas mirando hacia atrás, una A con una línea horizontal extra que la cruza, una S al revés, un vaso alto de cerveza, medio lleno, con un lazo atado en el borde; docenas de ellos no se parecen a nada en absoluto*». Sólo se pudieron establecer dos hechos útiles acerca del Lineal B.

Primero, la dirección de la escritura era claramente de izquierda a derecha, ya que cualquier espacio al final de una línea quedaba generalmente a la derecha. Segundo, había 90 caracteres distintos, lo que implicaba que la escritura era, casi sin duda silábica. Las escrituras puramente alfabéticas tienden a tener entre 20 y 41 caracteres (el ruso, por ejemplo, tiene 36 signos, y el árabe, 28). En el otro extremo, las escrituras que se basan en semagramas tienden a tener cientos o incluso miles de signos (el chino tiene más de 5.000). Las escrituras silábicas ocupan el punto medio, con entre 50 y 100 caracteres silábicos. Aparte de estos dos hechos, el Lineal B era un misterio insondable.

El problema fundamental era que nadie podía estar seguro de en qué idioma estaba escrito el Lineal B. Inicialmente, se especuló que el Lineal B era una forma escrita del griego, porque siete de los caracteres tenían gran similitud con caracteres de la escritura chipriota clásica, que se sabía que era una forma de escritura griega utilizada entre 600 y 200 a. C. Pero comenzaron a surgir dudas. La consonante final más frecuente en griego es la s, y, por consiguiente, el carácter final más frecuente en la escritura chipriota es

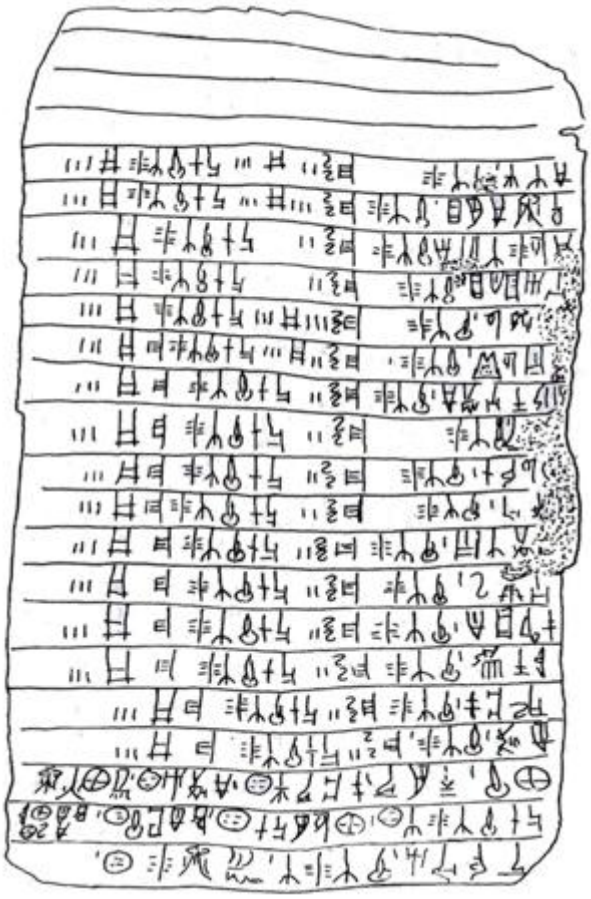
que representa la sílaba se; como los caracteres son silábicos, una consonante sola tiene que ser representada por una combinación de consonante-vocal, en la que la

vocal permanece muda. Este mismo carácter aparece también en el Lineal B, pero casi nunca se encuentra al final de una palabra, indicando que el Lineal B no podía ser el griego. El consenso general era que el Lineal B, una escritura más antigua, representaba una lengua desconocida y extinta. Cuando esta lengua se extinguió, la escritura permaneció y evoluciono a lo largo de los siglos hasta convertirse en la escritura chipriota, que se usaba para escribir el griego. Por tanto, las dos escrituras parecían similares pero expresaban lenguas totalmente diferentes.

Figura 58. Una tablilla del Lineal B, de aproximadamente 1400 a.C

Sir Arthur Evans era un gran partidario de la teoría de que el Lineal B no era una forma escrita del griego y creía que representaba una lengua nativa de Creta. Estaba convencido de que había una fuerte evidencia arqueológica para apoyar su argumento. Por ejemplo, sus descubrimientos en la isla de Creta sugerían que el imperio del rey Minos, conocido como el imperio minoico, era mucho más avanzado

que la civilización micénica de la península. El imperio minoico no era un dominio del imperio micénico, sino su rival, posiblemente incluso el poder dominante. El mito del Minotauro apoyaba esta posición. La leyenda describía cómo el rey Minos exigía que los atenienses le enviaran grupos de jovencitos y doncellas para ser sacrificados al Minotauro. En resumen Evans concluyó que los minoicos eran tan prósperos que habrían retenido su lengua nativa, en vez de adoptar el griego, el idioma de sus rivales.



Aunque llegó a ser ampliamente aceptado que los minoicos hablaban su propia lengua, diferente del griego (y el Lineal B representaba esta lengua), había uno o dos herejes que alegaban que los minoicos escribían y hablaban el griego. Sir Arthur no se tomó semejante disensión a la ligera e hizo uso de su influencia para castigar a los que no estaban de acuerdo con él. Cuando A. J. B. Wace, profesor de Arqueología en la Universidad de Cambridge, se pronunció a favor de la teoría de

que el Lineal B representaba al griego, sir Arthur lo excluyó de todas sus excavaciones y le obligó a retirarse de la Escuela Británica de Atenas.

En 1939 la controversia del «griego contra no-griego» creció cuando Cari Blegen, de la Universidad de Cincinnati, descubrió una nueva remesa de tablillas del Lineal B en el palacio de Néstor, en Pilos. Esto era extraordinario, ya que Pilos está en la península griega y habría formado parte del imperio micénico, no del minoico. La minoría de los arqueólogos que creían que el Lineal B era griego alegaron que esto apoyaba su hipótesis: el Lineal B se había encontrado en la península, donde hablaban griego, por tanto, el Lineal B representaba el griego; el Lineal B también se había encontrado en Creta, de modo que los minoicos de Creta también hablaban en griego. La facción de Evans planteó el argumento a la inversa: los minoicos de Creta hablaban la lengua minoica; el Lineal B fue encontrado en Creta, por tanto, el Lineal B representa la lengua minoica; el Lineal B también se encontró en la península, de modo que también se hablaba el minoico en la península. Sir Arthur se mostró enfático: «*No hay lugar en Micenas para reyes que hablaban griego... la cultura, como la lengua, era aún minoica hasta la médula*».

En realidad, el descubrimiento de Blegen no significaba necesariamente que los micénicos o los minoicos hablaran una sola lengua. En la Edad Media, muchos estados europeos, cualquiera que fuese su lengua nativa, seguían escribiendo sus archivos en latín Quizá la lengua del Lineal B era asimismo una *lingua franca* entre los contables del Egeo, permitiendo así la facilidad del comercio entre naciones que no hablaban una lengua común.

Durante cuatro décadas, todas las tentativas de descifrar el Lineal B desembocaron en el fracaso. Luego, en 1941, sir Arthur murió a la edad de noventa años. No vivió lo suficiente para presenciar el desciframiento del Lineal B, o para leer por sí mismo el significado de los textos que había descubierto. De hecho, en aquellos momentos parecía haber muy pocas perspectivas de llegar a descifrar alguna vez el Lineal B.

3. Sílabas de unión

Tras la muerte de sir Arthur Evans, el archivo de tablillas del Lineal B y sus propias notas arqueológicas quedaron disponibles tan sólo para un círculo restringido de arqueólogos, a saber, los que apoyaban su teoría de que el Lineal B representaba

una lengua minoica propia. Sin embargo, a mediados de los años cuarenta, Alice Kober, una clasicista del Brooklyn College, se las arregló para acceder al material y comenzó un análisis meticuloso e imparcial de la escritura. Para los que sólo la conocían de vista, Kober parecía bastante corriente: una profesora sin gracia, ni encantadora ni carismática, con una actitud vital prosaica. Sin embargo, su pasión por su investigación era inconmensurable. «Trabajaba con una intensidad contenida», recuerda Eva Brann, una antigua estudiante que llegó a ser arqueóloga en la Universidad de Yale. «*Una vez me dijo que la única manera de saber si has hecho algo realmente grande es cuando sientes un hormigueo por la columna vertebral*».

Figura 59. Alice Kober

Kober se dio cuenta de que para descifrar el Lineal B tendría que abandonar todas las ideas preconcebidas. Se concentró sólo en la estructura de la escritura en

conjunto y en la construcción de palabras individuales. En particular, notó que ciertas palabras formaban tríos, en la medida que parecían ser la misma palabra que reaparecía en tres formas ligeramente variadas. En un trío de palabras, las raíces parecían idénticas, pero había tres terminaciones posibles. Kober concluyó que el Lineal B representaba una lengua altamente declinable, lo que significa que las terminaciones de las palabras se cambian para reflejar el género, el tiempo, el caso, etcétera. El inglés es ligeramente declinable, porque, por ejemplo, el verbo añade una «s» para formar la tercera persona del singular. Sin embargo, las lenguas más antiguas tienden a ser mucho más rígidas y extremas en su uso de semejantes terminaciones. Kober publicó un artículo en el que describía la naturaleza declinable de dos grupos particulares de palabras, tal como se muestra en la Tabla 17. Cada grupo conserva su raíz respectiva y toma diferentes terminaciones según tres casos diferentes.

Tabla 17

Los signos del Lineal 3 y los números que fueron asignados.

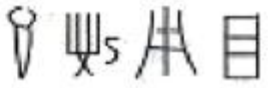
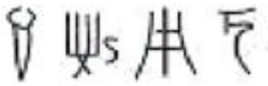
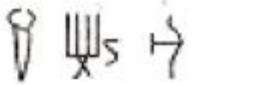
	Palabra A	Palabra B
Caso 1		
Caso 2		
Caso 3		

Tabla 18

Los signos del Lineal 3 y los números que fueron asignados.

Para simplificar, se asignó un número de dos cifras a cada símbolo del Lineal B, como se muestra en la Tabla 18. Usando estos números, las palabras de la Tabla 17 se pueden escribir como en la Tabla 19. Ambos grupos de palabras podrían ser nombres que cambian de terminación dependiendo de su caso: el caso 1 podría ser nominativo, el caso 2 acusativo y el caso 3 dativo, por ejemplo. Es evidente que los dos primeros signos en ambos grupos de palabras (25-67- y 70-52-) son raíces, ya que se repiten independientemente del caso. Sin embargo, el tercer signo es de alguna forma más desconcertante. Si el tercer signo formara parte de la raíz, entonces debería permanecer constante para una palabra dada, independientemente del caso, pero esto no es lo que sucede. En la palabra A el tercer signo es 37 para los casos 1 y 2, pero 05 para el caso 3. En la palabra B el tercer signo es 41 para los casos 1 y 2, pero 12 para el caso 3. De manera alternativa, si el tercer signo no forma parte de la raíz quizá forme parte de la terminación, pero esta posibilidad es igualmente problemática. Para un caso dado, la terminación debería ser la misma independientemente de la palabra, pero para los casos 1 y 2 el tercer signo es 37 en la palabra A, pero 41 en la palabra B, y para el caso 3 el tercer signo es 05 en la palabra A, pero 12 en la palabra B.

Tabla 19

Las dos palabras declinables del Lineal B reescritas en números.

	Palabra A	Palabra B
Caso 1	25-67-37-57	70-52-41-57
Caso 2	25-67-37-36	70-52-41-36
Caso 3	25-67-05	70-52-12

Los terceros signos desafiaban las expectativas porque no parecían formar parte ni de la raíz ni de la terminación. Kober resolvió la paradoja invocando la teoría de que cada signo representa una sílaba, probablemente una combinación de una consonante seguida de una vocal. Propuso que la tercera sílaba podría ser una sílaba de unión, que representaba parte de la raíz y parte de la terminación. La consonante podría contribuir a la raíz y la vocal a la terminación. Para ilustrar su

teoría dio un ejemplo de la lengua acadia, que también tiene sílabas de unión y que es altamente declinable. *Sadanu* es un nombre acadio de caso 1, que cambia a *sadani* en el caso segundo y a *sadu* en el caso tercero (Tabla 20). Es evidente que las tres palabras constan de una raíz, sad-, y una terminación, -anu (caso 1), - ani (caso 2), o -u (caso 3), con -da-, - da- o -du como sílaba de unión. La sílaba de unión es la misma en los casos 1 y 2, pero otra diferente en el caso 3. Este es exactamente el patrón que se observa en las palabras del Lineal B: el tercer signo en cada una de las palabras del Lineal B estudiadas por Kober debía ser una sílaba de unión.

Tabla 20

Sílaba de unión en el nombre aeadio sadanu.

Caso 1	sa-da-nu
Caso 2	sa-da-ni
Caso 3	sa-du

La mera identificación de la naturaleza declinable del Lineal B y la existencia de silabas de unión significó que Kober había progresado más que nadie en el desciframiento de la escritura minoica y, sin embargo, esto era sólo el principió. Estaba a punto de hacer una deducción aún mayor. En el ejemplo acadio, la sílaba de unión cambia de -da- a -du-, pero la consonante es la misma en las dos sílabas. De manera similar, las sílabas 37 y 05 del Lineal B en la palabra A deben compartir la misma consonante, así como también las sílabas 41 y 12 en la palabra B. Por primera vez desde que Evans había descubierto el Lineal B empezaban a surgir hechos acerca de la fonética de los caracteres. Kober pudo establecer también otra serie de relaciones entre los caracteres. Es evidente que las palabras A y B del Lineal B deberían tener la misma terminación en el caso 1. Sin embargo, la sílaba de unión cambia de 37 a 41.

Esto supone que los signos 37 y 41 representan sílabas con consonantes diferentes pero vocales idénticas. Esto explicaría por qué los signos son diferentes, si bien mantienen la misma terminación para las dos palabras. De manera similar para los

nombres del caso 3, las sílabas 05 y 12 tendrán una vocal común pero consonantes diferentes.

Kober no consiguió localizar con total precisión cuál es la vocal común para 05 y 12, y para 37 y 41; de manera similar, tampoco pudo identificar exactamente cuál es la consonante común para 37 y 05, y para 41 y 12. Sin embargo, independientemente de sus valores fonéticos absolutos, Kober había establecido relaciones rigurosas entre ciertos caracteres. Los resultados los resumió en una tabla como la de la Tabla 21. Lo que esto nos dice es que Kober no tenía idea de qué sílaba era representada por el signo 37, pero sabía que su consonante la compartía con el signo 05, y su vocal con el signo 41. De modo parecido, no tenía idea de qué sílaba era representada por el signo 12, pero sabía que su consonante la compartía con el signo 41 y su vocal con el signo 05. Luego aplicó su método a otras vocales y llegó a construir una tabla de diez signos, con dos vocales y cinco consonantes. Es bastante posible que Kober habría dado el siguiente paso crucial en el desciframiento e incluso que podría haber descifrado toda la escritura. Sin embargo, no vivió lo suficiente para sacar partido a las repercusiones de su trabajo. En 1950, a la edad de cuarenta y tres años, murió de cáncer de pulmón.

Tabla 21

La tabla de Kober de las relaciones entre caracteres del lineal B

	Vocal 1	Vocal 2
Consonante I	37	05
Consonante II	41	12

4. Una digresión frívola

Justo unos pocos meses antes de morir, Alice Kober recibió una carta de Michael Ventris, un arquitecto inglés que había estado fascinado por el Lineal B desde que era un niño. Ventris había nacido el 12 de julio de 1922, hijo de un oficial del ejército inglés y su esposa, de ascendencia polaca. Su madre fue, en gran medida, la que le inculcó el interés por la arqueología, acompañándole regularmente al Museo Británico, donde el joven podía embelesarse ante las maravillas del mundo antiguo. Michael era un niño brillante, con un talento especialmente prodigioso para

los idiomas. Cuando empezó a ir a la escuela, fue a Gstaad, en Suiza, y pronto dominó el francés y el alemán. Luego, a los seis años, se enseñó a sí mismo el polaco.

Como Jean-Frangois Champollion, Ventris se apasionó desde muy joven por las escrituras antiguas. A los siete años estudió un libro sobre los jeroglíficos egipcios, una hazaña impresionante para alguien tan joven, sobre todo porque el libro estaba escrito en alemán. Este interés por los escritos de las civilizaciones antiguas le acompañó a lo largo de toda su infancia. En 1936, a los catorce años, se avivó todavía más cuando acudió a una conferencia dada por sir Arthur Evans, el descubridor del Lineal B. El joven Ventris descubrió los detalles de la civilización minoica y del misterio del Lineal B y se prometió a sí mismo que descifraría esa escritura. Ese día nació una obsesión que acompañaría a Ventris a lo largo de su corta pero brillante vida.

Figura 60. Michael Ventris

Cuando tenía tan sólo dieciocho años compendió sus ideas iniciales sobre el Lineal B en un artículo que sería publicado en el altamente respetado *American Journal oj Archaeology.* Cuando presentó el artículo, tuvo buen cuidado de ocultar su edad a los editores de la publicación, por miedo a que no le tomasen en serio. Su artículo apoyaba muchísimo las críticas que sir Arthur había hecho a la hipótesis griega, alegando que «la teoría de que el minoico podría ser el griego se basa, por supuesto, en un desprecio deliberado a la verosimilitud histórica». Su propia creencia era que el Lineal B estaba relacionado con el etrusco, un punto de vista razonable, ya que existían pruebas de que los etruscos habían venido del Egeo antes de establecerse en Italia. Aunque su artículo no contenía ninguna tentativa de desciframiento, concluía con mucha confianza: «Se puede hacer».

Ventris se hizo arquitecto en vez de arqueólogo profesional, pero continuó apasionándose por el Lineal B, dedicando todo su tiempo libre al estudio de todos los aspectos de esa escritura. Cuando se enteró del trabajo de Alice Kober se mostró deseoso de conocer a fondo su avance y le escribió pidiéndole más detalles. Aunque ella murió antes de poder responder, sus ideas permanecieron en sus publicaciones y Ventris las estudió meticulosamente. Apreció completamente el poder de la tabla de Kober y trató de encontrar nuevas palabras que compartieran la raíz y la sílaba de unión. Amplió la tabla de Kober incluyendo estos nuevos signos y abarcando, por tanto, otras vocales y consonantes. Luego, después de un año de intenso estudio, se dio cuenta de algo peculiar, algo que parecía sugerir una excepción a la regla de que todos los signos del Lineal B son sílabas.

Había sido generalmente aceptado que cada signo del Lineal B representaba una combinación de una consonante con una vocal (CV), por lo que la ortografía requeriría que una palabra se descompusiera en componentes CV Por ejemplo, la palabra minuto se escribiría como mi-nu-to, una serie de tres sílabas CV Sin embargo, hay muchas palabras que no se dividen convenientemente en sílabas CV Por ejemplo, si descomponemos la palabra «visible» en pares de letras, obtenemos vi-si-bl-e, lo que resulta problemático, ya que no consta de una serie simple de sílabas CV: hay una sílaba de dos consonantes y una -e de sobra al final. Ventris supuso que los minoicos superaron este problema insertando una i muda para crear

una sílaba -bi- cosmética, de modo que la palabra se pueda escribir ahora como vi-si-bi-le, lo que sí es una combinación de sílabas CV

Sin embargo, la palabra invisible sigue siendo problemática. De nuevo, es necesario insertar vocales mudas, esta vez después de la n y de la b, convirtiéndolas así en sílabas CV Además, también es necesario hacer algo con la vocal i que queda sola al principio de la palabra: i-ni-vi-si-bi-le. La i inicial no puede ser convertida fácilmente en una sílaba *CV,* ya que insertar una consonante muda al comienzo de una palabra se prestaría a muchas confusiones.

En resumen, Ventris concluyó que debe haber signos del Lineal B que representan a vocales solas, para ser usados en palabras que comienzan con una vocal. Estos signos deberían ser fáciles de localizar, ya que sólo aparecerían al principio de las palabras. Ventris calculó la frecuencia con que cada signo aparece al principio, en el medio o al final de cualquier palabra. Observó que dos signos en particular, 08 y 61, aparecían predominantemente al principio de las palabras y concluyó que no representaban sílabas, sino vocales solas.

Ventris publicó sus ideas acerca de los signos de vocales y sus ampliaciones de la tabla en una serie de Notas de Trabajo, que envió a otros investigadores del Lineal B. El 1 de junio de 1952 publicó su resultado más significativo, la Nota de Trabajo 20, un punto decisivo en el desciframiento del Lineal B. Había pasado los dos últimos años ampliando la tabla de Kober hasta llegar a la versión que se muestra en la Tabla 22. La tabla constaba de cinco columnas de vocales y 15 líneas de consonantes, dando 75 cuadrículas en total, con 5 cuadrículas adicionales para vocales solas. Ventris había insertado signos en casi la mitad de las cuadrículas. La tabla es un tesoro de información. Por ejemplo, observando la sexta línea es posible decir que los signos silábicos 37, 05 y 69 comparten la misma consonante, VI, pero que contienen vocales diferentes, 1, 2 y 4. Ventris no tenía idea del valor exacto de la consonante VI o de las vocales 1, 2 y 4, y hasta entonces había resistido la tentación de asignar valores sonoros a ninguno de los signos. Sin embargo, sintió que había llegado el momento de seguir algunas de sus corazonadas y adivinar unos pocos valores sonoros y examinar las consecuencias.

Tabla 22

La tabla ampliada de Ventrin de la relación entre caracteres del Lineal B. Aunque la tabla no especifica vocales y consonantes, destaca qué caracteres comparte vocales y consonantes. Por ejemplo, todos los caracteres de la primera columna comparten la misma vocal, denominada I.

		Vocales				
		1	2	3	4	5
Consonantes	I					57
	II	40		75		54
	III	39				03
	IV		36			
	V		14			01
	VI	37	05		69	
	VII	41	12			31
	VIII	30	52	24	55	06
	IX	73	15			80
	X		70	44		
	XI	53				76
	XII		02	27		
	XIII					
	XIV			13		
	XV		32	78		
	Vocales puras		61			08

Ventris se había dado cuenta de que había tres palabras que aparecían con mucha frecuencia en muchas de las tablillas del Lineal B: 08-73-30-12, 7052-12 y 69-53-12. Basándose únicamente en su intuición, conjeturó que estas palabras podrían ser nombres de ciudades importantes. Ventris ya había especulado que el signo 08 era una vocal y, por tanto, el nombre de la primera ciudad tenía que comenzar con una vocal. El único nombre significativo que encajaba era Amnisos, una importante ciudad portuaria. Si tenía razón, entonces los signos segundo y tercero, 73 y 30, representarían -mi- y - ni-. Estas dos sílabas contenían la misma vocal, i, de modo que los números 73 y 30 deberían aparecer en la tabla en la columna de la misma

vocal. Sí aparecían El signo final, 12, representaría -so-. Ya tenía una traducción provisional[18]

Ciudad 1 = 08-73-30-12 = a- mi-ni-so = Amnisos

Era sólo una conjetura, pero sus repercusiones en la tabla de Ventris eran enormes. Por ejemplo, el signo 12, que parece representar -so-, está en la segunda columna de vocales y en la séptima línea de consonantes. Por consiguiente, si su conjetura era correcta, entonces todos los demás signos silábicos de la segunda columna de vocales contendrían la vocal o, y todos los demás signos silábicos de la séptima línea de consonantes contendrían la consonante s.

Cuando Ventris examinó la segunda ciudad se dio cuenta que también contenía el signo 12, -so-. Los otros dos signos, 70 y 52, estaban en la misma columna de vocales que -so-, lo que implicaba que estos signos también contenían la vocal o. Para la segunda ciudad podía insertar -so-, la o en los lugares apropiados, y dejar espacios para las consonantes que faltaban, lo que llevaba a lo siguiente:

Ciudad 2 = 70-52-12 = ?o-? o-so = ?

¿Podía tratarse de Cnosos? Los signos podrían representar ko-no-so. Ventris se mostró satisfecho al comprobar que el signo 52, que supuestamente representaba -no-, estaba en la misma línea de consonantes que el signo 30, que supuestamente representaba -ni- en Amnisos. Esto era tranquilizador, porque si contenían la misma consonante, n, deberían estar efectivamente en la misma línea de consonantes de la tabla. Utilizando la información silábica de Cnosos y Amnisos, insertó las siguientes letras en la tercera ciudad:

Ciudad 3 = 69-53-12 = ??-? i-so

[18] En inglés y castellano se escribe Amnisos, lo que dejaba a Ventris con una s final sola a la que no correspondía ningún signo. Ventris decidió ignorar el problema por el momento y ajustarse a su traducción provisional. (N. del T.)

El único nombre que parecía encajar era Tulisos (tu-li-so), una importante ciudad situada en el centro de Creta. Ahora Ventris había identificado tentativamente tres nombres de lugares y los valores sonoros de ocho signos diferentes:

Ciudad 1 = 08-73-30-12 = a- mi-ni-so = Amnisos
Ciudad 2 = 70-52-12 = ko-no-so = Cnosos
Ciudad 3 = 69-53-12 = tu-li- so = Tulisos

Las repercusiones de identificar ocho signos eran enormes. Ventris podía deducir los valores consonánticos y vocálicos de muchos de los demás signos de la tabla, si estaban en la misma línea o la misma columna. El resultado fue que muchos signos revelaron parte de su significado silábico y unos pocos pudieron ser identificados completamente. Por ejemplo, el signo 05 está en la misma línea que 12 (so), 52 (no) y 70 (ko), de modo que debe contener la vocal o.

Siguiendo el mismo tipo de razonamiento, el signo 05 está en la misma línea que el signo 69 (tu), de modo que debe contener la consonante t. En resumen, el signo 05 representa la sílaba -to-. Si observamos ahora el signo 31, vemos que está en la misma columna que el signo 08, la columna de la a, y en la misma línea que el signo 12, la línea de la s. Por tanto, el signo 31 representa la sílaba -sa-.

Deducir el valor silábico de estos dos signos, 05 y 31, fue particularmente importante, ya que permitió a Ventris leer dos palabras completas, 05-12 y 05-31, que a menudo aparecían en la parte inferior de los inventarios. Ventris ya sabía que el signo 12 representaba la sílaba -so-, porque este signo aparecía en la palabra Tulisos, por lo que 05-12 se podía leer como to-so. Y la otra palabra, 05-31, se podía leer como tosa. Éste era un resultado sorprendente.

Como estas palabras se encontraban en la parte inferior de los inventarios, los expertos habían sospechado que significaban «total». Ventris las leyó ahora como toso y tosa, misteriosamente similar a las palabras *tossos* y *tossa*, que eran las formas masculina y femenina del griego antiguo que significaban «tanto». Desde que tenía catorce años, cuando escuchó la conferencia de sir Arthur Evans, Ventris había creído que la lengua de los minoicos no podía ser el griego. Ahora estaba

descubriendo palabras que constituían una clara prueba a favor del griego como la lengua del Lineal B.

Fue la antigua escritura chipriota la que ofreció la primera señal contra la idea de que el Lineal B fuera el griego, porque sugería que las palabras del Lineal B raramente terminaban en s, mientras que ésa es una terminación muy corriente para las palabras griegas. Ventris había descubierto que, efectivamente, las palabras del Lineal B raramente terminan en s, pero quizá esto era así simplemente porque se omitía la s como parte de alguna convención de escritura. Amnisos, Cnosos, Tulisos y *tossos* se escribían sin s final en el Lineal B, indicando que los escribas simplemente no se molestaban en poner la s final, permitiendo que el lector rellenase la obvia omisión Ventris no tardó en descifrar varias otras palabras, que también se parecían al griego, pero todavía no estaba absolutamente convencido de que el Lineal B fuera una escritura del griego. En teoría, se podía considerar que las pocas palabras que había descifrado fueran palabras que se habían importado a la lengua minoica. Un extranjero que llegue a un hotel inglés podría oír palabras como *«rendezvous»* o *«bon appetit»,* pero se equivocaría al asumir que los ingleses hablan en francés.

Además, Ventris encontró palabras a las que no encontraba sentido, lo que ofrecía alguna prueba a favor de una lengua hasta entonces desconocida. En la Nota de Trabajo 20 no ignoró la tesis griega, pero la denominó «una digresión frívola». Concluyó: «Si las seguimos, sospecho que estas líneas de desciframiento conducirán tarde o temprano a un punto muerto, o se disiparán en el absurdo».

A pesar de sus recelos, Ventris siguió la línea de ataque griega. Mientras aún se estaba distribuyendo la Nota de Trabajo 20 empezó a descubrir más palabras griegas. Pudo identificar *poimen* (pastor), *kerameus* (alfarero), *khrusoworgos* (orfebre) y *khalkeus* (broncista), e incluso tradujo un par de frases enteras. Hasta ahora, ninguna de los absurdos advertidos había bloqueado su camino. Por primera vez en tres mil años, la escritura silenciosa del Lineal B estaba susurrando de nuevo y la lengua que hablaba era indudablemente el griego.

Casualmente, durante este período de progreso rápido Ventris había solicitado aparecer en la emisora BBC para hablar del misterio de los escritos minoicos. Decidió que ésta sería una oportunidad ideal para hacer público su descubrimiento.

Después de una charla bastante prosaica sobre la historia minoica y el Lineal B, hizo su revolucionario anuncio: «*En las últimas se manas he llegado a la conclusión de que, después de todo, las tablillas de Cnosos y Pilos deben estar escritas en griego, un griego difícil y arcaico considerando que es quinientos años más antiguo que Homero y está escrito en una forma bastante abreviada, pero, no obstante, griego*». Entre sus oyentes se encontraba John Chadwick, un investigador de Cambridge que había estado interesado en el desciframiento del Lineal B desde los años treinta. Durante la guerra, había pasado tiempo como criptoanalista en Alejandría, descifrando cifras italianas, antes de trasladarse a Bletchley Park, donde atacó las cifras japonesas. Después de la guerra intentó de nuevo descifrar el Lineal B, esta vez empleando las técnicas que había aprendido mientras trabajaba con códigos militares. Por desgracia, tuvo muy poco éxito.

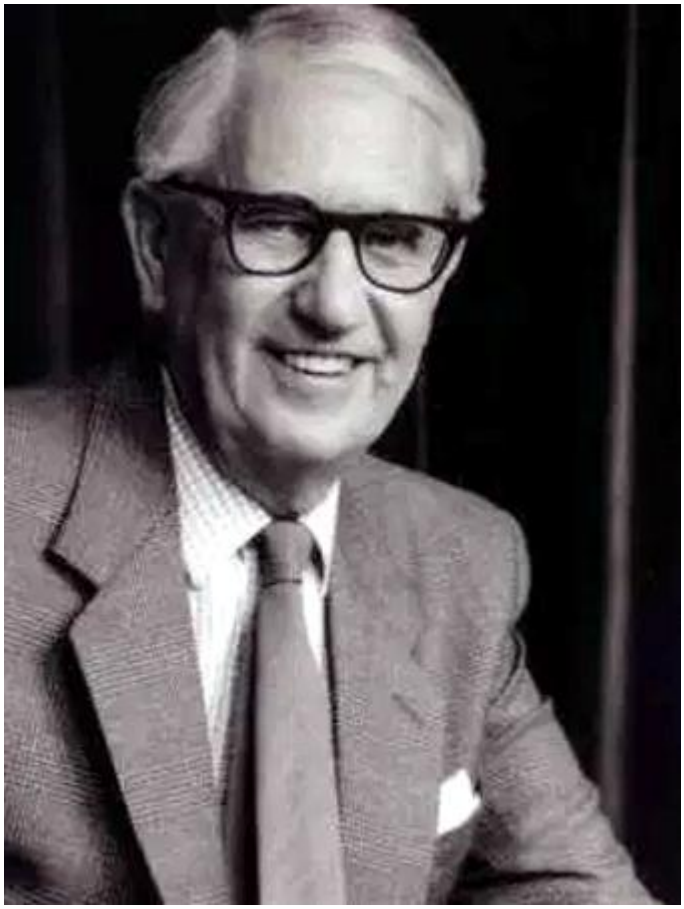


Figura 61. John Chadwick.

Cuando oyó la entrevista por la radio quedó absolutamente sorprendido por la aparentemente descabellada afirmación de Ventris. Chadwick, como la mayoría de los estudiosos que oyeron la emisión, consideraron la afirmación como el trabajo de un aficionado, en realidad lo era. Sin embargo, como profesor de griego, Chadwick se dio cuenta de que le asaetearían a preguntas con relación a la afirmación de Ventris, y para prepararse para la descarga decidió investigar en detalle este argumento. Obtuvo copias de las Notas de Trabajo de Ventris y las examinó, esperando que iban a estar llenas de lagunas. Sin embargo, en cuestión de días el escéptico erudito se convirtió en uno de los primeros seguidores de la teoría griega de Ventris sobre el Lineal B. Chadwick no tardó en admirar al joven arquitecto:

> *Su cerebro funcionaba con sorprendente velocidad, de modo que podía pensar todas las implicaciones de una sugerencia antes de que acabases de formularla. Tenía una aguda apreciación de las realidades de la situación; los micénicos no eran para él abstracciones vagas, sino personas vivas en cuyos pensamientos podía adentrarse. El mismo hacía hincapié en el enfoque visual del problema; se familiarizó tanto con el aspecto visual de los textos que tenía extensos fragmentos impresos en su mente simplemente como patrones visuales, mucho antes de que el desciframiento les diera significado. Pero una memoria meramente fotográfica no era suficiente, y era ahí donde su formación arquitectónica le servía de ayuda. El ojo de un arquitecto siempre ve en un edificio no sólo una mera fachada, una mezcolanza de rasgos ornamentales y estructurales: ve más allá de la apariencia y distingue las partes significativas del patrón, los elementos estructurales y el armazón del edificio. Así también Ventris era capaz de discernir, entre la desconcertante variedad de los misteriosos signos, patrones y regularidades que delataban la estructura subyacente. Es esta cualidad, el poder de ver orden en la aparente confusión, la que ha caracterizado el trabajo de todos los grandes hombres.*

Sin embargo, Ventris carecía de una pericia particular, a saber, un conocimiento profundo del griego arcaico. Los únicos estudios formales de griego que había cursado Ventris eran los de la Stowe School, cuando era niño, de modo que no podía sacarle todo el partido a su gran avance con el Lineal B. Por ejemplo, no era capaz de explicar algunas de las palabras descifradas porque no formaban parte de su vocabulario de griego. La especialidad de Chadwick era la filología griega, el estudio de la evolución histórica de la lengua griega, y, por tanto, estaba equipado para mostrar que estas palabras problemáticas encajaban con teorías de las formas más antiguas del griego. Juntos, Chadwick y Ventris formaban una asociación perfecta.

El griego de Homero tiene tres mil años de antigüedad, pero el griego del Lineal B es aún quinientos años más antiguo. Para traducirlo, Chadwick necesitaba extrapolar del griego antiguo establecido a las palabras del Lineal B, teniendo en cuenta las tres maneras en que se desarrolla una lengua. Primero, la pronunciación evoluciona con el tiempo. Por ejemplo, la palabra griega para «vertedores de baño» cambia de *lewotrokhowoi* en el Lineal B a *loutrokhooi* para la época de Homero. Segundo, se producen cambios en la gramática. Por ejemplo, en el Lineal B la terminación del genitivo es -oio, pero ésta es reemplazada en el griego clásico por -ou Finalmente, el léxico puede cambiar enormemente. Algunas palabras nacen, otras mueren, otras cambian de significado. En el Lineal B, *harmo* significa «rueda», pero en el griego posterior la misma palabra significa «carro». Chadwick señaló que esto es similar al uso de *wheels* (ruedas) para decir *car* (coche) en inglés moderno.

Con la habilidad descifradora de Ventris y la pericia en griego de Chadwick, el dúo llegó a convencer al resto del mundo de que el Lineal B es efectivamente el griego. El ritmo de traducción se aceleraba cada día. En el relato de Chadwick sobre su trabajo, titulado *The Decipherment of Linear B,* escribe:

> *La criptografía es una ciencia de deducción y experimento controlado; se forman hipótesis, se ponen a prueba y a menudo se descartan. Pero el residuo que pasa la prueba crece hasta que finalmente llega un punto en que quien realízalos experimentos siente un suelo sólido bajo sus pies: sus hipótesis adquieren coherencia, y surgen fragmentos de sentido de detrás de su*

camuflaje. El código «se rompe». Quizá esto se defina mejor como el punto en que las pistas probables aparecen más rápidamente de lo que pueden ser seguidas. Es como la iniciación de una reacción en cadena en física atómica; una vez se traspasa el umbral crítico, la reacción se propaga por sí misma.

Los dos hombres no tardaron mucho en poder demostrar su dominio de la escritura intercambiándose notas breves en el Lineal B.

Una prueba informal de la exactitud de un desciframiento es el número de dioses que aparecen en el texto. En el pasado, los que iban por mal camino generaban, obviamente, muchas palabras sin sentido, que excusaban diciendo que se trataba de los nombres de deidades desconocidas hasta entonces. Sin embargo, Chadwick y Ventris sólo reivindicaron cuatro nombres divinos, y todos ellos eran dioses bien establecidos.

En 1953, seguros de su análisis, redactaron las conclusiones de su trabajo en un artículo, titulado modestamente «Prueba a favor del dialecto griego en los archivos micénicos», que fue publicado en *The Journal of Hellenic Studies.* A partir de entonces, arqueólogos de todo el mundo comenzaron a darse cuenta de que estaban presenciando una revolución En una carta dirigida a Ventris, el erudito alemán Ernst Sittig resumió el estado de ánimo de la comunidad académica: «Lo repito: desde el punto de vista criptográfico, sus demostraciones son las más interesantes que he oído, además de ser realmente fascinantes. Si tiene razón, los métodos de la arqueología, la etnología, la historia y la filología de los últimos cincuenta años quedan reducidos *ad absurdum».*

Las tablillas del Lineal B contradecían casi todo lo que habían afirmado sir Arthur Evans y su generación. Para empezar, estaba el simple hecho de que el Lineal B era una escritura del griego. Segundo, si los minoicos de Creta escribían el griego y probablemente hablaban en griego, esto obligaría a los arqueólogos a reconsiderar sus opiniones sobre la historia minoica. Ahora parecía que la fuerza dominante en la región era Micenas, y que la Creta minoica era un estado menor cuya gente hablaba la lengua de sus poderosos vecinos. Sin embargo, hay evidencia de que, antes de 1450 a. C., Minos fue un estado verdaderamente independiente con una lengua

propia. Fue alrededor de 1450 a. C. cuando el Lineal B reemplazó al Lineal A, y aunque las dos escrituras parecen muy similares, hasta ahora nadie ha descifrado el Lineal A. Por tanto, el Lineal A representa probablemente una lengua marcadamente diferente a la del Lineal B. Parece probable que hacia 1450 a. C. los micénicos conquistaron a los minoicos, les impusieron su lengua, y transformaron el Lineal A en Lineal B para que funcionara como una escritura del griego.

Además de aclarar el amplio panorama histórico, el desciframiento del Lineal B ofrece también detalles. Por ejemplo, las excavaciones en Pilos no han logrado descubrir ningún objeto precioso en el lujoso palacio, que fue destruido por un incendio. Esto ha llevado a la sospecha de que el palacio fue incendiado deliberadamente por los invasores, que primero lo despojaron de los objetos de valor.

Aunque las tablillas del Lineal B aparecidas en Pilos no describen específicamente un ataque semejante, insinúan que se estaban preparando para una invasión. Una tablilla describe el establecimiento de una unidad militar especial para proteger la costa, mientras que otra describe cómo se estaban requisando los ornamentos de bronce para convertirlos en puntas de lanza.

Una tercera tablilla, menos ordenada que las otras dos, describe un ritual particularmente elaborado realizado en el templo, que posiblemente incluía sacrificios humanos. La mayoría de las tablillas del Lineal B están cuidadosamente dispuestas, dando a entender que los escribas comenzaban con un borrador que luego se destruía. La tablilla desordenada tiene largos espacios en blanco y texto que se sale por el otro lado. Una explicación posible es que la tablilla registraba una tentativa de invocar la intervención divina ante una invasión, pero antes de que la tablilla pudiera ser escrita de nuevo el palacio fue invadido.

La mayoría de las tablillas de Lineal B son inventarios, y como tales describen transacciones cotidianas. Indican la existencia de una burocracia que podía rivalizar con cualquier otra de la Historia, con tablillas que registran detalles de bienes manufacturados y productos agrícolas. Chadwick comparó el archivo de tablillas al *Domesday Book*[19], y el profesor Denys Page describió de esta forma el nivel de detalle: «Las ovejas se cuentan hasta ascender a un esplendoroso total de

[19] El Domesday Book es una amplia relación de la extensión, el valor, la propiedad y las responsabilidades de las tierras de Inglaterra, realizada en 1086 por orden de Guillermo el Conquistador. (N. del T.)

veinticinco mil; pero aún se considera necesario registrar el hecho de que un animal fue donado por Komawens... Se podría suponer que no se podía sembrar una semilla, ni trabajar un gramo de bronce, ni tejer una tela, ni criar una cabra o engordar un cerdo, sin rellenar un impreso en el Palacio Real». Estos archivos de palacio podrían parecer anodinos, pero son inherentemente románticos porque están tan íntimamente ligados con la *Odisea* y la *Ilíada.*

Mientras los escribas de Cnosos y Pilos apuntaban sus transacciones diarias, se estaba luchando la guerra de Troya. La lengua del Lineal B es la lengua de Ulises.

El 24 de junio de 1953, Ventris dio una conferencia pública esbozando el desciframiento del Lineal B. Al día siguiente apareció en *The Times*, junto a un comentario sobre la reciente conquista del Everest.

Tabla 23

Los signos del Lineal B con su número y su valor sonoro

Esto condujo a que el logro de Ventris y Chadwick se conoció como «el Everest de la arqueología griega». Al año siguiente, los dos hombres decidieron escribir un informe en tres volúmenes de su trabajo, que incluiría una descripción del desciframiento, un análisis detallado de trescientas tablillas, un diccionario de 630 palabras micénicas y una lista de los valores sonoros de casi todos los signos del Lineal B, como la ofrecida en la Tabla 23. La obra, titulada *Documents in Mycenaean Greek*, fue finalizada en el verano de 1955 y estaba lista para ser publicada en el

otoño de 1956. Sin embargo, unas pocas semanas antes de la impresión, el 6 de septiembre de 1956, Michael Ventris murió. Mientras volvía a casa por la noche conduciendo por la carretera nacional del norte, cerca de Hatfield, su coche chocó con un camión. John Chadwick rindió homenaje a su colega, un hombre que igualaba el genio de Champollion y que también había muerto a una edad trágicamente temprana: «*El trabajo que realizó sigue vivo y su nombre será recordado mientras se estudie la lengua y la civilización de la Grecia antigua*».

Capítulo 6

Alicia y Benito hacen pública su clave

Contenido:

1. *Dios premia a los tontos*
2. *El nacimiento de la criptografía de clave pública*
3. *Principales sospechosos*
4. *La historia alternativa de la criptografía de clave pública*

Durante la segunda guerra mundial, los descifradores británicos se impusieron a los codificadores alemanes principalmente porque los hombres y mujeres de Bletchley Park, siguiendo los pasos de los polacos, desarrollaron parte de la primera tecnología del desciframiento. Además de las *bombas* de Turing, que se utilizaron para romper la cifra de la Enigma, los británicos inventaron también otro artefacto de descodificación, el Colossus, para combatir una forma aún más potente de codificación, a saber, la cifra Lorenz alemana. De los dos tipos de máquinas descifradoras, fue el Colossus el que determinaría el desarrollo de la criptografía durante la segunda mitad del siglo XX.

La cifra Lorenz se utilizaba para codificar las comunicaciones entre Hitler y sus generales. La codificación la llevaba a cabo la máquina Lorenz SZ40, que funcionaba de manera similar a la máquina Enigma, pero la Lorenz era mucho más complicada, y presentó a los descifradores de Bletchley un desafío aún mayor. Sin embargo, dos de los descifradores de Bletchley, John Tiltman y Bill Tutte, descubrieron un punto débil en la manera en que se usaba la cifra Lorenz, un fallo al que Bletchley pudo sacar partido y, por consiguiente, leer los mensajes de Hitler.

Descifrar la cifra Lorenz requirió una mezcla de búsquedas, combinaciones, análisis estadísticos y decisiones cuidadosas, todo lo cual estaba más allá de las habilidades técnicas de las *bombas.* Las *bombas* podían llevar a cabo una tarea específica a gran velocidad, pero no eran lo suficientemente flexibles para enfrentarse a las sutilezas de la Lorenz. Los mensajes codificados con la Lorenz tenían que ser descifrados a mano, lo que costaba semanas de esfuerzo minucioso, y para entonces los mensajes eran ya en gran medida demasiado viejos. Finalmente, a

Max Newman, un matemático de Bletchley, se le ocurrió una manera de mecanizar el criptoanálisis de la cifra Lorenz. Inspirándose enormemente en el concepto de la máquina universal de Alan Turing, Newman diseñó una máquina capaz de adaptarse a diferentes problemas, lo que hoy llamaríamos un ordenador programable.

Se consideró que poner en práctica el diseño de Newman era técnicamente imposible, de modo que los altos oficiales de Bletchley dieron carpetazo al proyecto. Afortunadamente, Tommy Flowers, un ingeniero que había tomado parte en las discusiones sobre el diseño de Newman, decidió ignorar el escepticismo de Bletchley y procedió a construir la máquina. En el centro de investigación de la Oficina de Correos de Dollis Hill, en el norte de Londres, Flowers tomó el proyecto original de Newman y pasó diez meses convirtiéndolo en la máquina Colossus, que entregó en Bletchley Park el 8 de diciembre de 1943. Constaba de 1.500 válvulas electrónicas, que eran considerablemente más rápidas que los lentos conmutadores electromagnéticos de transmisión utilizados en las *bombas.* Pero aún más importante que la velocidad del Colossus era el hecho de que era programable. Fue esto lo que convirtió al Colossus en el precursor del ordenador digital moderno.

El Colossus, como todo lo que había en Bletchley Park, fue destruido después de la guerra, y a los que trabajaron en él se les prohibió que hablaran de ello. Cuando se ordenó a Tommy Flowers que se deshiciera del proyecto original del Colossus, obedientemente, lo llevó a la caldera y lo quemó. Los planes del primer ordenador del mundo se perdieron para siempre. Este secreto significó que otros científicos obtuvieron el crédito por la invención del ordenador. En 1945, J. Presper Eckert y John W. Mauchly, de la Universidad de Pensilvania, terminaron el ENIAC (Electronic Numerical Integrator And Calculator, Integrador y calculador numérico electrónico), que constaba de 18.000 válvulas electrónicas y era capaz de realizar 5.000 cálculos por segundo. Durante décadas, el ENIAC, y no el Colossus, fue considerado como la madre de todos los ordenadores.

Habiendo contribuido al nacimiento del ordenador moderno, después de la guerra los criptoanalistas continuaron desarrollando y usando la tecnología de los ordenadores para descifrar todo tipo de cifras. Ahora podían sacar partido a la velocidad y la flexibilidad de los ordenadores programables para probar todas las claves posibles hasta encontrar la correcta. A su debido tiempo, los criptógrafos

comenzaron a contraatacar, sacando partido al poder de los ordenadores para crear cifras cada vez más complejas. En resumen, el ordenador desempeñó un papel crucial en la posguerra en la batalla entre los codificadores y los descifradores.

Utilizar un ordenador para codificar un mensaje es, en gran medida, muy similar a las formas tradicionales de codificación. En realidad, sólo hay tres diferencias significativas entre la codificación por ordenador y el tipo de codificación mecánica que constituía la base de cifras como la Enigma. La primera diferencia es que una máquina de cifras mecánica tiene la limitación de lo que se puede construir prácticamente, mientras que un ordenador puede imitar una hipotética máquina de cifras de complejidad inmensa. Por ejemplo, se podría programar un ordenador para imitar la acción de cien modificadores, algunos girando en el sentido de las agujas de un reloj, otros en sentido contrario, otros desapareciendo después de cada diez letras, otros girando cada vez más rápido según avanza la codificación. Una máquina mecánica semejante sería imposible de construir en la práctica, pero su equivalente computarizada «virtual» proporcionaría una cifra de alta seguridad.

La segunda diferencia es simplemente una cuestión de velocidad. La electrónica puede funcionar muchísimo más rápidamente que los modificadores mecánicos: un ordenador programado para imitar la cifra Enigma podría codificar un mensaje extenso en un instante. De manera alternativa, un ordenador programado para llevar a cabo una forma de codificación muchísimo más compleja podría aún realizar la tarea en un tiempo razonable.

La tercera diferencia, y quizá la más importante, es que un ordenador modifica números en vez de las letras del alfabeto. Los ordenadores sólo operan con números binarios: secuencias de unos y ceros conocidos como *dígitos binarios,* o *bits,* para abreviar. Por tanto, antes de la codificación, hay que convertir cualquier mensaje en dígitos binarios. Esta conversión se puede realizar según varios protocolos, como el American Standard Code for Information Interchange (Código americano estándar para el intercambio de información), conocido familiarmente por el acrónimo ASCII, pronunciado «as-qui»[20]. ASCII asigna un número binario de 7 dígitos a cada letra del alfabeto. Por ahora, es suficiente considerar un número binario simplemente como un patrón de unos y ceros que identifica únicamente a

[20] En inglés, esta pronunciación suena igual que «ass key», lo que se presta a numerosos significados humorísticos: «clave del burro», «llave del culo», etc. (N. del T.)

cada letra (Tabla 24), igual que el código Morse identifica cada letra con una serie única de puntos y rayas. Hay 128 (2^7) maneras de ordenar una combinación de 7 dígitos binarios, de modo que ASCII puede identificar hasta 128 caracteres diferentes. Esto ofrece aún mucho espacio para definir también todas las letras minúsculas (p. e., a =1100001), toda la puntuación necesaria (p. e., ! = 0100001), además de otros símbolos (p. e., &= 0100110). Una vez que el mensaje se ha convertido en binario, puede comenzar la codificación.

Aunque estamos tratando con ordenadores y números, y no con máquinas y letras, la codificación todavía se lleva a cabo mediante los principios milenarios de sustitución y trasposición, en los que unos elementos del mensaje son sustituidos por otros elementos, o se cambian sus posiciones, o ambas cosas. Toda codificación, no inporta lo compleja que sea, se puede descomponer en combinaciones de estas simples operaciones. Los dos ejemplos siguientes demuestran la simplicidad esencial de la codificación por ordenador mostrando cómo un ordenador podría realizar una sencilla cifra de sustitución y una sencilla cifra de trasposición.

Primero, imagine que deseamos codificar el mensaje HELLO («HOLA»), utilizando una simple versión informatizada de una cifra de trasposición. Antes de poder comenzar la codificación, debemos traducir el mensaje a ASCII según la Tabla 24:

Tabla 24

Números binarios ASCII para las letras mayúsculas

A	1000001	N	1001110
B	1000010	O	1001111
C	1000011	P	1010000
D	1000100	Q	1010001
E	1000101	R	1010010
F	1000110	S	1010011
G	1000111	T	1010100
H	1001000	u	1010101
I	1001001	V	1010110
J	1001010	w	1010111

K	1001011	X	1011000
L	1001100	Y	1011001
M	1001101	Z	1011010

Texto llano = HELLO = 1001000 1000101 1001100 1001100 1001111

Una de las formas más sencillas de cifra de trasposición sería intercambiar los dígitos primero y segundo, los dígitos tercero y cuarto, y así sucesivamente. En este caso, el dígito final permanecería sin cambiar porque hay un número impar de dígitos. Para ver la operación más claramente he quitado los espacios que separan los bloques ASCII en el texto llano original para generar una única serie y luego la he situado junto al texto cifrado resultante para poder comparar:

Texto llano = 1001000100010110011001001100100

Texto cifrado = 0110001000101001100110001100011 01

Un aspecto interesante de la trasposición a nivel de los dígitos binarios es que la trasposición puede suceder dentro de la letra. Además, algunos bits de una letra pueden cambiar de lugar con bits de la letra vecina. Por ejemplo, intercambiando los números séptimo y octavo, el 0 final de la H se cambia con el 1 inicial de la E. El mensaje codificado es una serie única de 35 dígitos binarios, que se puede transmitir al receptor, que entonces invierte la trasposición para recrear la serie original de dígitos binarios. Finalmente, el receptor reinterpreta los dígitos binarios con ASCII para regenerar el mensaje HELLO.

A continuación, imagine que deseamos codificar el mismo mensaje, HELLO, esta vez empleando una simple versión computarizada de la cifra de sustitución. De nuevo, comenzamos convirtiendo el mensaje en ASCII antes de la codificación. Como de costumbre, la sustitución se basa en una clave que ha sido acordada entre el emisor y el receptor. En este caso, la clave es la palabra DAVID traducida a ASCII, y se usa de la siguiente manera. Cada elemento del texto llano se «añade» al elemento correspondiente de la clave. Añadir dígitos binarios puede entenderse en función de dos reglas simples. Si los elementos del texto llano y de la clave son los mismos, el elemento del texto llano se sustituye por 0 en el texto cifrado. Pero si los elementos

del mensaje y de la clave son diferentes, el elemento del texto llano se sustituye por 1 en el texto cifrado:

Mensaje HELLO

Mensaje en ASCII: 1001000100010110011001001100100

Clave = DAVID

10001001000001101011010010011

Texto cifrado: 00011000000100001101000001

El mensaje codificado resultante es una única serie de 35 dígitos binarios que se pueden retransmitir al receptor, que usa la misma clave para invertir la sustitución, recreando así la serie original de dígitos binarios. Finalmente, el receptor reinterpreta los dígitos binarios con ASCII para regenerar el mensaje HELLO.

La codificación por ordenador estaba restringida a los que tenían ordenadores, lo que al principio significaba al gobierno y al ejército. Sin embargo, una serie de avances científicos, técnicos y de ingeniería hicieron que los ordenadores, y la codificación por ordenador, fueran muchísimo más asequibles para el público en general. En 1947, los laboratorios de la compañía AT&T Bell inventaron el transistor, una alternativa barata a la válvula electrónica. La computación comercial comenzó a hacerse realidad en 1951, cuando compañías como Ferranti comenzaron a hacer ordenadores por encargo. En 1953, IBM lanzó su primer ordenador, y cuatro años después introdujo Fortran, un lenguaje de programación que permitía que la gente «corriente» escribiera programas de ordenador. Después, en 1959, la invención del circuito integrado anunció una nueva era informática.

Durante los años sesenta, los ordenadores se volvieron más potentes, y al mismo tiempo más baratos. Cada vez había más empresas que podían permitirse tener ordenadores y los podían usar para codificar comunicaciones importantes como transferencias de dinero o delicadas negociaciones comerciales. Sin embargo, según más y más empresas iban comprando ordenadores, y se extendía la codificación entre empresas, los criptógrafos tuvieron que afrontar nuevos problemas, dificultades que no habían existido cuando la criptografía era del dominio de los gobiernos y del ejército. Una de las preocupaciones primarias era el tema de la estandarización. Una compañía podía usar un sistema de codificación en particular

para garantizar la seguridad de las comunicaciones internas, pero no podía enviar un mensaje secreto a una organización externa a no ser que el receptor usara el mismo sistema de codificación. Finalmente, el 15 de mayo de 1973, la Oficina Nacional de Estándares norteamericana planeó resolver el problema y solicitó formalmente propuestas para un sistema de codificación estándar que permitiera que las empresas se comunicaran secretamente entre sí.

Uno de los algoritmos de cifra más establecido, y uno de los candidatos para el estándar, fue un producto de IBM conocido como Lucifer. Lo había desarrollado Horst Feistel, un emigrante alemán que había llegado a Estados Unidos en 1934. Estaba a punto de convertirse en ciudadano norteamericano cuando Estados Unidos entró en la guerra, lo que significó que fue puesto bajo arresto domiciliario hasta 1944. Después de eso, durante algunos años reprimió su interés en la criptografía para evitar despertar las sospechas de las autoridades estadounidenses. Cuando finalmente comenzó a investigar las cifras, en el Centro de Investigación de las Fuerzas Aéreas de Cambridge, no tardó en verse en dificultades con la NSA, la organización responsable de mantener la seguridad de las comunicaciones militares y gubernamentales, y que trata también de interceptar y descifrar las comunicaciones extranjeras. La NSA emplea a más matemáticos, compra más *hardware* de ordenadores e intercepta más mensajes que ninguna otra organización en el mundo. Es el líder mundial en lo referente a fisgonear.

La NSA no ponía reparos al pasado de Feistel; simplemente, quería tener el monopolio de la investigación criptográfica, y parece ser que dispusieron que se cancelase el proyecto de investigación de Feistel. En los años sesenta, Feistel se fue a la Mitre Corporation, pero la NSA continuó presionando y lo obligó a abandonar su trabajo por segunda vez. Feistel fue a parar finalmente al Laboratorio Thomas J. Watson de la IBM, cerca de Nueva York, donde durante varios años pudo realizar su investigación sin ser acosado. Fue entonces, al principio de los años setenta, cuando desarrolló el sistema Lucifer.

Lucifer codifica los mensajes según la siguiente operación de modificación. Primero, se traduce el mensaje a una larga serie de dígitos binarios. Segundo, la serie se divide en bloques de 64 dígitos, y se realiza la codificación separadamente para cada uno de los bloques. Tercero, centrándose en uno solo de los bloques, los 64

dígitos se revuelven y luego se dividen en dos semibloques de 32, denominados Izquierda^0 y Derecha^0. Los dígitos de Derecha^0 se someten entonces a una «función de deformación», que cambia los dígitos según una compleja sustitución La Derecha^0 «deformada» se añade entonces a la Izquierda^0 para crear un nuevo semibloque de 32 dígitos denominado Derecha^1. La Derecha^0 original se denomina ahora Izquierda^1. Esta serie de operaciones se llama una «ronda». Se repite el proceso entero en una segunda ronda, pero comenzando con los nuevos semibloques, Izquierda^1 y Derecha^1, y acabando con Izquierda^2 y Derecha^2. Este proceso se repite hasta que haya habido 16 rondas en total. El proceso de codificación se parece un poco a amasar un trozo de masa de hacer pan. Imagine un trozo largo de masa con un mensaje escrito en ella. Primero, el trozo largo se divide en bloques de 64 cm de longitud. Luego, se coge la mitad de uno de los bloques y se aplana, se dobla, se añade a la otra mitad y se extiende para hacer un nuevo bloque. Seguidamente se repite el proceso una y otra vez hasta que el mensaje se haya entremezclado completamente. Tras 16 rondas de amasado, se envía el texto cifrado, que entonces es descifrado al otro lado invirtiendo el proceso.

Los detalles exactos de la operación de deformación pueden variar, y los determina una clave acordada entre el emisor y el receptor. En otras palabras, el mismo mensaje se puede codificar de una miríada de maneras dependiendo de la clave que se elija.

Las claves utilizadas en la criptografía por ordenador son simplemente números. Por eso, el emisor y el receptor tienen meramente que acordar un número para decidir la clave. Después de eso, la codificación requiere que el emisor introduzca el número de la clave y el mensaje en Lucifer, que se ocupará de producir el texto cifrado. La descodificación requiere que el receptor introduzca el mismo número de la clave y el texto cifrado en Lucifer, que se ocupará de producir el mensaje original.

Se consideraba generalmente que Lucifer era uno de los más potentes productos de codificación disponibles comercialmente, y, por consiguiente, era usado por diferentes tipos de organizaciones.

Parecía inevitable que este sistema de codificación fuera adoptado como el estándar americano, pero una vez más la NSA interfirió con el trabajo de Feistel. Lucifer era tan potente que ofrecía la posibilidad de una codificación estándar que

probablemente estaba más allá de la capacidad de desciframiento de la NSA; evidentemente, la NSA no quería ver una codificación estándar que ella no pudiera descifrar. Por eso, se rumorea que la NSA presionó para que se debilitara un aspecto de Lucifer, el número de claves posibles, antes de permitir que se adoptase como estándar.

El número de claves posibles es uno de los factores cruciales que determinan la solidez de cualquier cifra. Un criptoanalista que intenta descifrar un mensaje codificado podría tratar de probar todas las claves posibles, y cuanto mayor sea el número de claves posibles, más tiempo le costará encontrar la correcta. Si sólo hay 1.000.000 de claves posibles, un criptoanalista podría usar un ordenador potente para encontrar la correcta en cuestión de minutos, y con ello descifrar un mensaje interceptado. Sin embargo, si el número de claves posibles es lo suficientemente grande, encontrar la clave correcta deja de ser práctico. Si Lucifer iba a convertirse en la codificación estándar, la NSA quería asegurarse de que sólo funcionaría con un número restringido de claves.

La NSA alegó a favor de limitar el número de claves a unas 100.000.000.000.000.000 (que se describe técnicamente como 56 bits, ya que este número consta de 56 dígitos cuando se escribe en binario). Parece que la NSA creía que semejante clave ofrecería seguridad dentro de la comunidad civil, porque ninguna organización civil tiene un ordenador lo suficientemente poderoso para probar todas esas claves posibles en un período de tiempo razonable. Sin embargo, la propia NSA, que tiene acceso a los mayores recursos informáticos del mundo, sí podría entrar en los mensajes. La versión de 56 bits de la cifra Lucifer de Feistel fue adoptada oficialmente el 23 de noviembre de 1976, y fue denominada DES (Data Encryption Standard, Estándar de cifrado de datos). Un cuarto de siglo después, DES sigue siendo el estándar oficial norteamericano para la codificación.

La adopción de DES resolvió el problema de la estandarización, alentando a las empresas a usar la criptografía para su seguridad. Además, DES era lo suficientemente potente para garantizar la seguridad frente a los ataques de rivales comerciales. De hecho, era imposible que una compañía con un ordenador civil entrara en un mensaje codificado con DES, porque el número de claves posibles era demasiado grande. Por desgracia, a pesar de la estandarización y a pesar de la

potencia de DES, las empresas aún tenían que afrontar otro gran tema, el problema de la *distribución de claves.*

Imagine que un banco quiere enviar algunos datos confidenciales a un cliente a través de la línea telefónica, pero le preocupa que pueda haber alguien que intervenga la línea. El banco elige una clave y utiliza DES para codificar los datos del mensaje. Para descodificar el mensaje, el cliente no sólo necesita tener una copia de DES en su ordenador, sino también saber qué clave ha sido usada para cifrar el mensaje. ¿Cómo informa el banco al cliente acerca de la clave? No puede enviar la clave a través de la línea telefónica, porque sospecha que hay un fisgón en la línea. La única forma verdaderamente segura de enviar la clave es entregarla en persona, lo que obviamente es una tarea que requiere mucho tiempo. Una solución menos segura pero más práctica es enviar la clave mediante un mensajero. En los años setenta, los bancos trataron de distribuir las claves empleando mensajeros especiales cuyos antecedentes habían sido investigados y que estaban entre los empleados en los que la compañía tenía más confianza. Estos mensajeros recorrían todo el mundo con maletines cerrados con candado, distribuyendo claves personalmente a todos los que iban a recibir mensajes del banco la semana siguiente. Según fue creciendo el tamaño de las redes de negocios y se enviaban más mensajes, y había que entregar más claves, los bancos vieron que este proceso de distribución se convertía en una horrible pesadilla logística y los gastos generales se volvieron prohibitivos.

El problema de la distribución de claves ha acosado a los criptógrafos a lo largo de la historia. Por ejemplo, durante la segunda guerra mundial, el Alto Mando alemán tenía que distribuir el libro mensual de claves del día a todos sus operadores de la Enigma, lo que suponía un enorme problema logístico. Asimismo, los submarinos, que tendían a pasar extensos períodos lejos de la base, tenían que obtener de alguna manera un suministro regular de claves. Anteriormente, los usuarios de la cifra Vigenére tenían que encontrar una forma de hacer que la palabra que constituía la clave llegara del emisor al receptor. No importa lo segura que sea una cifra en teoría, en la práctica puede ser socavada por el problema de la distribución de claves.

En cierta medida, el gobierno y el ejército han logrado afrontar el problema de la

distribución de claves invirtiendo dinero y medios para solucionarlo. Sus mensajes son tan importantes que harán cualquier cosa para garantizar la distribución segura de la clave. Las claves del gobierno de Estados Unidos y su distribución corren a cargo de COMSEC, abreviatura de Communications Security (Seguridad de las comunicaciones). En los años setenta, COMSEC era el responsable de transportar toneladas métricas de claves cada día. Cuando los barcos que llevaban material del COMSEC llegaban a puerto, los criptoguardianes entraban a bordo, recogían montones de tarjetas, cintas de papel, disquetes o cualquier otro soporte en que se hubieran almacenado las claves y luego las distribuían a los receptores deseados.

La distribución de claves podría parecer un tema anodino, pero se convirtió en el problema primordial para los criptógrafos de la posguerra. Si dos partes querían comunicarse de manera segura tenían que recurrir a una tercera parte para distribuir la clave, y éste se convirtió en el eslabón más débil de la cadena de la seguridad. El dilema para las empresas era evidente —si los gobiernos, con todo el dinero que tenían disponible, habían de luchar para garantizar la distribución segura de las claves, ¿cómo iban las compañías civiles a esperar conseguir alguna vez una distribución fiable de las claves sin arruinarse?

A pesar de las afirmaciones de que el problema de la distribución de claves no tenía solución, un equipo de personas independientes triunfó contra todo pronóstico y propuso una solución brillante a mediados de los años setenta. Crearon un sistema de cifrado que parecía desafiar toda lógica. Aunque los ordenadores transformaron la aplicación de las claves, la mayor revolución de la criptografía del siglo XX ha sido el desarrollo de técnicas para superar el problema de la distribución de claves. De hecho, este avance está considerado el mayor logro criptográfico desde la invención de la cifra monoalfabética, hace más de dos mil años.

1. Dios premia a los tontos

Whitfield Diffie es uno de los criptógrafos más exuberantes de su generación. Su mero aspecto ofrece una imagen llamativa y en cierta medida contradictoria. Su impecable traje refleja el hecho de que durante la mayor parte de los años noventa ha estado trabajando para una de las compañías gigantes de ordenadores de Estados Unidos; actualmente el título oficial de su trabajo es ingeniero distinguido

de Sun Microsystems. Sin embargo, su melena hasta los hombros y su larga barba blanca delatan el hecho de que su corazón todavía está anclado en los años sesenta. Pasa mucho tiempo ante una terminal de ordenador, pero parece que se sentiría igual de a gusto en un ashram de Bombay. Diffie es consciente de que su ropa y su personalidad pueden causar mucha impresión a los demás, y comenta: «*La gente siempre piensa que soy más alto de lo que realmente soy, y me han dicho que es el "efecto Saltarín". No importa lo que pese en kilos y gramos, siempre parece más grande a causa de los botes que da*».

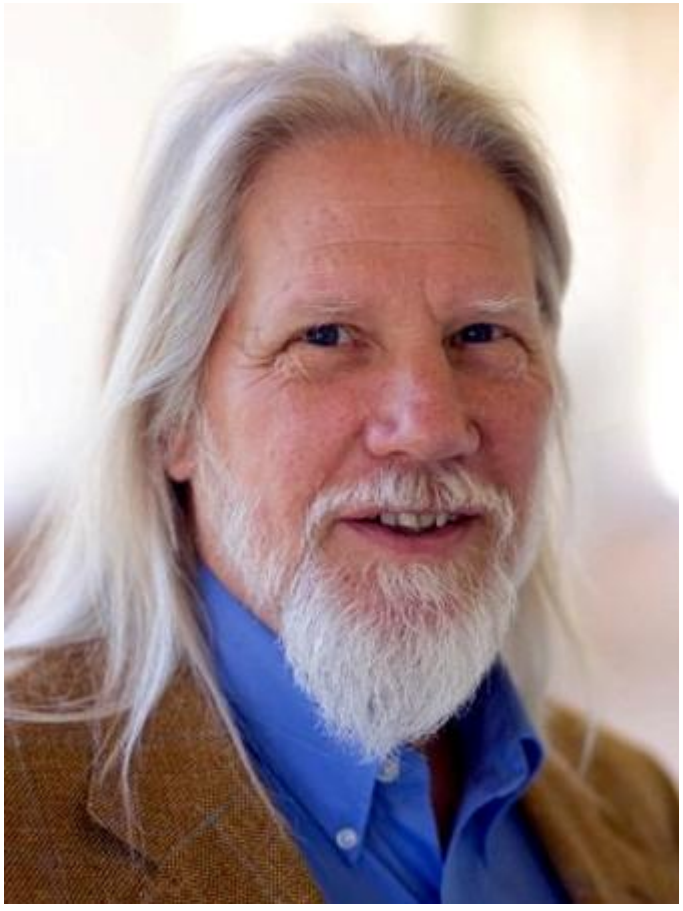


Figura 62. Whitfield Diffie

Diffie nació en 1944, y pasó la mayor parte de su infancia en Queens, Nueva York. De niño se fascinó con las matemáticas y leyó libros que iban del Manual de tablas matemáticas de la Compañía de goma química al Curso de matemática pura de G. H. Hardy. Después fue a estudiar matemáticas en el MIT (Massachusetts Institute of

Technology), graduándose en 1965. Entonces ejerció una serie de empleos relacionados con la seguridad informática, y para comienzos de los años setenta se había convertido en uno de los pocos expertos en seguridad verdaderamente independientes, un criptógrafo por libre, no empleado por el gobierno o por alguna de las grandes compañías. En retrospectiva, fue el primer cifropunk, o punk de las cifras[21].

Diffie estaba particularmente interesado en el problema de la distribución de claves y se dio cuenta de que quien lograra encontrar una solución pasaría a la historia como uno de los mejores criptógrafos de todos los tiempos. Se sentía tan cautivado por el problema de la distribución de claves que lo convirtió en la anotación más importante de su cuaderno especial, titulado «Problemas para una Teoría Ambiciosa de la Criptografía». Parte de la motivación de Diffie provenía de su visión de un mundo interconectado. En los años sesenta, el Departamento de Defensa de Estados Unidos comenzó a financiar una vanguardista organización de investigación llamada ARPA (Advanced Research Projects Agency, Agencia de Proyectos Avanzados de Investigación), y uno de los proyectos más avanzados de ARPA era encontrar una manera de conectar los ordenadores militares a través de grandes distancias. Esto permitiría que un ordenador que se hubiera deteriorado transfiriera sus responsabilidades a otro de la red. El objetivo principal era fortalecer la infraestructura informática del Pentágono ante la posibilidad de un ataque nuclear, pero la red permitiría también que los científicos intercambiaran mensajes y realizasen cálculos sacando partido a la capacidad de espacio de ordenadores remotos. ARPANet nació en 1969, y para finales de ese año había cuatro emplazamientos conectados. ARPANet creció constantemente, y en 1982 generó Internet. A finales de los años ochenta, se dio acceso a Internet a usuarios no académicos y no gubernamentales, y a partir de entonces el número de usuarios se disparó. Hoy día, más de cien millones de personas utilizan Internet para intercambiar información y enviar mensajes de correo electrónico, o *e- mail.*

Cuando ARPANet estaba todavía en pañales, Diffie tuvo la suficiente visión de futuro para pronosticar la llegada de la superautopista de la información y la revolución

[21] En la traducción al castellano se pierde el juego de palabras del original: el autor afirma que Diffie fue el primer cipherpunk (punk de las cifras), jugando con la similitud de esa palabra con cyberpunk (punk del ciberespacio), que alude a una corriente de ciencia ficción que presenta estilos y actitudes punk combinados con alta tecnología. (N. del T.)

digital. Un día, la gente corriente tendría su propio ordenador, y estos ordenadores estarían interconectados mediante las líneas telefónicas. Diffie creía que si la gente usaba entonces sus ordenadores para intercambiar *e-mails*, merecía el derecho a cifrar sus mensajes para garantizar su privacidad. Sin embargo, el cifrado requería el intercambio seguro de claves. Si los gobiernos y las grandes compañías estaban teniendo problemas para hacer frente a la distribución de las claves, entonces al público en general le resultaría imposible y de hecho se vería privado del derecho a la privacidad.

Diffie imaginó dos extraños que se conocen a través de Internet y se preguntan cómo podrían enviarse un mensaje codificado el uno al otro. También consideró la posibilidad de una persona que quisiera comprar un producto en Internet. ¿Cómo podría esa persona enviar un *e-mail* que contuviera detalles codificados de su tarjeta de crédito de modo que sólo ese vendedor en particular pudiera descifrarlos? En ambos casos, parecía que las dos partes necesitaban compartir una clave, pero ¿cómo podrían intercambiar claves de una forma segura? El número de contactos casuales y la cantidad de *e- mails* espontáneos entre la gente sería enorme y esto significaría que la distribución de claves no sería práctica. Diffie temía que la necesidad de la distribución de claves impediría que la gente tuviera acceso a la privacidad digital y se obsesionó con la idea de encontrar una solución al problema.

En 1974, Diffie, todavía un criptógrafo itinerante, visitó el laboratorio Thomas J. Watson de la IBM, donde le habían invitado a dar una charla. Habló sobre varias estrategias para atacar el problema de la distribución de claves, pero todas sus ideas eran muy tentativas y su audiencia se mostró escéptica acerca de las perspectivas de una solución.

La única respuesta positiva a la presentación de Diffie fue la de Alan Konheim, uno de los expertos criptográficos veteranos de la IBM, que mencionó que otra persona había visitado recientemente el laboratorio y había dado también una conferencia que abordaba el tema de la distribución de claves. Se trataba de Martin Hellman, un profesor de la Universidad de Stanford, en California. Esa misma tarde, Diffie se montó en su coche y comenzó el viaje de 5.000 km a la costa oeste para conocer a la única persona que parecía compartir su obsesión. La alianza entre Diffie y Hellman se convertiría en una de las asociaciones más dinámicas de la criptografía.

Martin Hellman había nacido en 1946 en un barrio judío del Bronx, en Nueva York, pero cuando tenía cuatro años su familia se mudó a un barrio predominantemente católico irlandés.

Según Hellman, esto cambió para siempre su actitud ante la vida: «Los demás niños iban a la iglesia y aprendían que los judíos mataron a Cristo, así que me llamaban "asesino de Cristo". También me daban palizas. Al principio, yo quería ser como los demás niños, quería un árbol de navidad y quería regalos cristianos. Pero luego me di cuenta de que no podía ser como todos los demás niños, y para defenderme adopté una actitud de "¿A quién le interesa ser como todos los demás?". Hellman ve el origen de su interés en las cifras en este persistente deseo de ser diferente. Sus colegas le habían dicho que estaba loco por hacer investigación en criptografía, porque estaría compitiendo con la NSA y su presupuesto multibillonario en dólares. ¿Cómo podía esperar descubrir algo que ellos no supieran ya? Y si llegaba a descubrir algo, la NSA lo clasificaría.

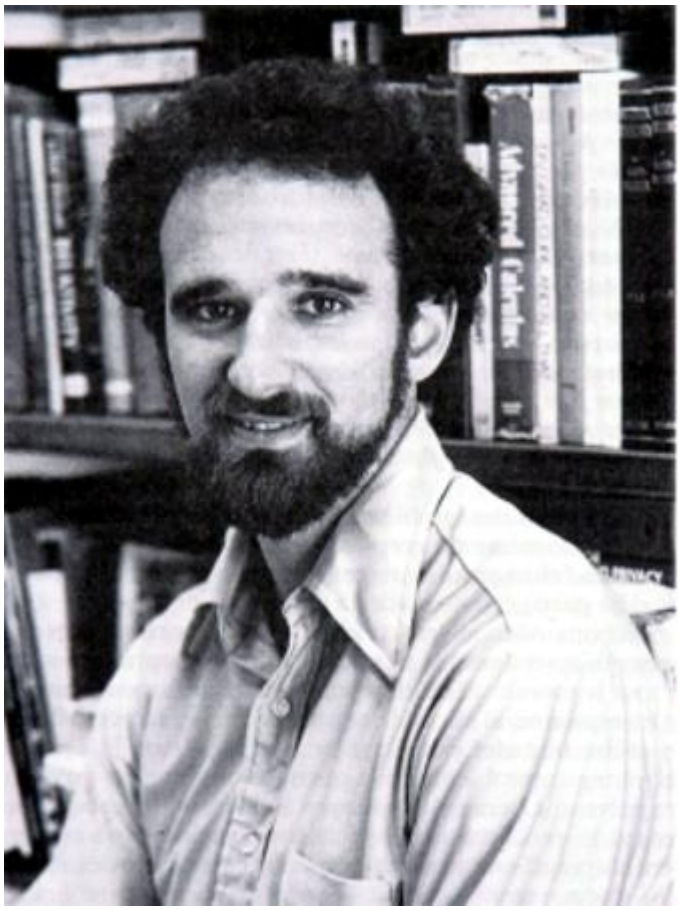


Figura 63. Martin Hellman

Justo cuando Hellman estaba comenzando su investigación, encontró *The Codebreakers* («Los descifradores») del historiador David Kahn. Este libro era la primera exposición detallada del desarrollo de las cifras, y como tal era la obra perfecta para un criptógrafo en ciernes.

The Codebreakers era el único compañero de Hellman en su investigación, hasta que en septiembre de 1974 recibió una inesperada llamada de teléfono de Whitfield Diffie, que acababa de cruzar el continente en su coche para conocerlo. Hellman nunca había oído hablar de Diffie, pero aceptó de mala gana una cita de media hora esa misma tarde. Al final del encuentro, Hellman se dio cuenta de que Diffie era la persona mejor informada que había conocido. Esa sensación era mutua. Hellman recuerda: «*Había prometido a mi mujer que iría a casa a cuidar a los niños, así que él se vino a casa conmigo y cenamos juntos. Se marchó hacia medianoche. Nuestras personalidades eran muy diferentes —él es mucho más contracultural que yo— pero el choque de personalidades resultó ser muy simbiótico. Era una bocanada de aire fresco para mí. Trabajar totalmente aislado había sido muy duro*».

Como Hellman no contaba con mucha financiación, no se podía permitir emplear a su nuevo compañero como investigador. En vez de eso, Diffie se matriculó como estudiante graduado. Juntos, Hellman y Diffie comenzaron a estudiar el problema de la distribución de claves, intentando desesperadamente encontrar una alternativa a la pesada tarea de transportar las claves físicamente cruzando grandes distancias. A su debido tiempo, se les unió Ralph Merkle. Merkle era un refugiado intelectual, que había emigrado de otro grupo de investigación en el que el profesor no sentía ninguna simpatía por el sueño imposible de resolver el problema de la distribución de claves. Dice Hellman:

> *Ralph, como nosotros, estaba dispuesto a ser un tonto. Y la forma de llegar a la cima en cuanto a desarrollar una investigación original es ser un tonto, porque sólo los tontos siguen intentándolo. Tienes la idea número 1, te entusiasmas y fracasa. Luego tienes la idea número 2, te entusiasmas y fracasa. Luego tienes la idea número 99, te entusiasmas y fracasa. Sólo un tonto se entusiasmaría con la*

idea número 100, pero puede que hagan falta 100 ideas antes de que una valga realmente la pena. A no ser que seas lo suficientemente tonto para entusiasmarte continuamente, no tendrás la motivación, no tendrás la energía para llegar hasta el final. Dios premia a los tontos.

Todo el problema de la distribución de claves es una situación clásica de círculo vicioso. Si dos personas quieren intercambiar un mensaje secreto por teléfono, el emisor debe codificarlo. Para codificar el mensaje secreto, el emisor debe usar una clave, que es en sí misma un secreto, de modo que entonces hay el problema de transmitir la clave secreta al receptor para transmitir el mensaje secreto. En resumen, antes de que dos personas puedan intercambiar un secreto (un mensaje codificado) deben ya compartir un secreto (la clave).

Al considerar el problema de la distribución de claves resulta útil imaginar a Alicia, Benito y Eva, tres personajes ficticios que se han convertido en estándares en las discusiones sobre criptografía[22]. En una situación típica, Alicia quiere enviar un mensaje a Benito, o viceversa, y Eva está tratando de enterarse. Si Alicia está enviando mensajes secretos a Benito codificará cada uno de ellos antes de enviarlo, utilizando una clave distinta cada vez. Alicia se tiene que enfrentar continuamente al problema de la distribución de claves, porque tiene que transmitir las claves a Benito de una manera segura, de otra forma él no podrá descodificar el mensaje.

Una manera de solucionar el problema es que Alicia y Benito se encuentren una vez a la semana e intercambien suficientes claves para cubrir los mensajes que podrían enviar durante los siete días siguientes. Intercambiar claves en persona es sin duda seguro, pero presenta muchos inconvenientes y si Alicia o Benito se ponen enfermos, todo el sistema se viene abajo. Como alternativa, Alicia y Benito podrían contratar a mensajeros, lo que sería menos seguro y más caro, pero al menos delegarían parte del trabajo. En cualquier caso, parece que la distribución de claves es inevitable. Durante dos mil años esto se consideraba un axioma de la criptografía —una verdad indiscutible—. Sin embargo, Diffíe y Hellman eran conscientes de una

[22] Los nombres originales en inglés son Alice, Bob y Eve. En este contexto informático, Bob (diminutivo de Robert) se traduce generalmente como Benito en castellano para conservar la inicial B que se usa al explicar los cálculos. (N. del T.)

anécdota que parecía desafiar al axioma.

Imagine que Alicia y Benito viven en un país donde el sistema postal es completamente inmoral, y los empleados postales leen toda la correspondencia desprotegida. Un día, Alicia quiere enviar un mensaje sumamente personal a Benito. Lo mete en una caja de hierro, la cierra y le pone un candado. Pone la caja cerrada con candado en el correo y se queda con la llave. Sin embargo, cuando Benito recibe la caja, no puede abrirla porque no tiene la llave. Alicia podría considerar poner la llave dentro de otra caja, cerrarla con candado y enviársela a Benito, pero sin la llave del segundo candado, él no puede abrir la segunda caja, de modo que no puede obtener la llave que abre la primera caja. La única manera de evitar el problema parece ser que Alicia haga una copia de la llave y se la dé a Benito de antemano cuando queden para tomar un café. Hasta ahora, lo único que he hecho es plantear el mismo viejo problema en una nueva situación. Evitar la distribución de la llave parece lógicamente imposible; indudablemente, si Alicia quiere encerrar algo en una caja para que sólo Benito pueda abrirla, debe darle una copia de la llave. O, en términos de criptografía, si Alicia quiere codificar un mensaje para que sólo Benito pueda descifrarlo, debe darle una copia de la clave. El intercambio de la clave es una parte inevitable de la codificación, ¿o no?

Ahora imagine la siguiente situación. Como antes, Alicia quiere enviar un mensaje sumamente personal a Benito. De nuevo, mete su mensaje secreto en una caja de hierro, la cierra con candado y se la envía a Benito. Cuando llega la caja, Benito añade su propio candado y vuelve a enviar la caja a Alicia. Cuando Alicia recibe la caja, ahora está cerrada con dos candados. Ella retira su propio candado, dejando que sólo el candado de Benito cierre la caja. Finalmente, vuelve a enviar la caja a Benito. Y aquí está la diferencia crucial: ahora Benito puede abrir la caja porque está cerrada sólo con su propio candado y únicamente él tiene la llave.

Las implicaciones de esta pequeña historia son enormes. Demuestra que un mensaje secreto se puede intercambiar de manera segura entre dos personas sin que tengan necesariamente que intercambiar una clave. Por vez primera, aparece una insinuación de que el intercambio de claves podría no ser una parte inevitable de la criptografía. Podemos reinterpretar la historia en términos de codificación. Alicia usa su propia clave para codificar un mensaje para Benito, el cual vuelve a

codificarlo con su propia clave y lo devuelve. Cuando Alicia recibe el mensaje doblemente codificado retira su propia codificación y se lo devuelve a Benito, que entonces puede retirar su propia codificación y leer el mensaje.

Parece que el problema de la distribución de claves podría estar resuelto, porque la estratagema de la codificación doble no requiere ningún intercambio de claves. Sin embargo, hay un obstáculo fundamental para la puesta en práctica de un sistema en el que Alicia codifica, Benito codifica, Alicia descodifica y Benito descodifica. El problema radica en el orden en que se realizan las codificaciones y las descodificaciones. En general, el orden de la codificación y la descodificación es crucial, y debería obedecer la máxima «lo último que se pone es lo primero que se quita».

En otras palabras, la última fase de codificación debería ser la primera en ser descodificada. En la situación anterior, Benito realizó la última fase de la codificación, de modo que esto debería ser lo primero que se descodifique, pero fue Alicia la que retiró su propia codificación primero, antes de que Benito retirase la suya. La importancia del orden se comprende más fácilmente al examinar algo que hacemos todos los días. Por la mañana nos ponemos los calcetines, y luego nos ponemos los zapatos, y por la noche nos quitamos los zapatos antes de quitarnos los calcetines: es imposible quitarse los calcetines antes que los zapatos. Debemos obedecer la máxima «lo último que se pone es lo primero que se quita».

Algunas cifras muy elementales, como la cifra del César, son tan simples que el orden no importa. Sin embargo, en los años setenta parecía que cualquier forma de codificación potente siempre debe obedecer la regla de «lo último que se pone es lo primero que se quita». Si un mensaje está codificado con la clave de Alicia y luego con la clave de Benito, entonces debe ser descodificado con la clave de Benito antes de poder descodificarlo con la clave de Alicia. El orden es crucial incluso con una cifra de sustitución monoalfabética. Imagine que Alicia y Benito tienen cada uno su propia clave, como se muestra a continuación, y observemos lo que sucede cuando el orden es incorrecto. Alicia usa su clave para codificar un mensaje dirigido a Benito, luego Benito vuelve a codificar el resultado utilizando su propia clave; Alicia usa su propia clave para realizar una descodificación parcial, y finalmente Benito trata de utilizar su propia clave para realizar la descodificación completa.

El resultado no tiene ningún sentido. Sin embargo, usted puede comprobar por sí mismo que si el orden de la descodificación se invirtiera y Benito descodificara antes que Alicia, obedeciendo así la regla de «lo último que se pone es lo primero que se quita», entonces el resultado habría sido el mensaje original. Pero si el orden es tan importante, ¿por qué pareció que funcionaba el sistema en la anécdota de la caja cerrada con candados? La respuesta es que el orden no es importante para los candados. Podemos ponerle veinte candados a una caja y quitarlos en cualquier orden, y al final la caja estará abierta.

Desgraciadamente, los sistemas de cifrado son mucho más sensibles que los candados en lo que respecta al orden.

Clave de Alicia

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
H	F	S	U	G	T	A	K	V	D	E	O	Y	J	B	P	N	X	W	C	Q	R	I	M	Z	L

Clave de Benito

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
C	P	M	G	A	T	N	O	J	E	F	W	I	Q	B	U	R	Y	H	X	S	D	Z	K	L	V

Mensaje	n	o	s		v	e	m	o	s		a		m	e	d	i	o	d	í	a						
Codificado con la clave de Alicia	J	B	W		R	G	Y	B	W		H		Y	G	U	V	B	U	V	H						
Codificado con la clave de Benito	E	P	Z		Y	N	L	P	Z		O		L	N	S	D	P	S	D	O						
Descodificado con la clave de Alicia	K	P	Y		M	Q	Z	P	Y		L		Z	Q	C	J	P	C	J	L						
Descodificado con la clave de Benito	x	b	r		c	n	w	b	r		y		w	n	a	i	b	a	i	y						

Aunque el enfoque de la caja cerrada con dos candados no funcionaría en la criptografía de la vida real, inspiró a Diffie y Hellman a buscar un método práctico para resolver el problema de la distribución de claves. Pasaron mes tras mes tratando de encontrar una solución. Aunque cada idea terminaba en fracaso se comportaron como perfectos tontos y perseveraron. Su investigación se centró en el examen de varias *funciones* matemáticas. Una función es cualquier operación matemática que convierte un número en otro. Por ejemplo, «doblar» es un tipo de función, porque convierte el número 3 en el número 6, o el número 9 en el número

18. Además, podemos considerar todas las formas de codificación por ordenador como funciones, porque convierten un número (el texto llano) en otro número (el texto cifrado).

La mayoría de las funciones matemáticas son clasificadas como funciones de doble vía, porque son fáciles de hacer y fáciles de deshacer. Por ejemplo, «doblar» es una función de doble vía porque es fácil doblar un número para generar un nuevo número y es igual de fácil deshacer la función y obtener otra vez el número original partiendo del número doblado. Por ejemplo, si sabemos que el resultado de doblar es 26, es muy simple invertir la función y deducir que el número original era el 13. La manera más fácil de comprender el concepto de función de doble vía es desde el punto de vista de una actividad cotidiana. El acto de pulsar un interruptor de la luz es una función, porque convierte una bombilla normal en una bombilla encendida. Esta función es de doble vía porque si se enciende el interruptor es fácil apagarlo y poner de nuevo la bombilla en su estado original.

Sin embargo, Diffie y Hellman no estaban interesados en las funciones de doble vía. Concentraron su atención en las funciones de una sola vía. Como su nombre sugiere, una función de una sola vía es fácil de hacer pero muy difícil de deshacer. En otras palabras, las funciones de doble vía son reversibles, pero las funciones de una sola vía son irreversibles. Una vez más, la mejor manera de ilustrar una función de una sola vía es desde el punto de vista de una actividad cotidiana. Mezclar pintura amarilla y azul para hacer pintura verde es una función de una sola vía, porque es fácil mezclar las pinturas, pero es imposible separarlas. Otra función de una sola vía es cascar un huevo, porque es fácil cascarlo, pero es imposible volver a poner el huevo en su condición original.

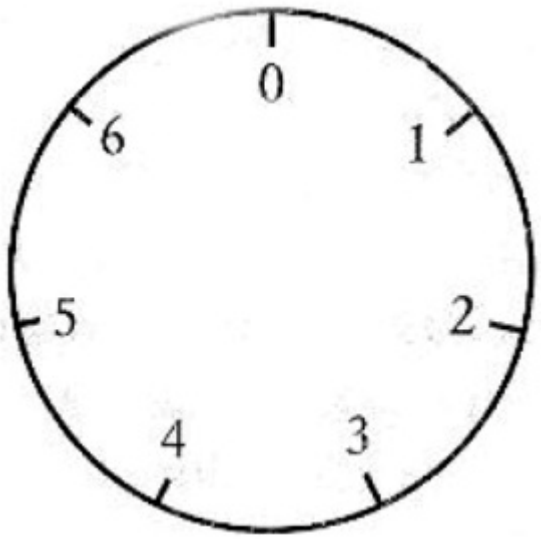


Figura 64. La aritmética modular se realiza con una serie finita de números, que pueden ser imaginados como números en una esfera de reloj. En este caso, podemos calcular 6 + 5 en modular 7 empezando en 6 y avanzando cinco espacios, lo que nos lleva a 4.

La *aritmética modular*, denominada a veces *aritmética de reloj*, es un área de las matemáticas muy rica en funciones de una sola vía. En aritmética modular, los matemáticos consideran un grupo finito de números dispuestos en círculo, de manera bastante similar a los números de un reloj. Por ejemplo, la Figura 64 muestra un reloj para el modular 7 (o mod 7), que sólo tiene los 7 números del 0 al 6. Para calcular 2 + 3, empezamos en el 2 y avanzamos 3 lugares para llegar a 5, que es la misma respuesta que en aritmética normal. Para calcular 2 + 6, comenzamos en el 2 y avanzamos 6 lugares, pero esta vez vamos más allá de número mayor y llegamos a 1, que no es el resultado que obtendríamos en aritmética normal. Estos resultados se pueden expresar de esta manera:

$$2 + 3 = 5 \pmod 7 \text{ y } 2 + 6 = 1 \pmod 7$$

La aritmética modular es relativamente simple, y de hecho la practicamos todos los días cuando hablamos de la hora. Si ahora son las nueve, y tenemos una reunión dentro de 8 horas, diremos que la reunión es a las cinco, no a las 17. Hemos calculado mentalmente 9 + 8 en (mod 12). Imagine la esfera de un reloj, mire el 9 y luego avance 8 espacios, y acabamos en el 5:

$$9 + 8 = 5 \pmod{12}$$

En vez de visualizar relojes, los matemáticos a menudo toman el atajo de realizar cálculos modulares según la siguiente receta. Primero, realizamos el cálculo en aritmética normal. Segundo, si queremos saber la respuesta en (mod x), dividimos la respuesta normal por x y anotamos el resto que queda. Este resto es la respuesta en (mod x). Para encontrar la respuesta a 11 x 9 (mod 13), hacemos lo siguiente:

$$11 \times 9 = 99$$

$$99 : 13 = 7, \text{ y quedan } 8$$

$$11 \times 9 = 8 \pmod{13}$$

Las funciones realizadas en el ámbito de la aritmética modular tienden a comportarse de manera irregular, lo que a su vez las convierte en ocasiones en funciones de una sola vía. Esto se vuelve evidente cuando una simple función en aritmética normal se compara con la misma simple función en aritmética modular. En el primer ámbito, la función será de doble vía y será fácil invertirla; en el segundo ámbito, será de una sola vía y difícil de invertir. Como ejemplo, tomemos la función 3^X. Esto significa que se toma un número x, luego se multiplica el 3 por sí mismo x veces para obtener el nuevo número. Por ejemplo, si x = 2, y realizamos la función, entonces:

$$3^x = 3^2 = 3 \times 3 = 9$$

En otras palabras, la función convierte a 2 en 9. En aritmética normal, según aumenta el valor de x, aumenta también el resultado de la función. Por eso, si se nos diera el resultado de la función sería relativamente fácil invertir el cálculo y deducir el número original. Por ejemplo, si el resultado es 81, podemos deducir que x es 4, porque $3^4 = 81$.

Si cometemos un error y suponemos que x es 5, podríamos calcular que $3^5 = 243$, lo que nos indica que nuestra elección de x es demasiado alta. Entonces reduciríamos nuestra elección de x a 4, y tendríamos la respuesta correcta. En

resumen, incluso cuando suponemos mal podemos alcanzar el valor correcto de x, y con ello invertir la función.

Sin embargo, en aritmética modular esta misma función no se comporta tan sensatamente. Imagine que nos dicen que 3^X en (mod 7) es 1, y nos piden que encontremos el valor de x. Ningún valor nos viene a la mente, porque en general no estamos familiarizados con la aritmética modular. Podríamos hacer la conjetura de que x = 5, y podríamos calcular el resultado de 3^5 (mod 7). La respuesta resulta ser 5, es decir, demasiado alta, porque estamos buscando una respuesta de sólo 1. Podríamos sentirnos tentados a reducir el valor de x e intentarlo de nuevo. Pero no estaríamos yendo en la dirección correcta, porque la respuesta verdadera es x= 6.

En la aritmética normal podemos probar números y darnos cuenta si nos estamos acercando a la solución o no.

Tabla 25.

Valores de la función 3^x calculados en aritmética normal (línea 2) y en aritmética modular (línea 3). La función aumenta continuamente en aritmética normal, pero es sumamente irregular en aritmética modular.

x	1	2	3	4	5	6
3^x	3	9	27	81	243	729
$3^x \pmod 7$	3	2	6	4	5	1

El ámbito de la aritmética modular no nos proporciona pistas útiles, e invertir las funciones es mucho más difícil. A menudo, la única manera de invertir una función en aritmética modular es compilar una tabla calculando la función para muchos valores de x hasta que encontremos la respuesta correcta. La Tabla 25 muestra el resultado de calcular varios valores de la función tanto en aritmética normal como en aritmética modular. La tabla demuestra claramente la conducta irregular de la función cuando se calcula en aritmética modular. Aunque elaborar semejante tabla es sólo un poco tedioso cuando se trata de números relativamente pequeños, sería

terriblemente penoso construir una tabla con una función como 453^x (mod 21.997). Éste es un ejemplo clásico de función de una sola vía, porque yo podría elegir un valor para x y calcular el resultado de la función, pero si le ofrezco un resultado, pongamos 5.787, usted tendría enormes dificultades para invertir la función y deducir mi elección de x. Sólo me costó unos segundos realizar el cálculo y generar el número 5.787, pero a usted le llevaría horas elaborar la tabla y calcular mi elección de x.

Después de dos años concentrándose en la aritmética modular y las funciones de una sola vía, la «tontería» de Hellman empezó a producir frutos. En la primavera de 1976 dio con una estrategia para resolver el problema de la distribución de claves. Escribiendo frenéticamente durante media hora, demostró que Alicia y Benito podían acordar una clave sin reunirse, deshaciéndose así de un axioma que había durado siglos. La idea de Hellman se basaba en una función de una sola vía de la forma Y^x (mod P). Inicialmente, Alicia y Benito acuerdan valores para Y y P. Casi cualquier valor sirve, pero hay algunas restricciones, como que Y debe ser un número más bajo que P. Estos valores no son secretos, de modo que Alicia puede llamar por teléfono a Benito y sugerir, pongamos, Y = 7 y P = 11. Incluso si la línea de teléfono no es segura y la malvada Eva oye esta conversación, no importa, como veremos después. Alicia y Benito han acordado ahora la función 7^x (mod 11). Ahora pueden comenzar el proceso de tratar de establecer una clave sin reunirse. Como trabajan paralelamente, explico sus acciones en las dos columnas de la Tabla 26.

Siguiendo las fases de la Tabla 26 se verá que, sin reunirse, Alicia y Benito han acordado la misma clave, que pueden utilizar para codificar un mensaje. Por ejemplo, podrían usar su número, 9, como la clave para una codificación DES. (En realidad, DES utiliza números mucho mayores como clave, y el intercambio descrito en la Tabla 26 se realizaría con números mucho más altos, resultando en una clave alta apropiada para DES).

Usando la estratagema de Hellman, Alicia y Benito han conseguido acordar una clave, pero no tuvieron que reunirse y susurrarse la clave.

El extraordinario logro es que la clave secreta se acordó mediante un intercambio de información en una línea telefónica normal. Pero si Eva intervino esta línea, también sabrá la clave, ¿no?

Tabla 26

La función general de una sola vía es Y^X (mod *P).* Alicia y Benito han elegido valores para *Y* y *P,* y de esta forma han acordado la función de una sola vía 7^X (mod 11).

	Alicia	Benito
Fase 1	Alicia elige un número, pongamos el 3, y lo mantiene secreto. Denominamos a su número *A*.	Benito elige un número, pongamos el 6, y lo mantiene secreto. Denominamos a su número *B*.
Fase 2	Alicia pone 3 en la función de una sola vía y calcula el resultado de 7^A (mod 11): 7^3 (mod 11) = 343 (mod 11) = 2	Benito pone 6 en la función de una sola vía y calcula el resultado de 7^B (mod 11): 7^6 (mod 11) = 117.649 (mod 11) = 4
Fase 3	Alicia llama al resultado de este cálculo α, y envía su resultado, 2, a Benito.	Benito llama al resultado de este cálculo β, y envía su resultado, 4, a Alicia.
El intercambio	Normalmente, éste sería un momento crucial, porque Alicia y Benito están intercambiando información y, por tanto, ésta es una oportunidad para que Eva escuche subrepciamente y descubra los detalles de la información. Sin embargo, resulta que Eva puede escuchar sin que esto afecte la seguridad final del sistema. Alicia y Benito podrían usar la misma línea telefónica que utilizaron para acordar los valores para *Y* y *P,* y Eva podría interceptar los dos números que están siendo intercambiados, 2 y 4. Sin embargo, estos números no son la clave, y es por esto por lo que no importa que Eva los sepa.	
Fase 4	Alicia toma el resultado de Benito, y calcula el resultado de β^A (mod 11): 4^3 (mod 11) = 64 (mod 11) = 9	Benito toma el resultado de Alicia, y calcula el resultado de α^B (mod 11): 2^6 (mod 11) = 64 (mod 11) = 9
La clave	Milagrosamente, Alicia y Benito han acabado con el mismo número, el 9. ¡Ésta es la clave!	

Examinemos el sistema de Hellman desde el punto de vista de Eva. Si ella está interviniendo la línea, conoce sólo los siguientes hechos: que la función es 7^X (mod 11), que Alicia envía a = 2 y que Benito envía B = 4. Para encontrar la clave, tiene

que hacer lo que hace Benito, que es convertir *a* en la clave conociendo el valor de B, o bien hacer lo que hace Alicia, que es convertir B en la clave conociendo el valor de A. Sin embargo, Eva no conoce el valor de A o de B porque Alicia y Benito no han intercambiado estos números, sino que los han mantenido en secreto. A Eva sólo le queda una esperanza: en teoría, podría calcular A a partir de a, porque surgió de poner A en una función, y Eva sabe de qué función se trata. O podría calcular B a partir de B, porque B surgió de poner B en una función y, de nuevo, Eva sabe de qué función se trata. Desgraciadamente para Eva, la función es de una sola vía, de modo que, aunque fue fácil para Alicia convertir A en a, y para Benito convertir B en B, es muy difícil para Eva invertir el proceso, especialmente si los números son muy altos.

Benito y Alicia intercambiaron tan sólo la información suficiente para permitirles establecer una clave, pero esta información fue insuficiente para que Eva calculase la clave. Como analogía del sistema de Hellman, imagine una cifra que de alguna forma utiliza el color como clave. Primero, supongamos que todo el mundo, incluidos Alicia, Benito y Eva, tiene un bote de tres litros que contiene un litro de pintura amarilla. Si Alicia y Benito quieren acordar una clave secreta, cada uno de ellos añade un litro de su propio color secreto a su propio bote. Alicia podría añadir un tono peculiar de morado, mientras que Benito podría añadir carmesí. Cada uno envía al otro su propio bote mezclado. Finalmente, Alicia toma la mezcla de Benito y le añade un litro de su propio color secreto, y Benito toma la mezcla de Alicia y le añade un litro de su propio color secreto. Ambos botes deben ser ahora del mismo color, porque ambos contienen un litro de amarillo, un litro de morado y un litro de carmesí. Es el color exacto de los botes doblemente contaminados el que se utiliza como clave. Alicia no tiene ni idea sobre qué color añadió Benito, y Benito no tiene ni idea sobre qué color añadió Alicia, pero ambos han conseguido el mismo resultado. Mientras tanto, Eva está furiosa. Incluso si intercepta los botes intermedios, no puede deducir el color de los botes finales, que es la clave acordada. Podría ver el color del bote mezclado que va camino de Benito y que contiene amarillo y el color secreto de Alicia, y podría ver el color del bote mezclado que va camino de Alicia y que contiene amarillo y el color secreto de Benito, pero para deducir la clave necesita saber realmente los colores secretos originales de

Alicia y Benito. Sin embargo, Eva no puede deducir los colores secretos de Alicia y Benito mirando los botes mezclados. Incluso si toma una muestra de uno de los botes mezclados, no puede separar las pinturas para descubrir el color secreto, porque mezclar pintura es una función de una sola vía.

El avance de Hellman se le ocurrió mientras estaba trabajando en casa por la noche, de modo que para cuando finalizó su cálculo era demasiado tarde para llamar a Diffie y Merkle. Tuvo que esperar hasta la mañana siguiente para revelar su descubrimiento a las otras dos únicas personas en el mundo que habían creído que una solución al problema de la distribución de claves era siquiera posible. «La musa me sonrió a mí», dice Hellman, «pero todos nosotros sentamos las bases juntos». Diffie reconoció inmediatamente el poder del avance de Hellman: «*Marty explicó su sistema de intercambio de claves en toda su inquietante simplicidad. Al escucharle, me di cuenta de que el concepto me había estado rondando la cabeza por algún tiempo, pero nunca se había abierto paso realmente*».

El sistema Diffie-Hellman-Merkle de intercambio de claves, como se conoce, permite que Alicia y Benito establezcan un secreto a través de una conversación pública. Es uno de los descubrimientos más contraintuitivos de la historia de la ciencia y obligó al mundo criptográfico establecido a reescribir las reglas de la codificación. Diffie, Hellman y Merkle demostraron públicamente su descubrimiento en el Congreso Nacional de Informática de junio de 1976 y asombraron a la audiencia de criptoexpertos. Al año siguiente solicitaron una patente. A partir de entonces, Alicia y Benito ya no necesitaban reunirse para intercambiar una clave. En vez de ello, Alicia podía simplemente llamar a Benito por teléfono, intercambiar con él un par de números, establecer mutuamente una clave secreta y luego ponerse a codificar.

Aunque el sistema Diffie-Hellman- Merkle de intercambio de claves constituyó un gigantesco paso adelante, aún no era perfecto, porque tenía un inconveniente inherente. Imagine que Alicia vive en Hawai, y que quiere enviar un *e-mail* a Benito en Estambul. Probablemente, Benito esté durmiendo, pero lo bueno del *e-mail* es que Alicia puede enviar un mensaje en cualquier momento y estará esperando en el ordenador de Benito cuando éste se despierte.

Sin embargo, si Alicia quiere codificar su mensaje, necesita acodar una clave con Benito, y para llevar a cabo el intercambio de clave es preferible que estén

conectados al mismo tiempo: establecer una clave requiere un intercambio mutuo de información. De hecho, Alicia tiene que esperar a que Benito se despierte. Como alternativa, Alicia podría transmitir su parte del intercambio de clave y esperar 12 horas la respuesta de Benito.

En ese momento, se establece la clave y Alicia puede, si no está durmiendo ella misma, codificar y enviar el mensaje. En ambos casos, el sistema Hellman de intercambio de clave entorpece la espontaneidad del *e-mail.*

Hellman había echado por tierra uno de los principios de la criptografía y demostrado que Benito y Alicia no necesitaban reunirse para acordar una clave secreta. A continuación, a alguien sólo se le tenía que ocurrir un sistema más eficaz para vencer el problema de la distribución de claves.

2. El nacimiento de la criptografía de clave pública

Mary Fisher nunca ha olvidado la primera vez que Whitfield Diffie le pidió que salieran juntos:

> «*El sabía que yo era una apasionada del espacio, así que sugirió que fuéramos a ver el lanzamiento de un cohete. Whit explicó que se iba esa noche a ver el despegue del Skylab, y condujimos toda la noche, llegando hacia las tres de la mañana. El pájaro estaba en camino, como solían decir entonces. Whit tenía credenciales de prensa, pero yo no. Así que cuando pidieron irá identificación y preguntaron quién era yo, Whit dijo: "Mi esposa". Eso fue el 16 de noviembre de 1973*».

Efectivamente, llegaron a casarse, y durante los primeros años de matrimonio, Mary ayudó a su marido durante sus meditaciones criptográficas. Diffie todavía estaba empleado como estudiante graduado, lo que significaba que recibía tan sólo un salario exiguo. Mary, que era arqueóloga, se puso a trabajar para BP (British Petroleum) para apañarse económicamente.

Mientras Martin Hellman había estado desarrollando su método de intercambio de claves, Whitfield Diffie trabajaba en un enfoque completamente diferente para solucionar el problema de la distribución de claves. A menudo, atravesaba períodos

de contemplación estéril, y en una ocasión, en 1975, se sintió tan frustrado que le dijo a Mary que no era más que un científico fracasado que nunca llegaría a nada. Incluso le aconsejó que debería encontrar a otro hombre. Mary le respondió que tenía una fe absoluta en él, y tan sólo dos semanas después a Diffie se le ocurrió una idea verdaderamente brillante.

Todavía recuerda cómo la idea destelló en su mente, y luego casi desapareció: «*Bajaba por la escalera para coger una Coca-Cola, y casi se me olvidó la idea. Me acordaba que había estado pensando sobre algo interesante, pero no lograba acordarme de lo que era. Entonces volvió con una gran subida de adrenalina de excitación. Por vez primera en mi trabajo de criptografía era verdaderamente consciente de haber descubierto algo realmente valioso. Todo lo que había descubierto en ese campo hasta entonces me pareció que eran meros detalles técnicos*».

Era por la tarde temprano, y tenía que esperar un par de horas a que volviera Mary. «Whit estaba esperando delante de la puerta», recuerda ella. «Dijo que tenía que decirme algo y tenía una expresión peculiar en la cara. Entré y me dijo: “Siéntate, por favor; quiero hablar contigo. Creo que he hecho un gran descubrimiento; sé que soy la primera persona que lo ha hecho”. El mundo se detuvo para mí por un momento. Me sentí como si estuviera viviendo en una película de Hollywood».

Diffie había inventado un nuevo tipo de cifra, una cifra que incorporaba lo que se ha denominado un *clave asimétrica.* Hasta ahora, todas las técnicas de codificación descritas en este libro han sido *simétricas*, lo que significa que el proceso de descodificación es simplemente el opuesto al de codificación. Por ejemplo, la máquina Enigma utiliza cierta clave para codificar un mensaje y el receptor usa una máquina idéntica con la misma disposición de clave para descifrarlo. De manera similar, la codificación DES usa una clave para realizar 16 rondas de codificación, y luego la descodificación DES utiliza la misma clave para realizar 16 rondas a la inversa. Tanto el emisor como el receptor tienen, de hecho, un conocimiento equivalente, y ambos usan la misma clave para codificar y descodificar: su relación es simétrica. Por otra parte, en un sistema de clave asimétrica, como su nombre sugiere, la clave de codificación y la clave de descodificación no son idénticas. En una cifra asimétrica, si Alicia sabe la clave de codificación puede codificar un

mensaje, pero no puede descodifícar un mensaje. Para descodifícar, Alicia debe tener acceso a la clave de descodificación. Esta distinción entre las claves de codificación y de descodificación es lo que hace que una cifra asimétrica sea especial.

Hay que señalar, sin embargo, que aunque Diffie había concebido el concepto general de una cifra asimétrica no tenía realmente un ejemplo específico de semejante cifra. No obstante, el mero concepto de una cifra asimétrica era revolucionario. Si los criptógrafos podían encontrar una cifra asimétrica genuina que funcionase, un sistema que satisficiera los requisitos de Diffie, entonces las consecuencias para Alicia y Benito serían enormes. Alicia podría crear su propio par de claves: una clave de codificación y una clave de descodificación. Si suponemos que la cifra asimétrica es una forma de codificación por ordenador, entonces la clave de codificación de Alicia es un número, y su clave de descodificación es un número diferente. Alicia mantiene en secreto la clave de descodificación, por lo que normalmente se la llama la *clave privada* de Alicia. Sin embargo, ella publica su clave de codificación para que todo el mundo tenga acceso a ella, y por esta razón se la llama normalmente la *clave pública* de Alicia.

Si Benito quiere enviar un mensaje a Alicia, simplemente busca su clave pública, que debería aparecer en algo parecido a una guía telefónica. Entonces, Benito usa la clave pública de Alicia para codificar el mensaje. Le envía el mensaje codificado a Alicia y cuando llega, Alicia lo puede descodificar usando su clave de descodificación privada. De manera similar, si Carlos, Alba o Eduardo quieren enviar a Alicia un mensaje codificado, también ellos pueden buscar la clave de codificación pública de Alicia, y en todos los casos sólo Alicia tiene acceso a la clave de descodificación privada requerida para descodificar los mensajes.

La gran ventaja de este sistema es que no hay idas y venidas, como en el intercambio de claves Diffie-Hellman-Merkle. Benito no tiene que esperar a que Alicia le envíe cierta información antes de poder codificar un mensaje y enviárselo a ella; simplemente, tiene que buscar su clave de codificación pública. Además, el cifrado asimétrico soluciona aún el problema de la distribución de claves. Alicia no tiene que transportar la clave de codificación pública de una manera segura a Benito: por el contrario, ahora puede dar a conocer su clave de codificación pública

de la manera más amplia posible. Ahora, Alicia quiere que todo el mundo conozca su clave de codificación pública, para que cualquiera pueda enviarle mensajes codificados. Al mismo tiempo, incluso si todo el mundo conoce la clave pública de Alicia, nadie, incluida Eva, puede descifrar ningún mensaje codificado con ella, porque el conocimiento de la clave pública no ayudará a descodificar. De hecho, una vez que Benito ha codificado un mensaje utilizando la clave pública de Alicia, ni siquiera él puede descodificarlo. Sólo Alicia, que posee la clave privada, puede descodificar el mensaje.

Esto es exactamente lo opuesto a una cifra simétrica tradicional, en la que Alicia tiene que tomarse muchas molestias para transportar la clave de codificación de manera segura a Benito. En una cifra simétrica, la clave de codificación es la misma que la clave de descodificación, de modo que Alicia y Benito deben tomar enormes precauciones para asegurarse de que la clave no caiga en manos de Eva. Ésta es la raíz del problema de la distribución de claves.

Volviendo a la analogía de los candados, la criptografía asimétrica se puede considerar de la siguiente manera. Cualquiera puede cerrar un candado simplemente presionándolo hasta que haga clic, pero sólo la persona que tenga la llave podrá abrirlo. Cerrarlo (codificación) es fácil, cualquiera puede hacerlo, pero abrirlo (descodificación) es algo que sólo lo puede hacer el dueño de la llave. El simple conocimiento de saber cómo cerrar el candado no te dice cómo abrirlo. Llevando la analogía aún más lejos, imagine que Alicia diseña un candado y una llave. Guarda la llave, pero fabrica miles de réplicas del candado y los distribuye a oficinas de correos de todo el mundo.

Si Benito quiere enviar un mensaje, lo pone en una caja, va a la oficina de correos local, pide un «candado de Alicia» y cierra la caja con él. Ahora ya no puede abrir la caja, pero cuando Alicia la reciba podrá abrirla con su llave única. El candado y el proceso de cerrarlo son equivalentes a la clave de codificación pública, porque todo el mundo tiene acceso a los candados, y cualquiera puede utilizar un candado para encerrar un mensaje en una caja. La llave del candado es equivalente a la clave de descodificación privada, porque sólo Alicia la tiene, sólo ella puede abrir el candado y sólo ella puede tener acceso al mensaje que hay en la caja.

El sistema parece simple cuando se explica en términos de candados, pero no tiene

nada de simple encontrar una función matemática que haga el mismo trabajo, algo que se pueda incorporar a un sistema criptográfico factible. Para convertir la gran idea de las cifras asimétricas en un invento práctico, alguien tenía que descubrir una función matemática apropiada. Diffie imaginó un tipo especial de función de una sola vía que pudiera ser invertida en circunstancias excepcionales.

En el sistema asimétrico de Diffie, Benito codifica el mensaje usando la clave pública, pero no puede descodificarlo puesto que es esencialmente una función de una sola vía. Sin embargo, Alicia puede descodificar el mensaje porque tiene la clave privada, una información especial que le permite invertir la función. Una vez más, los candados son una buena analogía: cerrar el candado es una función de una sola vía, porque en general es difícil abrir el candado a no ser que tengas algo especial (la llave), en cuyo caso la función puede invertirse fácilmente.

Diffie publicó un esbozo de su idea en el verano de 1975, después de lo cual otros científicos se unieron a la búsqueda de una función de una sola vía apropiada, una función que satisficiera los criterios requeridos para un cifrado asimétrico. Al principio había un gran optimismo, pero al final de año nadie había logrado encontrar una candidata idónea. Según pasaban los meses, parecía cada vez más probable que esas funciones de una sola vía especiales no existían Parecía que la idea de Diffie funcionaba en teoría pero no en la práctica. No obstante, para finales de 1976, el equipo de Diffie, Hellman y Merkle había revolucionado el mundo de la criptografía. Habían convencido al resto del mundo de que existía una solución al problema de la distribución de claves, y habían creado el intercambio de claves Diffie-Hellman-Merkle, un sistema viable pero imperfecto. También habían propuesto el concepto de una cifra asimétrica, un sistema perfecto pero todavía inviable. Continuaron su investigación en la Universidad de Stanford, tratando de encontrar una función de una sola vía especial que convirtiera en realidad las cifras asimétricas. Sin embargo, no lograron descubrirla. La carrera para encontrar una cifra asimétrica la ganó otro trío de investigadores, establecido a 5.000 km de distancia, en la costa este de Estados Unidos.

3. Principales sospechosos

«Entré en la oficina de Ron Rivest», recuerda Leonard Adleman, «y Ron tenía un

artículo en la mano. Empezó a decir: “Estos tíos de Stanford realmente tienen este bla, bla, bla” Y recuerdo haber pensado: “Eso está muy bien, Ron, pero hay otra cosa de la que quiero hablarte”. Yo no conocía la historia de la criptografía, y no tenía el mínimo interés en lo que me estaba diciendo». El artículo que había excitado tanto a Ron Rivest era de Diffíe y Hellman, y describía el concepto de las cifras asimétricas. Finalmente, Rivest convenció a Adleman de que podría haber ciertas matemáticas interesantes en el problema y juntos decidieron intentar encontrar una función de una sola vía que se adaptara a los requisitos de una cifra asimétrica. Adi Shamir se les unió en la caza. Los tres eran investigadores en el octavo piso del laboratorio de Informática del MIT (Massachusetts Institute of Technology).

Rivest, Shamir y Adleman formaban un equipo perfecto. Rivest es un científico de la informática con una habilidad tremenda para absorber nuevas ideas y aplicarlas en lugares improbables. Siempre se mantuvo al tanto de los últimos artículos científicos, lo que le inspiró a dar con toda una serie de extrañas y estupendas candidatas para la función de una sola vía que constituye el núcleo de una cifra asimétrica. Sin embargo, cada una de las candidatas resultaba defectuosa de alguna forma. Shamir, otro científico de la informática, tiene un intelecto rapidísimo y la habilidad de distinguir lo accesorio y centrarse en la esencia de un problema.

Él también aportaba regularmente ideas para formular una cifra asimétrica, pero sus ideas también resultaban inevitablemente defectuosas. Adleman, un matemático con una energía, rigor y paciencia enormes, era en gran medida el responsable de detectar los fallos en las ideas de Rivest y Shamir, asegurando que no perdieran el tiempo siguiendo pistas falsas. Rivest y Shamir pasaron un año dando con nuevas ideas, y Adleman pasó un año echándolas por tierra. El trío empezó a perder la esperanza, pero no era consciente de que este proceso de fracasos continuos era una parte necesaria de su investigación, que los separaba lentamente del estéril territorio matemático y los llevaba hacia un terreno más fértil. A su debido tiempo, sus esfuerzos fueron recompensados.

En abril de 1977, Rivest, Shamir y Adleman celebraron la Pascua judía en casa de un estudiante y habían bebido una cantidad importante de vino Manischewitz antes de volver a sus respectivos hogares hacia la medianoche. Rivest, que no podía

dormir, se tumbó en su sofá a leer un libro de texto de matemáticas. Empezó a darle vueltas a la pregunta que llevaba semanas devanándole los sesos: ¿es posible construir una cifra asimétrica? ¿Es posible encontrar una función de una sola vía que sólo se pueda invertir si el receptor tiene alguna información especial? De pronto, la niebla empezó a despejarse y tuvo una revelación. Pasó el resto de esa noche formalizando su idea y, de hecho, escribiendo un artículo científico completo antes de que amaneciera. Rivest había dado un gran paso adelante, pero había sido el resultado de una colaboración de todo un año con Shamir y Adleman, y no habría sido posible sin ellos. Rivest finalizó el artículo enumerando a los autores alfabéticamente: Adleman, Rivest, Shamir.

Figura 65. Ronald Rivest, Adi Shamir y Leonard Adleman.

A la mañana siguiente, Rivest le entregó el artículo a Adleman, que realizó su habitual proceso de tratar de echarlo por tierra, pero esta vez no pudo encontrar ningún defecto. Su única crítica tenía que ver con la lista de autores. «Le dije a Ron que quitase mi nombre del artículo», recuerda Adleman. «Le dije que era su invento, no el mío. Pero Ron se negó y empezamos a discutir sobre ello. Acordamos que me iría a casa y me lo pensaría durante una noche, considerando lo que quería hacer. \blví al día siguiente y le sugerí a Ron que yo fuera el tercer autor. Recuerdo que pensé que este artículo sería el menos interesante que firmaría». Adleman no podía equivocarse más. El sistema, apodado RSA (Rivest, Shamir, Adleman) en vez de ARS, se convertiría en la cifra más influyente de la criptografía moderna.

Antes de explorar la idea de Rivest recordemos rápidamente lo que los científicos

estaban buscando para construir una cifra asimétrica:

1. Alicia debe crear una clave pública, que publicaría para que Benito (y todo el mundo) pueda usarla para codificar los mensajes dirigidos a ella. Como la clave pública es una función de una sola vía debe ser virtualmente imposible que nadie la invierta y descodifique los mensajes de Alicia.
2. Sin embargo, Alicia necesita descodificar los mensajes que le envían. Por tanto, debe tener una clave privada, una información especial, que le permita invertir el efecto de la clave pública. Por consiguiente, Alicia (y sólo Alicia) tiene el poder para descodificar cualquier mensaje dirigido a ella.

El núcleo de la cifra asimétrica de Rivest es una función de una sola vía basada en el tipo de funciones modulares descritas anteriormente en este capítulo. La función de una sola vía de Rivest se puede usar para codificar un mensaje; el mensaje, que en realidad es un número, se pone en la función, y el resultado es el texto cifrado, otro número. No describiré la función de una sola vía de Rivest en detalle (para ello véase el Apéndice G), pero explicaré uno de sus aspectos en particular, conocido simplemente como *N,* porque es *N* lo que hace que esta función de una sola vía sea reversible en ciertas circunstancias y, por tanto, que resulte ideal para ser usada como clave asimétrica.

N es importante porque es un componente flexible de la función de una sola vía, lo que significa que cada persona puede elegir su valor personal de *N,* y personalizar la función de una sola vía. Para elegir su valor personal de *N,* Alicia escoge dos números primos, p y q, y los multiplica el uno por el otro. Un número primo es un número que sólo se puede dividir por sí mismo y 1. Por ejemplo, 7 es un número primo porque no hay ningún número además de 7 y 1 que pueda dividirlo sin dejar un resto. Asimismo, 13 es un número primo porque ningún número, aparte de 13 y 1, puede dividirlo sin dejar un resto. Sin embargo, 8 no es un número primo, porque puede ser dividido por 2 y por 4.

De modo que Alicia podría decidir que sus números primos fueran p = 17.159 y q = 10.247. Multiplicando estos dos números obtenemos

$$N = 17.159 \times 10.247 = 175.828.273$$

La elección de *N* de Alicia se convierte de hecho en su clave de codificación pública y podría imprimirla en su tarjeta, anunciarla en Internet o publicarla en una guía de claves públicas junto al valor de *N* del resto de la gente. Si Benito quiere enviar un mensaje cifrado a Alicia, busca el valor de *N* de Alicia (175.828.273) y lo inserta en el formato general de la función de una sola vía, que también debería ser de dominio público.

Benito tiene ahora una función de una sola vía confeccionada con la clave pública de Alicia, de modo que podríamos llamarla la función de una sola vía de Alicia. Para codificar un mensaje para Alicia, Benito toma la función de una sola vía de Alicia, inserta el mensaje, anota el resultado y se lo envía a Alicia.

Ahora, el mensaje codificado es seguro porque nadie puede descodificarlo. El mensaje ha sido codificado con una función de una sola vía, de modo que invertir la función de una sola vía y descodificar el mensaje es, por definición, muy difícil. Sin embargo, permanece la pregunta: ¿cómo puede Alicia descodificar el mensaje?

Para leer los mensajes que le envían, Alicia debe tener una manera de invertir la función de una sola vía. Necesita tener acceso a alguna información especial que le permita descodificar el mensaje. Afortunadamente para Alicia, Rivest diseñó la función de una sola vía de modo que sea reversible para alguien que conozca los valores de p y q, los dos números primos que se multiplican el uno por el otro para obtener *N.* Aunque Alicia ha anunciado al mundo que su valor para *N* es 175.828.273, no ha revelado sus valores para p y q, de manera que sólo ella tiene la información especial necesaria para descodificar sus propios mensajes.

Podemos considerar *N* como la clave pública, la información que está disponible para todo el mundo, la información necesaria para codificar los mensajes dirigidos a Alicia. Mientras que p y q son la clave privada, disponible sólo para Alicia, la información necesaria para descodificar esos mensajes.

Los detalles exactos de cómo p y q se pueden usar para invertir la función de una sola vía se esbozan en el Apéndice G. Sin embargo, hay una cuestión que hay que tratar inmediatamente. Si todo el mundo conoce el valor de *N,* la clave pública, entonces sin duda la gente podrá deducir p y q, la clave privada, y leer los mensajes de Alicia, ¿no? Después de todo, *N* surgió de p y q. En realidad, resulta

que si A es un número lo suficientemente alto es virtualmente imposible deducir p y q a partir de *N,* y éste es posiblemente el aspecto más bello y elegante de la clave asimétrica RSA.

Alicia creó *N* eligiendo p y q y multiplicándolos. El punto fundamental es que esto constituye en sí mismo una función de una sola vía. Para demostrar la naturaleza de una sola vía de multiplicar números primos podemos tomar dos números primos, como 9.419 y 1.933, y multiplicarlos el uno por el otro. Una calculadora sólo tarda unos segundos en obtener la respuesta, 18.206.927. Sin embargo, si nos dieran el número 18.206.927 y nos pidieran que encontrásemos los factores primos (los dos números que se multiplicaron para obtener 18.206.927) nos costaría muchísimo más tiempo.

Si aún duda la dificultad de encontrar los factores primos, considere lo siguiente. Sólo me costó diez segundos generar el número 1.709.023, pero a usted y a su calculadora les costará casi una tarde entera calcular los factores primos.

Este sistema de criptografía asimétrica, conocido como RSA, se considera una forma de *criptografía de clave pública.* Para descubrir hasta qué punto RSA es seguro, podemos examinarlo desde el punto de vista de Eva y tratar de descifrar un mensaje de Alicia a Benito. Para codificar un mensaje para Benito, Alicia debe buscar la clave pública de Benito. Para crear su clave pública, Benito eligió sus propios números primos, p_B y q_B, y los multiplicó el uno por el otro para obtener N_B. Ha mantenido p_B y q_B en secreto, porque constituyen su clave de decodificación privada, pero ha anunciado N_B, que es igual a 408.508.091. Alicia inserta la clave pública de Benito (N_B) en la función de una sola vía general de codificación y luego codifica el mensaje que quiere enviarle. Cuando llega el mensaje codificado, Benito puede invertir la función y descodificarlo usando sus valores para p_B y q_B, que constituyen su clave privada. Mientras tanto, Eva ha interceptado el mensaje en ruta. Su única esperanza de descodificar el mensaje es invertir la función de una sola vía, y esto sólo es posible si conoce los valores de p_B y q_B. Benito ha mantenido p_B y q_B en secreto, pero Eva, como todo el mundo, sabe que N_B es 408.508.091. Entonces, Eva intenta deducir los valores de p_B y q_B calculando qué números serían necesarios para que, al ser multiplicados el uno por el otro, dieran 408.508.091, un proceso que se conoce como *factorizar.*

Factorizar requiere mucho tiempo, pero ¿cuánto tardaría Eva exactamente en encontrar los factores de 408.508.091? Hay varios métodos para tratar de factorizar N_B. Aunque algunos métodos son más rápidos que otros, esencialmente todos ellos conllevan probar cada número primo para ver si divide N_b sin dejar un resto. Por ejemplo, 3 es un número primo, pero no es un factor de 408.508.091, porque 3 no dividirá perfectamente 408.508.091. De modo que Eva pasa al siguiente número primo, 5. De manera similar, 5 no es un factor, por lo que Eva pasa al siguiente número primo, y así sucesivamente. Finalmente, Eva llega a 18.313, el 2.000° número primo, que efectivamente es un factor de 408.508.091.

Al haber encontrado un factor, es fácil encontrar el otro, que resulta ser 22.307. Si Eva tuviera una calculadora y pudiera probar cuatro número primos al minuto le habría costado 500 minutos, es decir, más de 8 horas, encontrar p_B y q_B. En otras palabras, Eva sería capaz de calcular la clave privada de Benito en menos de un día y, por consiguiente, podría descifrar el mensaje interceptado en menos de un día.

Esto no constituye un nivel muy alto de seguridad, pero Benito podría haber elegido números primos muchísimo más elevados y aumentar la seguridad de su clave privada. Por ejemplo, podría haber elegido números primos tan altos como 10^{65} (esto significa 1 seguido de 65 ceros, es decir, cien mil millones de millones de millones de millones de millones de millones de millones de millones de millones). Esto hubiera resultado en un valor de *N* que sería aproximadamente 10^{65} x 10^{65}, que es 10^{130} Un ordenador podría multiplicar los dos números primos y generar *N* en un solo segundo, pero si Eva quisiera invertir el proceso y calcular p_B y q_B, le costaría un tiempo desorbitadamente mayor. Cuánto exactamente depende de la velocidad del ordenador de Eva. El experto en seguridad Simson Garfinkel estimó que un ordenador Intel Pentium de 100 MHZ con 8 MB de RAM tardaría aproximadamente cincuenta años en factorizar un número tan alto como 10^{130}.

Los criptógrafos tienden a tener una vena paranoica y ponerse en el peor de los casos, como una conspiración mundial para descifrar sus cifras. Así que Garfinkel consideró lo que podría suceder si cien millones de ordenadores personales (el número vendido en 1995) se confabularan contra esa cifra. El resultado es que se podría factorizar un número tan alto como 10^{130} en unos quince segundos. Por consiguiente, se acepta ahora generalmente que para una seguridad genuina es

necesario emplear números primos aún más altos. Para transacciones bancarias importantes, *N* tiende a ser al menos 10^{308}, que es diez millones de billones más alto que 10^{130}.

Los esfuerzos combinados de cien millones de ordenadores personales tardarían más de mil años en descifrar semejante clave. Con valores de p_B y q_B suficientemente elevados, RSA es indescifrable.

El único peligro potencial para la criptografía de clave pública RSA es que en algún tiempo futuro alguien lograra encontrar una manera rápida de factorizar *N.* Es concebible que dentro de una década, o incluso mañana, alguien descubrirá un método para factorizar rápidamente, y a partir de entonces RSA ya no servirá. Sin embargo, durante dos mil años los matemáticos han intentado inútilmente encontrar un atajo y en nuestros días factorizar continúa siendo un cálculo que requiere un tiempo enorme. La mayoría de los matemáticos cree que factorizar es inherentemente una tarea difícil, y que hay alguna ley matemática que no permite ningún atajo. Si asumimos que tienen razón, entonces RSA parece seguro para el futuro previsible.

La gran ventaja de la criptografía de clave pública RSA es que elimina todos los problemas asociados con las cifras tradicionales y el intercambio de claves. Alicia ya no tiene que preocuparse sobre cómo llevar de una manera segura la clave a Benito, o de que Eva pueda interceptar la clave. De hecho, a Alicia no le importa quién vea la clave pública: cuanta más gente la vea, mejor, porque la clave pública sólo sirve para codificar, no para descodificar. Lo único que se necesita mantener en secreto es la clave privada utilizada para la descodificación, y Alicia puede tenerla consigo continuamente.

El sistema RSA fue anunciado por vez primera en agosto de 1977, cuando Martin Gardner escribió un artículo titulado «Un nuevo tipo de cifra que costaría millones de años descifrar» para su columna «Juegos matemáticos» en la revista *Scientific American.* Tras explicar cómo funciona la criptografía de clave pública, Gardner lanzó un desafío a sus lectores. Publicó un texto cifrado y proporcionó también la clave pública que se había utilizado para

N=114.331.625.757.633.867.569.235.779
976.146.612.010.218.296.721.242.362
562.361.842.935.706.935.245.733.097
030.597.123.563.958.705.058.989
075.147.599.290.026.879.543.541.

El desafío era factorizar TV en p y q, y luego usar estos números para descodificar el mensaje. El premio era de 100 dólares. Gardner no contaba con espacio suficiente para explicar los detalles prácticos del RSA, por lo que pidió a los lectores que escribieran al laboratorio de Informática del MIT, que a su vez les enviaría un memorándum técnico que se acababa de preparar. A Rivest, Shamir y Adleman les sorprendieron las tres mil peticiones que recibieron. Sin embargo, no respondieron inmediatamente, porque les preocupaba que la distribución pública de su idea pudiera poner en peligro sus posibilidades de obtener una patente. Cuando los asuntos relacionados con la patente se solucionaron finalmente, el trío dio una fiesta de celebración en la que profesores y estudiantes consumían *pizza* y cerveza a la vez que metían en sobres los memorandos técnicos para los lectores de *Scientific American.*

En cuanto al desafío de Gardner, pasarían diecisiete años antes de que se lograra romper la cifra. El 26 de abril de 1994, un equipo de seiscientos voluntarios anunció los factores de *N*

q = 3.490.529.510.847.650.949.147.849.619.903.898.133.417.764.
638.493.387.843.990.820.577

p = 32.769.132.993.266.709.549.961.988.190.834.461.413.177.
642.967.992.942.539.798.288.533.

Utilizando estos valores como clave privada, lograron descifrar el mensaje, formado por una serie de números, que, cuando se convertían en letras, decía *«the magic words are squeamish ossifrage»* («las palabras mágicas son un quebrantahuesos impresionable»). El problema de la factorización había sido dividido entre los

voluntarios, que procedían de países tan distantes como Australia, Reino Unido, Estados Unidos y Venezuela. Los voluntarios empleaban su tiempo libre en sus terminales, ordenadores centrales y superordenadores, abordando cada uno de ellos una pequeña parte del problema.

En realidad, una red de ordenadores de todo el mundo se había unido y trabajaban simultáneamente para afrontar el desafío de Gardner. Incluso teniendo en consideración el gigantesco esfuerzo paralelo, puede que a algunos lectores aún les sorprenda que RSA fuera descifrado en tan poco tiempo, pero hay que señalar que el desafío de Gardner utilizaba un valor relativamente pequeño de *N:* era sólo de alrededor de 10^{129} Hoy día, los usuarios de RSA elegirían un valor mucho más elevado para garantizar la seguridad de la información importante. Ahora es ya habitual codificar un mensaje con un valor de *N* lo suficientemente grande como para que todos los ordenadores del mundo necesitaran más tiempo que la edad del universo para romper la cifra.

4. La historia alternativa de la criptografía de clave pública

En los últimos veinte años, Diffie, Hellman y Merkle se han hecho famosos en todo el mundo como los criptógrafos que inventaron el concepto de la criptografía de clave pública, mientras que Rivest, Shamir y Adleman son reconocidos por haber desarrollado RSA, la mejor aplicación de criptografía de clave pública. Sin embargo, un anuncio reciente significa que va a haber que reescribir los libros de Historia. Según el gobierno británico, la criptografía de clave pública fue inventada originalmente en el GCHQ de Cheltenham, la institución de alto secreto que se formó con los restos de Bletchley Park después de la segunda guerra mundial. Se trata de una historia de ingenio extraordinario, héroes anónimos y un encubrimiento gubernamental que se prolongó durante décadas.

La historia comienza a finales de los años sesenta, cuando el ejército británico empezó a preocuparse por el problema de la distribución de claves. Haciendo planes para los años setenta, los oficiales militares de alto rango imaginaron una situación en la que la miniaturización de las radios y la reducción de los costes significaría que todo soldado podría estar continuamente en contacto radiofónico con su oficial. Las ventajas de la comunicación general serían enormes, pero las comunicaciones

tendrían que codificarse, y el problema de la distribución de claves sería insuperable.

En aquellos momentos, la única forma de criptografía era la simétrica, de modo que una clave individual tendría que ser transportada de manera segura a cada miembro de la red de comunicaciones. Cualquier expansión de las comunicaciones sería finalmente asfixiada por la carga de la distribución de las claves. A comienzos de 1969, el ejército pidió a James Ellis, uno de los principales criptógrafos gubernamentales del Reino Unido, que estudiase formas de afrontar el problema de la distribución de claves.

Ellis era un personaje curioso y ligeramente excéntrico. Presumía con orgullo de haber atravesado medio mundo antes siquiera de haber nacido: fue concebido en Inglaterra, pero nació en Australia. Luego, cuando aún era un bebé, volvió a Londres y creció en el East End en los años veinte. En la escuela, lo que más le interesaba era la ciencia, y luego estudió física en el Imperial College, donde Tommy Flowers había construido el Colossus, el primer ordenador de descifrамiento.

La división criptográfica de Dollis Hill fue finalmente absorbida por el GCHQ, de modo que el 1 de abril de 1965 Ellis se mudó a Cheltenham para unirse al recién formado CESG (Communications-Electronics Security Group, Grupo de seguridad de la electrónica de comunicaciones), una sección especial del GCHQ dedicada a garantizar la seguridad de las comunicaciones británicas.

Como estaba involucrado en asuntos de la seguridad nacional, Ellis prestó juramento de guardar secreto a lo largo de su carrera. Aunque su esposa y su familia sabían que trabajaba en el GCHQ, no conocían nada de sus descubrimientos y no tenían ni idea de que era uno de los creadores de códigos más distinguidos de la nación.

Figura 66. John Ellis

A pesar de su habilidad como creador de códigos, Ellis nunca fue puesto a cargo de ninguno de los grupos de investigación importantes del GCHQ. Era brillante, pero también introvertido, de reacciones imprevisibles, y no dotado naturalmente para el trabajo en equipo. Su colega Richard Walton recordó:

> *Era un trabajador con bastantes rarezas, y no encajaba realmente en los asuntos cotidianos del GCHQ. Pero en cuanto a aportar ideas nuevas era realmente excepcional. A veces tenías que ignorar algunas tonterías, pero era muy innovador y siempre estaba dispuesto a desafiar la ortodoxia. Habríamos tenido muchos problemas si todo el mundo hubiera sido como él en el GCHQ, pero podemos tolerar una proporción más elevada de semejantes personas que la mayoría de las organizaciones. Nos las arreglamos con varias personas como él.*

Una de las mayores cualidades de Ellis era la amplitud de sus conocimientos. Leía cualquier revista científica que podía obtener y nunca tiraba ninguna. Por razones de seguridad, los empleados del GCHQ debían despejar sus mesas de trabajo cada noche y meterlo todo en armarios cerrados con llave, lo que significaba que los armarios de Ellis estaban abarrotados con las publicaciones más desconocidas imaginables. Se ganó una reputación de criptogurú, y si otros investigadores se encontraban con problemas imposibles, llamaban a su puerta con la esperanza de que sus amplios conocimientos y su originalidad proporcionasen una solución. Fue probablemente a causa de esta reputación que le pidieron que examinase el problema de la distribución de claves.

El coste de la distribución de claves era ya enorme, y se convertiría en el factor limitador de cualquier expansión del cifrado. Incluso una reducción del 10 por 100 del coste de la distribución de claves reduciría considerablemente el presupuesto militar de seguridad. Sin embargo, en vez de limitarse a roer lentamente el problema, Ellis buscó inmediatamente una solución radical y completa. «Siempre afrontaba un problema preguntando: "¿Es esto lo que realmente queremos hacer?"», dice Walton. «Siendo como era, una de las primeras cosas que hizo James fue desafiar el requisito de que era necesario compartir datos secretos, es decir, la clave. No había ningún teorema que dijera que tenías que tener un secreto compartido. Esto era algo que se podía cambiar».

Ellis comenzó su ataque al problema buscando entre su tesoro de artículos científicos. Muchos años después, escribió sobre el momento en que descubrió que la distribución de claves no era una parte inevitable de la criptografía:

> *Lo que cambió este punto de vista fue el descubrimiento de un informe de tiempos de la guerra de la compañía de teléfonos Bell, en el que un autor anónimo describía una ingeniosa idea para garantizar la seguridad de las charlas telefónicas. Proponía que el receptor enmascarase lo que decía el emisor añadiendo ruido a la línea. El podría sustraer el ruido después, ya que él lo había añadido y, por tanto, sabía lo que era. Las obvias desventajas prácticas de este sistema impidieron que fuera realmente utilizado, pero tenía*

algunas características interesantes. La diferencia entre éste y el cifrado convencional es que en este caso el receptor forma parte del proceso de cifrado... Fue así como surgió la idea.

«Ruido» es el término técnico para designar cualquier señal que afecta a una comunicación. Normalmente es generado por fenómenos naturales, y su rasgo más irritante es que es enteramente aleatorio, lo que implica que es muy difícil eliminar el ruido de un mensaje. Si un sistema de radio está bien diseñado, el nivel de ruido es bajo y el mensaje es claramente audible, pero si el nivel de ruido es alto y encenaga el mensaje, no hay forma de recuperarlo. Ellis estaba sugiriendo que el receptor, Alicia, crease ruido a propósito, un ruido que pudiera medir antes de añadirlo al canal de comunicación que la conecta con Benito. Entonces, Benito podría enviar un mensaje a Alicia, y si Eva intervenía el canal de comunicaciones no podría leer el mensaje porque estaría inundado de ruido. Eva no podría separar el ruido del mensaje. La única persona que puede eliminar el ruido y leer el mensaje es Alicia, porque está en la posición única de conocer la naturaleza exacta del ruido, ya que ha sido ella misma la que lo puso ahí. Ellis se dio cuenta de que se había conseguido la seguridad sin intercambiar ninguna clave. La clave era el ruido, y sólo Alicia necesitaba saber los detalles del ruido.

En un memorándum, Ellis enumeró su proceso de pensamiento: «La siguiente pregunta era obvia. ¿Se puede hacer esto con la codificación ordinaria? ¿Podemos producir un mensaje cifrado seguro, que el receptor autorizado pueda leer sin ningún intercambio secreto previo de la clave? Esta pregunta se me ocurrió una noche en la cama, y la prueba de la posibilidad teórica sólo me llevó unos minutos. Teníamos un teorema de existencia. Lo impensable era realmente posible». (Un teorema de existencia muestra que un concepto particular es posible, pero no entra en los detalles del concepto). En otras palabras, hasta ese momento, buscar una solución al problema de la distribución de claves era como buscar una aguja en un pajar, con la posibilidad de que la aguja podría no estar allí. Sin embargo, gracias al teorema de existencia, Ellis ahora sabía que la aguja estaba allí en alguna parte.

Las ideas de Ellis eran muy similares a las de Diffie, Hellman y Merkle sólo que les llevaba varios años de ventaja. Sin embargo, nadie conocía el trabajo de Ellis

porque era un empleado del gobierno británico y, por tanto, había prestado juramento de guardar secreto. Para finales de 1969, parece ser que Ellis había llegado al mismo punto muerto al que llegaría el trío de Stanford en 1975. Se había probado a sí mismo que la criptografía de clave pública (o cifrado no secreto, como él lo llamó) era posible, y había desarrollado el concepto de claves públicas y claves privadas separadas. También sabía que necesitaba encontrar una función de dirección única especial, que pudiera invertirse si el receptor tenía acceso a una información especial. Desgraciadamente, Ellis no era matemático. Experimentó con unas pocas funciones matemáticas, pero no tardó en darse cuenta de que no podría progresar más por sí solo.

Entonces, Ellis reveló su avance a sus jefes. Sus reacciones son aún material clasificado, pero, en una entrevista, Richard Walton se mostró dispuesto a parafrasear para mí los diversos memorandos que fueron intercambiados. Sentado con su maletín en su regazo, con la tapa protegiendo los papeles de mi vista, hojeó los documentos:

> *No le puedo enseñar los papeles que tengo aquí porque todavía llevan por todas partes sellos con palabras traviesas como alto secreto.*
>
> *Esencialmente, la idea de James llega al jefe, que se la pasa a otro, como suelen hacer los jefes, para que la puedan ver los expertos. Éstos afirman que lo que dice James es totalmente cierto. En otras palabras, no pueden descartar a este hombre como un chiflado. Al mismo tiempo, no pueden imaginar ninguna manera de poner en práctica su idea. De modo que les impresiona el ingenio de James, pero no saben cómo sacarle partido.*

Durante los siguientes tres años, las mentes más brillantes del GCHQ se esforzaron por encontrar una función de una sola vía que satisficiera los requisitos de Ellis, pero no surgió nada. Entonces, en septiembre de 1973, un nuevo matemático se unió al equipo. Clifford Cocks acababa de licenciarse en la Universidad de Cambridge, donde se había especializado en teoría de los números, una de las formas más puras de las matemáticas. Cuando se unió al GCHQ sabía muy poco

sobre cifrado y el enigmático mundo de la comunicación militar y diplomática, de modo que le asignaron un mentor, Nick Patterson, que lo orientó durante sus primeras semanas en el GCHQ.

Figura 67. Clifford Cocks

Después de unas seis semanas, Patterson le habló a Cocks de «una idea realmente loca». Le esbozó la teoría de Ellis para una criptografía de clave pública y le explicó que todavía nadie había logrado encontrar una función matemática que sirviera. Patterson se lo estaba contando a Cocks porque era la idea criptográfica más excitante que andaba rondando, no porque esperase que intentara resolverla. Sin embargo, como explica Cocks, ese mismo día se puso a trabajar: «*No pasaba nada en particular, así que me puse a pensar en la idea. Como había estado trabajando en teoría de los números, era natural que pensara en funciones de una sola vía, algo que se puede hacer pero no deshacer. Los números primos y la factorización*

eran un candidato natural, y se convirtieron en mi punto de partida». Cocks estaba empezando a formular lo que después se conocería como la clave asimétrica RSA. Rivest, Shamir y Adleman descubrieron su fórmula para la criptografía de clave pública en 1977, pero cuatro años antes el joven licenciado de Cambridge atravesaba exactamente los mismos procesos de pensamiento. Cocks recuerda: «*De principio a fin, no me llevó más de media hora. Estaba muy satisfecho de mí mismo. Pensé: "Oh, qué bien. Me han dado un problema y lo he resuelto"*».

Cocks no apreció completamente la trascendencia de su descubrimiento. No era consciente de que las mentes más brillantes del GCHQ habían estado luchando con el problema durante tres años, y no tenía ni idea de que había hecho uno de los avances criptográficos más importantes del siglo. Puede que la ingenuidad de Cocks fuera parte de la razón de su éxito, permitiéndole atacar el problema con confianza, en vez de tantearlo tímidamente. Cocks le contó a su mentor su descubrimiento, y fue Patterson quien informó a la dirección. Cocks tenía poca confianza en sí mismo y era aún muy novato, mientras que Patterson comprendía perfectamente el contexto del problema y era más capaz de tratar las cuestiones técnicas que surgirían inevitablemente. Muy pronto, gente que no lo conocía de nada empezó a acercarse a Cocks, el chico prodigio, y a felicitarlo. Uno de esos extraños era James Ellis, ansioso por conocer al hombre que había convertido su sueño en realidad. Como Cocks aún no comprendía la enormidad de su logro, los detalles de este encuentro no le causaron una gran impresión, de modo que ahora, más de dos décadas después, no recuerda la reacción de Ellis.

Cuando Cocks se dio cuenta finalmente de lo que había hecho, se le ocurrió que su descubrimiento podría haber decepcionado a G. H. Hardy, uno de los grandes matemáticos ingleses de la primera parte del siglo. En su obra *La apología del matemático*, escrita en 1940, Hardy había afirmado orgullosamente: «La matemática real no tiene efectos en la guerra. Nadie ha descubierto aún ningún propósito belicoso al que pueda servir la teoría de los números». Matemática real significa matemática pura, como la teoría de los números que constituía el fundamento del trabajo de Cocks. Éste demostró que Hardy se equivocaba. La complejidad de la teoría de los números se puede usar ahora para ayudar a los generales a planear sus batallas en completo secreto. Como su trabajo tenía

implicaciones para las comunicaciones militares, Cocks, como Ellis, tenía prohibido hablar a nadie externo al GCHQ de lo que había hecho. Trabajar en una organización gubernamental de alto secreto significaba que no podía decírselo ni a sus padres ni a sus antiguos colegas de la Universidad de Cambridge. La única persona a la que podía decírselo era a su esposa, Gilí, porque ella también trabajaba en el GCHQ.

Aunque la idea de Cocks era uno de los secretos más fuertes del GCHQ, tenía el problema de anticiparse a su tiempo. Cocks había descubierto una función matemática que permitía la criptografía de clave pública, pero quedaba aún la dificultad de poner en práctica el sistema. El cifrado mediante la criptografía de clave pública requiere mucha más potencia informática que el cifrado mediante una cifra simétrica como DES. A principios de los años setenta, los ordenadores eran todavía relativamente primitivos e incapaces de llevar a cabo el proceso de cifrado de clave pública en un período de tiempo razonable. Por eso, el GCHQ no estaba en posición de sacar partido a la criptografía de clave pública. Cocks y Ellis habían demostrado que lo aparentemente imposible era posible, pero nadie pudo encontrar una manera de hacer que lo posible fuera práctico.

Al año siguiente, 1974, Clifford Cocks explicó su trabajo en criptografía de clave pública a Malcolm Williamson, que acababa de incorporarse al GCHQ como criptógrafo. Daba la casualidad que eran viejos amigos. Ambos habían ido al instituto de enseñanza secundaria de Manchester, cuyo lema es *Sapere aude*, «Atrévete a ser sabio». En 1968, cuando aún estudiaban en el instituto, los dos muchachos habían representado al Reino Unido en la Olimpiada Matemática, celebrada en la Unión Soviética. Tras estudiar juntos en la Universidad de Cambridge, fueron cada uno por su lado durante un par de años, pero ahora estaban reunidos en el GCHQ. Habían estado intercambiando ideas matemáticas desde que tenían once años, pero la revelación de Cocks de la criptografía de clave pública era la idea más sorprendente que Williamson había oído en su vida. «Cliff me explicó su idea», recuerda Williamson, «y la verdad es que no me lo creí. Desconfiaba, porque se trata de algo muy peculiar para poder hacerse».

Williamson se fue y comenzó a tratar de probar que Cocks había cometido un error y que la criptografía de clave pública no existía realmente. Sondeó las matemáticas,

buscando un fallo subyacente. La criptografía de clave pública parecía algo demasiado bueno para ser verdad, y Williamson estaba tan decidido a encontrar un error que se llevó el problema a casa. Los empleados del GCHQ no deben llevarse trabajo a casa, porque todo lo que hacen es clasificado y el ámbito hogareño es potencialmente vulnerable al espionaje.

Figura 68. Malcolm Williamson

Sin embargo, Williamson no podía sacarse el problema de la cabeza, por lo que no podía dejar de pensar en ello. Desobedeciendo órdenes, se llevó su trabajo a casa. Pasó cinco horas tratando de encontrar un fallo. «Esencialmente, fracasé», dice Williamson. «En vez de ello, di con otra solución al problema de la distribución de claves». Williamson estaba descubriendo el intercambio de clave Diffie-Hellman-Merkle, más o menos al mismo tiempo que lo descubrió Martin Hellman. La reacción inicial de Williamson reflejaba su propensión al cinismo: «Esto tiene muy buena pinta», me dije a mí mismo. «Me pregunto si puedo encontrar un fallo es esto. Me imagino que ese día estaba de un humor negativo».

En 1975 James Ellis, Clifford Cocks y Malcolm Williamson habían descubierto todos los aspectos fundamentales de la criptografía de clave pública, pero tenían que

permanecer en silencio. Los tres británicos tuvieron que sentarse y mirar cómo sus descubrimientos eran reinventados por Dififie, Hellman, Merkle, Rivest, Shamir y Adleman durante los tres años siguientes. Curiosamente, el GCHQ descubrió RSA antes que el intercambio de claves Diffie-Hellman-Merkle, mientras que el mundo exterior, el intercambio de claves Diffie-Hellman-Merkle llegó antes. La prensa científica informó de los avances de Stanford y el MIT, y los investigadores que no tenía prohibido publicar su trabajo en las revistas científicas se hicieron famosos en la comunidad de criptógrafos. Una ojeada rápida en Internet con un servicio de búsqueda encuentra 15 páginas web que mencionan a Clifford Cocks, frente a 1.382 páginas que mencionan a Whitfield Diffie. La actitud de Cocks es admirablemente comedida: «Uno no se mete en estos asuntos buscando el reconocimiento público». Williamson es igualmente desapasionado: «Mi reacción fue “Muy bien, así son las cosas”. Básicamente, seguí viviendo mi vida».

Figura 69. Malcolm Williamson (el segundo por la izquierda) y Clifford Cocks (en el extremo derecho) llegando a la Olimpiada Matemática de 1968.

Lo único que le duele a Williamson es que el GCHQ no patentara la criptografía de clave pública. Cuando Cocks y Williamson realizaron sus descubrimientos existía un acuerdo entre los directivos del GCHQ de que patentar era imposible por dos razones. En primer lugar, patentar significaría tener que revelar los detalles de su trabajo, lo que sería incompatible con los objetivos del GCHQ. En segundo lugar, a principios de los años setenta, no estaba nada claro que los algoritmos matemáticos se pudiesen patentar. Sin embargo, cuando Diffie y Hellman trataron de obtener

una patente en 1976 resultó evidente que sí se podían patentar. En esos momentos, Williamson se mostró deseoso de hacer público su descubrimiento y bloquear la solicitud de Diffie y Hellman, pero su propuesta fue rechazada por los directivos, que no tenían la suficiente visión de futuro para prever la revolución digital y el potencial de la criptografía de clave pública. A comienzos de los años ochenta, los jefes de Williamson empezaron a arrepentirse de la decisión que habían tomado, cuando los avances de la informática y la embrionaria Internet evidenciaron que tanto RSA como el intercambio de claves Diffie- Hellman-Merkle serían productos comerciales de enorme éxito. En 1996, RSA Data Security, Inc., la compañía responsable de los productos RSA, se vendió por 200 millones de dólares.

Aunque el trabajo del GCHQ todavía estaba clasificado había otra organización que era consciente de los avances que se habían logrado en el Reino Unido. A principios de los años ochenta, la NSA norteamericana conocía la existencia del trabajo de Ellis, Cocks y Williamson, y probablemente fue a través de la NSA como Whitfield Diffie oyó un rumor sobre los descubrimientos británicos. En septiembre de 1982 Diffie decidió ver si había algo de verdad en el rumor y viajó con su esposa a Cheltenham para hablar con James Ellis cara a cara. Se reunieron en un *pub* local, y rápidamente Mary quedó sorprendida por el notable carácter de Ellis:

> *Nos sentamos a hablar, y de pronto me di cuenta de que ésta era la persona más maravillosa que uno pudiera imaginar. La amplitud de sus conocimientos matemáticos no es algo de lo que yo pueda hablar con seguridad, pero sí puedo decir que era un verdadero caballero, inmensamente modesto, una persona con una gran generosidad de espíritu y finura. Al decir finura no quiero decir anticuado y mohoso. Este hombre era un chevalier. Era un buen hombre, un hombre realmente bueno. Era un espíritu dulce.*

Diffie y Ellis hablaron de temas diversos, desde la arqueología a cómo las ratas en el tonel mejoran el sabor de la sidra, pero cada vez que la conversación se acercaba a la criptografía, Ellis cambiaba con cuidado de tema. Al final de la visita de Diffie, cuando ya estaba apunto de subir al coche e irse, ya no pudo resistir más y le preguntó directamente a Ellis acerca de lo que realmente tenía en mente: «¿Me

puede decir cómo inventó la criptografía de clave pública?». Hubo una larga pausa. Ellis susurró finalmente: «Bueno, no sé cuánto debería decirle. Digamos simplemente que ustedes le sacaron mucho más partido que nosotros».

Aunque el GCHQ fue el primero que descubrió la criptografía de clave pública, esto no debería mermar los logros de los académicos que la redescubrieron. Fueron los académicos los que primero se dieron cuenta del potencial del cifrado de clave pública, y fueron ellos los que impulsaron su puesta en práctica. Además, es bastante posible que el GCHQ nunca hubiera revelado su trabajo, bloqueando así una forma de cifrado que permitiría que la revolución digital alcanzase todo su potencial. Finalmente, el descubrimiento de los académicos se realizó de manera totalmente independiente del descubrimiento del GCHQ y tiene el mismo valor intelectual. El ámbito académico está totalmente separado del dominio de alto secreto de la investigación clasificada, y los académicos no tienen acceso a los medios y a los conocimientos secretos que se pueden ocultar en el mundo clasificado. En cambio, los investigadores gubernamentales siempre tienen acceso a las publicaciones académicas. Se podría considerar este flujo de información en términos de una función de una sola vía —la información fluye libremente en una dirección, pero está prohibido enviar información en dirección contraria.

Cuando Diffie le habló a Hellman de Ellis, Cocks y Williamson, su actitud fue que los descubrimientos de los académicos deberían ser una nota a pie de página en la historia de la investigación clasificada, y que los descubrimientos del GCHQ deberían ser una nota a pie de página en la historia de la investigación académica. Sin embargo, en aquellos momentos nadie excepto el GCHQ, la NSA, Diffie y Hellman sabía acerca de la investigación clasificada, de modo que ni siquiera se podía considerar como una nota a pie de página.

A mediados de los años ochenta, el ambiente en el GCHQ estaba cambiando y la directiva se planteó anunciar públicamente el trabajo de Ellis, Cocks y Williamson. Las matemáticas de la criptografía de clave pública estaban ya muy establecidas en el dominio público y no parecía haber ninguna razón para seguir guardando secreto. De hecho, produciría marcados beneficios si los británicos revelaban su trabajo de pioneros en la criptografía de clave pública. Como recuerda Richard Walton:

Jugamos con la idea de confesarlo todo en 1984. Empezamos a ver

las ventajas de que el GCHQ fuera más reconocido públicamente. Era una época en la que el mercado de la seguridad gubernamental estaba expandiéndose más allá de los tradicionales clientes militares y diplomáticos, y necesitábamos ganar la confianza de los que tradicionalmente no trataban con nosotros. Estábamos en pleno thatcherismo, tratando de contrarrestar un ambiente general de «el gobierno es malo, lo privado es bueno». Así que teníamos la intención de publicar un artículo, pero la idea fue frustrada por ese tío, Peter Wright, que escribió Spycatcher («Cazador de espías»). Estábamos convenciendo a los directivos para que aprobasen la publicación de este artículo, cuando se produjo todo ese alboroto en torno a Spycatcher. Entonces la orden del día fue pasar lo más desapercibidos posible.

Peter Wright era un oficial retirado de la Inteligencia británica, y la publicación de *Spycatcher*, sus memorias, fue sumamente embarazosa para el gobierno británico. Tendrían que pasar otros trece años antes de que el GCHQ finalmente hiciera pública la información, veintiocho años después del avance inicial de Ellis. En 1997, Clifford Cocks completó un importante trabajo no clasificado sobre RSA, que sería de interés para la comunidad general y que no constituiría un riesgo de seguridad si se publicaba. Como resultado, le pidieron que presentara una ponencia en el Instituto de Matemáticas y su Congreso sobre Aplicaciones que se iba a celebrar en Cirencester. La sala estaría llena de expertos en criptografía. Un puñado de ellos sabría que Cocks, que estaría hablando sólo de un aspecto de RSA, era en realidad su no celebrado inventor. Existía el riesgo de que alguien pudiera formular una pregunta embarazosa, como: «¿Inventó usted RSA?». Si surgía semejante pregunta, ¿qué se suponía que debía hacer Cocks? Según la política del GCHQ, tendría que negar su papel en el desarrollo del RSA, viéndose obligado a mentir sobre un tema que era totalmente inocuo. La situación era obviamente ridicula, y el GCHQ decidió que había llegado el momento de cambiar su política. Dieron permiso a Cocks para que comenzara su charla ofreciendo una breve historia de la contribución del GCHQ a la criptografía de clave pública.

El 18 de diciembre de 1977 Cocks pronunció su charla. Después de casi tres décadas de secreto, Ellis, Cocks y Williamson recibieron el reconocimiento que merecían.

Lamentablemente, James Ellis acababa de morir hacía sólo un mes, el 25 de noviembre de 1997, a la edad de setenta y tres años. Ellis se unió a la lista de expertos en cifras británicos cuya contribución nunca llegaría a ser reconocida mientras vivían. El desciframiento de Babbage de la cifra Vigenére nunca fue revelado mientras vivía, porque su trabajo era inestimable para las fuerzas británicas en Crimea. En vez de ello, el crédito recayó sobre Friedrich Kasiski. De manera similar, la contribución de Alan Turing al esfuerzo de la guerra fue incomparable y, sin embargo, el gobierno exigió que su trabajo sobre la Enigma no fuera revelado.

En 1987, Ellis escribió un documento clasificado que registraba su contribución a la criptografía de clave pública, que incluía sus pensamientos sobre el secreto que a menudo rodea el trabajo criptográfico:

> *La criptografía es una ciencia sumamente excepcional. La mayoría de los científicos profesionales aspiran a ser los primeros en publicar su trabajo, porque ese trabajo realiza su valor mediante la diseminación. En cambio, el valor más pleno de la criptografía se realiza minimizando la información disponible para los adversarios potenciales. Por eso, los criptógrafos profesionales trabajan normalmente en comunidades cerradas para proveer suficiente interacción profesional para asegurar la calidad a la vez que se mantiene el secreto frente a los extraños. Normalmente, la revelación de estos secretos sólo se autoriza en beneficio de la exactitud histórica después de que se ha demostrado que ya no se puede obtener ninguna ventaja manteniendo el secreto.*

Capítulo 7
Pretty Good Privacy

Contenido:

1. Codificación para las masas... ¿O no?

2. La rehabilitación de Zimmermann

Tal como predijo Whit Diffie a principios de los años setenta, estamos entrando ahora en la Era de la Información, una era posindustrial en la que la información es la mercancía más valiosa. El intercambio de información digital se ha convertido en una parte fundamental de nuestra sociedad. Decenas de millones de *e-mails* se envían ya cada día, y el correo electrónico no tardará en ser más popular que el correo convencional.

Internet, aún en pañales, ha proporcionado la infraestructura para el mercado digital y se estima que cada día la mitad del producto interno bruto del mundo viaja a través de la red SWIFT (Society of Worldwide International Financial Telecomunication, Sociedad de telecomunicación financiera internacional a escala mundial). En el futuro, las democracias que estén a favor de los referendos comenzarán a tener votaciones por la red, y los gobiernos usarán Internet en la administración de sus países, ofreciendo facilidades como por ejemplo la declaración de la renta por la red.

Sin embargo, el éxito de la Era de la Información depende de la habilidad para proteger la información cuando ésta fluye por todo el mundo, y esto depende del poder de la criptografía. Se puede considerar que el cifrado proporciona los candados y las llaves de la Era de la Información. Durante dos mil años, el cifrado ha sido importante sólo para los gobiernos y el ejército, pero hoy día tiene un papel que desempeñar en la facilitación de los negocios, y el día de mañana la gente corriente dependerá de la criptografía para proteger su privacidad. Afortunadamente, justo cuando comienza la Era de la Información, tenemos acceso a formas de cifrado extraordinariamente potentes.

El desarrollo de la criptografía de clave pública, especialmente la cifra RSA, ha proporcionado a los criptógrafos de nuestros días una clara ventaja en su continua

lucha de poder contra los criptoanalistas. Si el valor de N es lo suficientemente alto, encontrar p y q le lleva a Eva un tiempo desmedido y, por tanto, el cifrado RSA es de hecho indescifrable. Lo más importante es que la criptografía de clave pública no está debilitada por ningún problema de distribución de claves. En resumen, RSA garantiza cerrojos casi irrompibles para nuestras piezas de información más valiosas.

Sin embargo, como sucede con toda tecnología, la codificación tiene también un lado oscuro. Además de proteger las comunicaciones de los ciudadanos respetuosos de la ley, la codificación protege también las comunicaciones de criminales y terroristas.

Figura 70. Phil Zimmermann

Actualmente, uno de los medios de la policía para recoger pruebas en casos muy serios, como el crimen organizado y el terrorismo, es intervenir ciertas líneas

telefónicas, pero esto no sería posible si los criminales utilizaran cifras indescifrables. Según entramos en el siglo XXI, el dilema fundamental de la criptografía es encontrar una forma de permitir que el público y las empresas usen el cifrado para sacar partido a las ventajas de la Era de la Información sin permitir que los criminales abusen de la codificación y eludan a la justicia.

Existe actualmente un activo y vigoroso debate acerca del mejor camino a seguir, y gran parte de la discusión ha sido inspirada por la historia de Phil Zimmermann, un hombre cuyas tentativas de alentar el uso generalizado de una codificación potente han causado el pánico de los expertos en seguridad norteamericanos, han amenazado la eficacia de la billonaria NSA y han hecho que el FBI abriera una investigación sobre su persona y que tuviera que aparecer ante un jurado de acusación.

Phil Zimmermann pasó la mitad de los años setenta en la Universidad Atlantic de Florida, donde estudió física y luego informática. Al graduarse, todo parecía indicar que tendría una carrera estable en la industria informática que crecía tan rápidamente, pero los sucesos políticos de principios de los años ochenta transformaron su vida y se mostró menos interesado en la tecnología de los chips de silicona y más preocupado por la amenaza de una guerra nuclear. Se sintió alarmado por la invasión soviética de Afganistán, la elección de Ronald Reagan, la inestabilidad causada por el envejecido Breznev y la creciente tensión de la guerra fría. Incluso llegó a considerar trasladarse a Nueva Zelanda con toda su familia, porque creía que ése sería uno de los pocos lugares de la Tierra que sería habitable tras un conflicto nuclear.

Pero justo cuando había obtenido los pasaportes y los papeles necesarios para la inmigración acudió con su esposa a una reunión convocada por la Campaña por el Bloqueo de las Armas Nucleares. En vez de escapar, los Zimmermann decidieron quedarse y luchar la batalla en su propio país, convirtiéndose en activistas antinucleares de primera línea. Educaron a los candidatos políticos sobre temas de política militar y fueron detenidos en los terrenos de las pruebas nucleares de Nevada, junto a Cari Sagan y otros cuatrocientos manifestantes.

Unos pocos años después, en 1988, Mijaíl Gorbachov se convirtió en jefe de Estado de la Unión Soviética, anunciando *perestroika, glasnost* y una reducción de la

tensión entre el Este y el Oeste. Los miedos de Zimmermann empezaron a calmarse, pero no perdió su pasión por el activismo político, simplemente la canalizó en una dirección diferente. Comenzó a centrar su atención en la revolución digital y la necesidad de codificación:

> *La criptografía solía ser una ciencia oscura, de poca relevancia para la vida cotidiana. Históricamente, tuvo siempre un papel especial en las comunicaciones militares y diplomáticas. Pero en la Era de la Información, la criptografía tiene que ver con el poder político, y en particular con las relaciones de poder entre un gobierno y su gente. Tiene que ver con el derecho a la privacidad, la libertad de expresión, la libertad de asociación política, la libertad de prensa, la libertad contra el registro y la confiscación irrazonables, la libertad de que te dejen en paz.*

Estos puntos de vista podrían parecer paranoicos, pero, según Zimmermann, existe una diferencia fundamental entre la comunicación tradicional y la digital, una diferencia que tiene implicaciones importantes para la seguridad:

> *En el pasado, si el gobierno quería violar la privacidad de los ciudadanos corrientes tenía que dedicar una cierta cantidad de esfuerzo para interceptar, abrir al vapor y leer el correo de papel, o escuchar y posiblemente transcribir conversaciones telefónicas. Esto es similar a capturar pescado con un anzuelo y una caña, un pez cada vez. Afortunadamente para la libertad y la democracia, este tipo de vigilancia que requiere tanto esfuerzo no es práctico a gran escala. Hoy día, el correo electrónico está reemplazando gradualmente al correo convencional de papel y pronto será la norma para todos, no la novedad que es hoy. A diferencia del correo de papel, los mensajes de* e- mail *son facilísimos de interceptar y escudriñar buscando palabras clave interesantes. Esto se puede llevar a cabo de manera fácil, rutinaria, automática e indetectable a gran escala. Es similar a la pesca con red de arrastre, lo que constituye una diferencia orwelliana cuantitativa y cualitativa para la*

salud de la democracia.

La diferencia entre el correo ordinario y el digital se puede ilustrar imaginando que Alicia quiere enviar invitaciones para su fiesta de cumpleaños, y que Eva, que no ha sido invitada, quiere saber la hora y el lugar de la fiesta. Si Alicia usa el método tradicional de enviar cartas por correo es muy difícil que Eva intercepte una de las invitaciones. Para empezar, Eva no sabe dónde entraron las invitaciones de Alicia en el sistema postal, porque Alicia pudo usar cualquier buzón de la ciudad. Su única esperanza de interceptar una de las invitaciones es conseguir de alguna forma la dirección de uno de los amigos de Alicia e infiltrarse en la oficina de reparto local. Luego tiene que revisar manualmente todas y cada una de las cartas. Si se las arregla para encontrar una carta enviada por Alicia tendrá que abrirla al vapor para obtener la información que desea y luego volverla a su estado original para evitar cualquier sospecha de manipulación.

En cambio, la tarea de Eva se vuelve mucho más fácil si Alicia envía sus invitaciones por *e-mail.* Cuando los mensajes salen del ordenador de Alicia van a un servidor local, un punto de entrada principal en Internet; si Eva es lo suficientemente lista puede piratear su entrada en ese servidor local sin salir de su casa. Las invitaciones llevarán la dirección de *e-mail* de Alicia y resultaría sumamente fácil establecer un filtro electrónico para encontrar los *e- mails* que contengan la dirección de Alicia. Una vez que se ha encontrado una invitación, no hay que abrir ningún sobre, de modo que no hay ningún problema para leerla. Además, la invitación se puede volver a poner en camino sin que muestre ningún signo de que ha sido interceptada. Alicia no sería consciente de lo que pasaba. Sin embargo, existe una forma de impedir que Eva lea los *e-mails* de Alicia, a saber, la codificación.

Más de cien millones de *e-mails* se envían por todo el mundo cada día, y todos ellos son vulnerables a la interceptación. La tecnología digital ha ayudado a la comunicación, pero también ha aumentado la posibilidad de que estas comunicaciones sean observadas. Según Zimmermann, los criptógrafos tienen la obligación de alentar el uso del cifrado, para así proteger la privacidad del individuo:

Un gobierno futuro podría heredar una infraestructura tecnológica optimada para la vigilancia, con la que pueden observar los

> *movimientos de su oposición política, cada transacción financiera, cada comunicación, cada bit de* e-mail*, cada llamada telefónica. Todo podría ser filtrado y escudriñado y reconocido automáticamente con la tecnología de reconocimiento de la voz y transcrito. Es hora de que la criptografía abandone las sombras de los espías y el ejército, y salga al sol y se deje abrazar por el resto de nosotros.*

En teoría, cuando se inventó el RSA en 1977, ofreció un antídoto a la posibilidad del Gran Hermano[23] porque los individuos podían crear sus propias claves públicas y privadas, y enviar y recibir mensajes perfectamente seguros. Sin embargo, en la práctica existía un gran problema, porque el proceso real de cifrado RSA requería una cantidad sustancial de poder informático comparado con las formas simétricas de codificación como el DES. Por consiguiente, en los años ochenta sólo el gobierno, el ejército y las grandes empresas tenían ordenadores lo suficientemente potentes para utilizar RSA. No es de extrañar, por tanto, que RSA Data Security, Inc., la compañía montada para comercializar el RSA, desarrollase sus productos de codificación teniendo en mente tan sólo estos mercados.

En cambio, Zimmermann creía que todo el mundo merecía el derecho a la privacidad que ofrecía la codificación RSA, y canalizó su entusiasmo político al desarrollo de un producto de codificación RSA para las masas. Intentó hacer uso de sus estudios de informática para diseñar un producto económico y eficaz, que no sobrecargara la capacidad de un ordenador personal corriente. También quería que su versión del RSA poseyera un interfaz particularmente acogedor, para que el usuario no tuviera que ser un experto en criptografía para manejarlo. Llamó a su producto *Pretty Good Privacy,* o PGP para abreviar[24]. El nombre se inspiró en *Ralph 's Pretty Good Groceries* («Comestibles bastante buenos de Ralph»), uno de los patrocinadores de *Prairie Home Companion* («Guía casera de la llanura»), de Garrison Keillor, uno de los programas radiofónicos favoritos de Zimmermann.

Durante la última parte de los años ochenta, trabajando en su casa de Boulder,

[23] «Gran Hermano» (Big Brother): nombre del jefe de Estado en la novela de George Orwell 1984. (N. del T.)
[24] La traducción al castellano sería «Privacidad (o intimidad) bastante buena», pero su nombre original en inglés, así como el acrónimo PGP, se han impuesto en el uso generalizado. (N. del T.)

Colorado, Zimmermann fue construyendo su paquete informático de codificación. Su objetivo principal era acelerar la codificación RSA. Normalmente, si Alicia quiere usar RSA para codificar un mensaje para Benito busca la clave pública de éste y luego aplica al mensaje la función de una sola vía RSA. A la inversa, Benito descodifica el texto cifrado usando su clave privada para invertir la función de una sola vía RSA. Ambos procesos requieren una considerable manipulación matemática, de modo que, si el mensaje es largo, la codificación y la descodificación pueden llevar varios minutos en un ordenador personal.

Si Alicia envía cien mensajes al día no puede permitirse pasar varios minutos codificando cada uno de ellos. Para acelerar la codificación y la descodificación, Zimmermann empleó un ingenioso truco que utilizaba la codificación asimétrica RSA junto a la anticuada codificación simétrica. La codificación simétrica tradicional puede ser igual de segura que la codificación asimétrica y es mucho más rápida de realizar, pero la codificación simétrica tiene el problema de tener que distribuir la clave, que ha de ser transportada de manera segura del emisor al receptor. Es ahí donde el RSA viene a socorrerla, porque el RSA se puede utilizar para codificar la clave simétrica.

Zimmermann imaginó la siguiente situación. Si Alicia quiere enviar un mensaje cifrado a Benito empieza por codificarlo con una cifra simétrica. Zimmermann sugirió utilizar una cifra conocida como IDEA, que es similar a DES. Para codificar con IDEA, Alicia necesita elegir una clave, pero para que Benito descifre el mensaje, Alicia necesita pasar de alguna forma la clave a Benito. Alicia supera este problema buscando la clave pública RSA de Benito y luego la usa para codificar la clave IDEA. De esta forma, Alicia termina enviando dos cosas a Benito: el mensaje codificado con la cifra simétrica IDEA, y la clave IDEA codificada con la cifra asimétrica RSA. Al otro lado, Benito utiliza su clave privada RSA para descifrar la clave IDEA y luego usa la clave IDEA para descifrar el mensaje. Esto podría parecer enrevesado, pero la ventaja es que el mensaje, que puede que contenga una gran cantidad de información, se está codificando con una rápida cifra simétrica, y sólo la clave simétrica IDEA, que consiste en una cantidad relativamente pequeña de información, se codifica con una lenta cifra asimétrica. Zimmermann planeó tener esta combinación de RSA e IDEA dentro del producto PGP, pero disponer de un

interfaz fácil de manejar significaría que el usuario no tendría que inmiscuirse en las complicadas operaciones que se están realizando.

Tras haber solucionado el problema de la velocidad, Zimmermann incorporó también una serie de funciones prácticas en PGP. Por ejemplo, antes de utilizar el componente RSA del PGP, Alicia necesita generar sus propias claves, la privada y la pública. Generar claves no es algo trivial, porque requiere encontrar un par de números primos gigantes. Sin embargo, Alicia sólo tiene que mover su ratón de manera irregular, y el programa PGP creará una clave privada y otra pública para ella: los movimientos del ratón introducen un factor aleatorio que PGP utiliza para asegurar que todo usuario tenga sus propias claves privada y pública únicas. Después, lo único que tiene que hacer Alicia es dar a conocer su clave pública.

Otro aspecto práctico de PGP es su función para firmar digitalmente un *e- mail.* Normalmente, el correo electrónico no lleva firma, lo que significa que es imposible verificar el autor verdadero de un *e-mail.* Por ejemplo, si Alicia utiliza el correo electrónico para enviar una carta de amor a Benito, normalmente la codifica con la clave pública de éste, y cuando él la recibe la descodifica con su propia clave privada. Al principio, Benito se siente halagado, pero ¿cómo puede estar seguro de que la carta de amor es realmente de Alicia? Quizá la malévola Eva escribió el *e-mail* y tecleó el nombre de Alicia al final. Sin la garantía de una firma escrita a mano con tinta no hay ninguna forma obvia de verificar quién lo ha escrito. De manera alternativa, podemos imaginar que un banco recibe un *e-mail* de un cliente, dando instrucciones para que todos los fondos del cliente se transfieran a una cuenta bancaria de número privado en las islas Caimán. De nuevo, sin una firma escrita a mano, ¿cómo sabe el banco que el *e-mail* procede realmente del cliente? El *e-mail* podría haber sido escrito por un criminal que trata de transferir el dinero a su propia cuenta bancaria de las islas Caimán. Para crear la confianza en Internet, es esencial que haya alguna forma de firma digital fiable.

La firma digital de PGP se basa en un principio que fue desarrollado por vez primera por Whitfield Diffie y Martin Hellman. Cuando propusieron la idea de las claves públicas y claves privadas separadas se dieron cuenta de que, además de resolver el problema de la distribución de claves, su invento proporcionaría también un mecanismo natural para generar firmas para el *e- mail.* En el Capítulo 6 vimos que

la clave pública es para codificar y la clave privada para descodificar. En realidad, el proceso se puede invertir, de modo que la clave privada se use para codificar y la clave pública para descodificar. Este modo de cifrado se ignora normalmente porque no ofrece seguridad. Si Alicia utiliza su clave privada para codificar un mensaje para Benito, entonces todo el mundo puede descodificarlo, porque todo el mundo tiene la clave pública de Alicia. Sin embargo, este modo de operación sirve para verificar quién ha escrito un mensaje, porque si Benito puede descodificar un mensaje usando la clave pública de Alicia, entonces tiene que haber sido codificado utilizando su clave privada; sólo Alicia tiene acceso a su clave privada, de modo que el mensaje debe haber sido enviado por Alicia.

En efecto, si Alicia quiere enviar una carta de amor a Benito tiene dos opciones. O bien codifica el mensaje con la clave pública de Benito para garantizar la privacidad, o bien lo codifica con su propia clave privada para garantizar que ha sido ella quien lo ha escrito. Sin embargo, si combina ambas opciones puede garantizar la privacidad y también que ha sido ella quien lo ha escrito. Hay maneras más rápidas de lograr esto, pero ésta es una forma en la que Alicia podría enviar su carta de amor. Comienza codificando el mensaje utilizando su clave privada y luego codifica el texto cifrado resultante usando la clave pública de Benito. Podemos imaginar que el mensaje está rodeado por un frágil caparazón interno, que representa la codificación con la clave privada de Alicia, y un fuerte caparazón externo, que representa la codificación con la clave pública de Benito. El texto cifrado resultante sólo puede ser descifrado por Benito, porque sólo él tiene acceso a su clave privada, que es necesaria para romper el fuerte caparazón externo. Después de haber descifrado el caparazón externo, Benito puede descifrar fácilmente el caparazón interno usando la clave pública de Alicia: el caparazón interno no se propone proteger el mensaje, sino que verifica que el mensaje provino de Alicia, y no de un impostor.

Para entonces, enviar un mensaje codificado con PGP se está volviendo muy complicado. La cifra IDEA se está usando para codificar el mensaje, RSA se está utilizando para codificar la clave IDEA y hay que incorporar otra fase de codificación si se necesita una firma digital. Sin embargo, Zimmermann desarrolló su producto de tal manera que lo haría todo automáticamente, de modo que Alicia y Benito no

tendrían que preocuparse por los procesos matemáticos. Para enviar un mensaje a Benito, Alicia simplemente escribe su *email* y selecciona la opción PGP de un menú en la pantalla de su ordenador. A continuación teclea el nombre de Benito, y PGP encuentra la clave pública de Benito y realiza automáticamente toda la codificación. Al mismo tiempo, PGP lleva a cabo todas las maniobras necesarias que se requieren para firmar digitalmente el mensaje. Al recibir el mensaje codificado, Benito selecciona la opción PGP, y PGP descifra el mensaje y verifica el autor. No había nada original en PGP —Diffie y Hellman ya habían pensado en las firmas digitales y otros criptógrafos habían usado una combinación de cifras simétricas y asimétricas para acelerar la codificación— pero Zimmermann fue el primero que lo puso todo junto en un producto de cifrado de fácil manejo, que era lo suficientemente eficiente para funcionar en un ordenador personal moderadamente potente.

Durante el verano de 1991, Zimmermann estaba a punto de convertir PGP en un producto listo para ser usado. Sólo quedaban dos problemas, ninguno de ellos técnico. Un problema a largo plazo lo constituía el hecho de que RSA, que es el núcleo de PGP, es un producto patentado y la ley de patentes requería que Zimmermann obtuviese una licencia de RSA Data Security, Inc., antes de lanzar PGP. Sin embargo, Zimmermann decidió dejar de lado este problema. PGP no estaba pensado como un producto para las empresas, sino más bien como algo para el individuo. Zimmermann pensó que no estaría compitiendo directamente con RSA Data Security, Inc., y confío en que la compañía le otorgaría una licencia gratuita a su debido tiempo.

Un problema más serio e inmediato lo constituía el amplio proyecto de ley contra el crimen de 1991 del Senado de Estados Unidos, que contenía la siguiente cláusula: «Es el parecer del Congreso que los proveedores de servicios electrónicos de comunicación y los fabricantes de maquinaria relacionada con el servicio electrónico de comunicación se asegurarán que los sistemas de comunicaciones permitan que el gobierno obtenga el contenido en texto llano de las comunicaciones orales, por datos o por cualquier otro medio, cuando así lo autorice la ley». Al Senado le preocupaba que los avances de la tecnología digital, como los teléfonos celulares, podrían impedir que la policía llevase a cabo intervenciones de línea efectivas. Sin embargo, además de obligar a las compañías a garantizar la posibilidad de

intervención de las líneas, el proyecto de ley parecía amenazar también todas las formas seguras de cifrado.

El esfuerzo conjuntado de RSA Data Security, Inc., la industria de las comunicaciones, y los grupos defensores de las libertades civiles hizo que se abandonara la cláusula, pero el consenso era que esto era tan sólo un respiro temporal. Zimmermann temía que tarde o temprano el gobierno intentaría de nuevo introducir legislación que prohibiese de hecho codificaciones como PGR Siempre había tenido la intención de vender PGP, pero ahora reconsideró sus opciones. En vez de esperar y correr el riesgo de que PGP fuera prohibido por el gobierno decidió que era más importante que fuese asequible para todo el mundo antes de que fuera demasiado tarde. En junio de 1991 dio el paso drástico de pedir a un amigo que expusiera PGP en un *bulletin board* («hoja de anuncios») de Usenet. PGP es sólo un trozo de *software* y, por tanto, cualquiera podía copiarlo (download) gratis del *bulletin board* e instalarlo en su propio ordenador. Ahora PGP andaba suelto por Internet.

Al principio, PGP causó excitación tan sólo entre los aficionados a la criptografía. Luego fue copiado por un sector más amplio de entusiastas de Internet. A continuación, las revistas informáticas publicaron unos breves informes y luego largos artículos sobre el fenómeno PGP. Gradualmente, PGP comenzó a extenderse hasta los rincones más remotos de la comunidad digital. Por ejemplo, los grupos defensores de los derechos humanos de todo el mundo empezaron a utilizar PGP para cifrar sus documentos e impedir que la información cayera en manos de regímenes que estaban siendo acusados de violar los derechos humanos. Zimmermann comenzó a recibir *e-mails* elogiándolo por su creación. «Hay grupos de resistencia en Birmania», dice Zimmermann, «que lo utilizan en campos de entrenamiento en la selva. Dicen que les ayudó a subir la moral allí, porque antes de que se introdujera PGP, los documentos interceptados causaban la detención, la tortura y la ejecución de familias enteras». En octubre de 1993, recibió el siguiente *e-mail* de alguien de Letonia el día que Boris Yeltsin bombardeaba el edificio del Parlamento letonio: «Phil, quiero que lo sepas: ojalá que no suceda nunca, pero si la dictadura se apodera de Rusia, tu PGP está extendido ahora desde el Báltico al Lejano Oriente, y ayudará a la gente democrática si es necesario. Gracias».

Mientras Zimmermann se ganaba *fans* por todo el mundo, en Estados Unidos era objeto de críticas. RSA Data Security, Inc., decidió no otorgarle una licencia gratuita y estaba furiosa por infringirse su patente. Aunque Zimmermann lanzó PGP como *freeware (.software* gratuito), contenía el sistema RSA de criptografía de clave pública, y, por consiguiente, RSA Data Security, Inc., tachó a PGP de «*banditware*» *{«software* bandido»), Zimmermann había regalado algo que pertenecía a otro. La disputa sobre la patente continuaría varios años, durante los cuales Zimmermann tuvo que afrontar un problema aún mayor.

En febrero de 1993, dos investigadores del gobierno visitaron a Zimmermann. Después de sus preguntas iniciales acerca de la violación de la patente comenzaron a interrogarle sobre la acusación más seria de exportar ilegalmente un arma. Como el gobierno de Estados Unidos incluye el *software* de codificación en su definición de municiones, junto a los misiles, los morteros y las ametralladoras, PGP no se podía exportar sin una licencia del Departamento de Estado. En otras palabras, Zimmermann fue acusado de ser un traficante de armas porque había exportado PGP a través de Internet. Durante los tres años siguientes, Zimmermann fue objeto de una investigación por parte de un jurado y se vio perseguido por el FBI.

1. Codificación para las masas... ¿O no?

La investigación a que estaban siendo sometidos Phil Zimmermann y el PGP encendió un debate sobre los efectos positivos y negativos de la codificación en la Era de la Información. La propagación de PGP hizo reaccionar a los criptógrafos, los políticos, los defensores de las libertades civiles y la policía, obligándolos a plantearse las implicaciones de la codificación generalizada. Estaban los que, como Zimmermann, creían que el uso generalizado de una codificación segura aportaría ventajas a la sociedad, proporcionando privacidad a los individuos para sus comunicaciones digitales. Frente a ellos estaban los que creían que la codificación era una amenaza para la sociedad, porque los criminales y los terroristas podrían comunicarse en secreto, con la seguridad de que la policía no había intervenido sus líneas.

El debate continuó a lo largo de los años noventa, y hoy día es tan conflictivo como siempre. La cuestión fundamental es si el gobierno debería legislar o no contra la

criptografía. La libertad criptográfica permitiría que cualquiera, incluidos los criminales, pudiera tener la certeza de que sus *e- mails* son seguros. Por otra parte, restringir el uso de la criptografía permitiría que la policía espiase a los criminales, pero también facultaría que la policía y todos los demás espiasen al ciudadano medio. En última instancia, seremos nosotros, a través del gobierno que elijamos, los que decidamos el papel futuro de la criptografía. Esta sección está dedicada a esbozar las dos partes del debate. Gran parte de la discusión se referirá a las normas y a los que las crean en Estados Unidos, en parte porque allí surgió PGP, y en parte porque cualquiera que sea la política que se adopte en ese país, en última instancia afectará a las políticas de todo el mundo.

El argumento en contra del uso generalizado de la codificación, como lo presentan los encargados de hacer que se cumplan las leyes, se centra en el deseo de mantener el *statu quo.* Durante décadas, la policía de todo el mundo ha llevado a cabo intervenciones legales de líneas telefónicas para capturar a criminales. Por ejemplo, en 1918, en Estados Unidos se utilizó la intervención de teléfonos para contrarrestar la presencia de espías de guerra, y en los años veinte demostraron ser especialmente eficaces para condenar a los contrabandistas. El punto de vista de que la intervención de teléfonos era un mal necesario para imponer el cumplimiento de la ley se estableció firmemente a finales de los años sesenta, cuando el FBI se dio cuenta de que el crimen organizado se estaba convirtiendo en una creciente amenaza para la nación. Los responsables del cumplimiento de la ley tenían muchos problemas para condenar a los sospechosos porque la mafia amenazaba a cualquiera que pudiera testificar contra ellos, y existía también el código de *omertá*, o silencio. La policía pensó que su única esperanza era obtener pruebas mediante la intervención de teléfonos, y el Tribunal Supremo se mostró favorable a esta argumentación. En 1967 dictaminó que la policía podía hacer uso de intervenciones de teléfonos siempre que hubiera obtenido previamente la autorización de un tribunal.

Veinte años después, el FBI aún mantenía que «la intervención de teléfonos ordenada por los tribunales es la técnica de investigación más eficaz que la policía puede utilizar para combatir las drogas ilegales, el terrorismo, los delitos violentos, el espionaje y el crimen organizado». Sin embargo, las intervenciones de líneas

serían inútiles si los criminales tuvieran acceso a la codificación. Una llamada de teléfono hecha través de una línea digital no es más que un flujo de números y se puede cifrar en base a las mismas técnicas usadas para cifrar los *e-mails.* PGPfone, por ejemplo, es uno de los numerosos productos capaces de cifrar las comunicaciones de voz realizadas por Internet.

Los representantes de la ley alegan que la intervención eficaz de líneas es necesaria para mantener el orden público y que la codificación debería ser restringida para que ellos puedan continuar con sus intervenciones. La policía ya ha tropezado con criminales que usaban una codificación potente para protegerse. Un experto legal alemán dijo que «los negocios calientes, como el tráfico de armas y de drogas, ya no se hacen por teléfono, sino que se están estableciendo en forma cifrada en las redes de datos mundiales». Un oficial de la Casa Blanca señaló una tendencia igualmente preocupante en Estados Unidos, afirmando que «los miembros del crimen organizado están entre los usuarios más avanzados de los sistemas informáticos y de la codificación potente». Por ejemplo, el cártel de Cali organiza sus negocios de drogas a través de comunicaciones cifradas. Los representantes de la ley temen que Internet, unida a la criptografía, ayudará a los criminales a comunicarse y a coordinar sus esfuerzos, y se sienten especialmente preocupados por los denominados Cuatro Jinetes del Infocalipsis —los traficantes de droga, el crimen organizado, los terroristas y los pedófilos—, los grupos que más se beneficiarán de la codificación.

Además de cifrar sus comunicaciones, los criminales y los terroristas están cifrando también sus planes y sus documentos, dificultando la recuperación de pruebas. Se descubrió que la secta Aum Shinrikyo, responsable de los atentados con gas en el metro de Tokio en 1995, había codificado algunos de sus documentos utilizando RSA. Ramsey Yousef, uno de los terroristas involucrados en el atentado con bombas contra el World Trade Center de Nueva York, guardaba sus planes para futuros actos terroristas cifrados en su ordenador portátil. Además de las organizaciones terroristas, también otros criminales más ramplones se benefician de la codificación. Un consorcio ilegal de apuestas norteamericano, por ejemplo, codificó su contabilidad durante cuatro años. Un estudio de Dorothy Denning y William Baugh, encargado en 1997 por el Grupo de Trabajo contra el Crimen Organizado del Centro

de Información de Estrategia Nacional de Estados Unidos, estimó que había quinientos casos penales relacionados con la codificación en todo el mundo y predijo que este número tendería a duplicarse cada año.

Además de lo relacionado con la vigilancia policial, hay también asuntos de seguridad nacional. La NSA norteamericana es la responsable de reunir datos sobre los enemigos de la nación descifrando sus comunicaciones. La NSA opera una red mundial de estaciones de escucha, en cooperación con el Reino Unido, Australia, Canadá y Nueva Zelanda, en la que todas ellas acumulan información y la comparten. La red incluye lugares como la base de señales de Inteligencia de Menwith Hill, Yorkshire, la mayor estación de espionaje del mundo. Parte del trabajo realizado en Menwith Hill tiene que ver con el sistema Echelon, que es capaz de escanear *e-mails*, faxes, télexy llamadas telefónicas buscando palabras concretas. Echelon funciona basado en un diccionario de palabras sospechosas, como «Hezbolá», «asesino» y «Clinton», y el sistema es suficientemente inteligente para reconocer estas palabras en tiempo real. Echelon puede conservar mensajes cuestionables para examinarlos más a fondo, lo que le permite vigilar los mensajes de grupos políticos concretos u organizaciones terroristas. Sin embargo, Echelon resultaría inútil si todos los mensajes estuvieran fuertemente codificados. Cada una de las naciones que participan en Echelon perdería valiosa información referente a conspiraciones políticas y atentados terroristas.

Al otro lado del debate están los defensores de las libertades civiles, incluidos grupos como el Centro por la Democracia y la Tecnología, o la Fundación Frontera Electrónica. El argumento a favor de la codificación se basa en la creencia de que la privacidad es un derecho humano fundamental, reconocido en el Artículo 12 de la Declaración Universal de los Derechos Humanos: «Nadie estará sujeto a la interferencia arbitraria con su privacidad, familia, hogar o correspondencia, así como tampoco a ataques contra su honor y su reputación. Todos los individuos tienen derecho a la protección de la ley contra semejantes interferencias o ataques».

Los defensores de las libertades civiles alegan que el uso de la codificación es esencial para garantizar el derecho a la privacidad. De otra forma, temen que la llegada de la tecnología digital, que facilita muchísimo la vigilancia, anunciará una

nueva era de intervenciones de líneas y los abusos que inevitablemente se producen. En el pasado, los gobiernos han utilizado frecuentemente su poder para llevar a cabo intervenciones de líneas de ciudadanos inocentes. Los presidentes Lyndon Johnson y Richard Nixon fueron culpables de realizar intervenciones telefónicas injustificadas, y el presidente John F. Kennedy llevó a cabo intervenciones sospechosas en el primer mes de su mandato presidencial. Durante el período que precedió a un proyecto de ley relacionado con importaciones de azúcar de la República Dominicana, Kennedy pidió que se interviniesen los teléfonos de varios miembros del Congreso. Su justificación fue que pensaba que los estaban sobornando, lo que aparentemente constituía una preocupación válida relacionada con la seguridad nacional. Sin embargo, nunca se encontró ninguna prueba de soborno, y la intervención de los teléfonos proporcionó a Kennedy información política útil que ayudó al gobierno a pasar el proyecto de ley.

Uno de los casos más famosos de intervención telefónica continuada e injustificada fue el caso de Martin Luther King, cuyas conversaciones telefónicas fueron vigiladas durante varios años. Por ejemplo, en 1963 el FBI obtuvo información referente a King mediante la intervención de su teléfono y se la entregó al senador James Eastland para ayudarlo en los debates sobre un proyecto de ley relacionado con los derechos civiles. De manera más general, el FBI acumuló detalles sobre la vida privada de King, que fueron utilizados para desacreditarlo. Ciertas grabaciones de King contando historias un tanto subidas de tono fueron enviadas a su esposa y se las hicieron oír al presidente Johnson. Luego, después de que King fuera galardonado con el Premio Nobel, se enviaban detalles embarazosos de la vida de King a cualquier organización que estuviera considerando concederle algún honor.

Otros gobiernos son igualmente culpables de abusar de las intervenciones telefónicas. La Commission Nationale de Contróle des Interceptions de Sécurité estima que en Francia se realizan aproximadamente 100.000 intervenciones ilegales de líneas al año. Posiblemente, la mayor violación de la privacidad de todos los individuos sea el programa internacional Echelon. Echelon no tiene que justificar sus interceptaciones y no se centra en ciertas personas en particular. En vez de ello, recoge información indiscriminadamente, utilizando receptores que detectan las telecomunicaciones que pasan por los satélites. Si Alicia envía un inofensivo

mensaje transatlántico a Benito, será sin duda interceptado por Echelon, y si da la casualidad que el mensaje contiene algunas palabras que aparecen en el diccionario Echelon, será conservado para ser examinado con más detalle, junto a mensajes de grupos políticos extremos y bandas terroristas. Mientras que los representantes de la ley alegan que la codificación debería ser prohibida porque haría que Echelon perdiera su eficacia, los defensores de los derechos civiles argumentan que la codificación es necesaria exactamente porque haría que Echelon perdiera su eficacia.

Cuando los representantes de la ley alegan que la codificación reducirá el número de criminales condenados, los defensores de los derechos civiles responden que la cuestión de la privacidad es más importante. En cualquier caso, los defensores de los derechos civiles insisten que la codificación no constituiría una enorme barrera para los representantes de la ley, porque la intervención de líneas no es un elemento crucial en la mayoría de los casos.

Por ejemplo, en 1994 hubo en Estados Unidos unas mil intervenciones autorizadas por los tribunales, en comparación con un cuarto de millón de casos federales.

No extrañará que entre los defensores de la libertad criptográfica se encuentren algunos de los inventores de la criptografía de clave pública. Whitfield Diffie afirma que los individuos han gozado de completa privacidad durante la mayor parte de la Historia:

> *En la década de 1790, cuando se ratificó la Bill of Rights*[25]*, dos personas cualquiera podían mantener una conversación privada —con una seguridad que nadie en el mundo disfruta hoy en día— simplemente caminando unos pocos metros por el camino y mirando a ver si no había nadie escondido en los arbustos. No había aparatos de grabación, ni micrófonos parabólicos, ni interferómetros láser rebotando en sus gafas. Es evidente que la civilización sobrevivió. Muchos de nosotros consideramos ese período como la edad dorada de la cultura política norteamericana.*

[25] Bill of Rights («Ley de Derechos»): en términos generales, es toda la ley que establece los derechos de los individuos, o de una cierta clase. Diffie se refiere aquí concretamente a la Ley de 1791 que estableció las enmiendas constitucionales de Estados Unidos. (N. del T.)

Ron Rivest, uno de los inventores de RSA, piensa que restringir la criptografía sería temerario:

> *Es una política muy pobre tomar medidas drásticas indiscriminadamente contra una tecnología sólo porque algunos criminales podrían utilizarla para su propio beneficio. Por ejemplo, cualquier ciudadano americano puede comprar libremente un par de guantes, a pesar de que un ladrón podría utilizarlos para saquear una casa sin dejar huellas dactilares. La criptografía es una tecnología de protección de datos, igual que los guantes son una tecnología de protección de manos. La criptografía protege los datos contra los piratas informáticos, los espías de empresa y los timadores, mientras que los guantes protegen las manos contra los cortes, los rasguños, el calor, el frío y las infecciones. La criptografía puede frustrar las intervenciones de línea del FBI y los guantes pueden frustrar los análisis de huellas dactilares del FBI. Tanto la criptografía como los guantes son baratísimos y al alcance de todos. De hecho, se puede copiar software criptográfico de buena calidad en Internet por menos del precio de un buen par de guantes.*

Posiblemente, los mayores aliados de la causa a favor de los derechos civiles sean las grandes empresas. El comercio por Internet está todavía en pañales, pero las ventas están creciendo rápidamente, con los vendedores de libros, CD musicales y *software* a la cabeza, seguidos de los supermercados, las compañías de viajes y otros negocios. En 1998, un millón de británicos usaron Internet para comprar productos por valor de 400 millones de libras esterlinas, una cifra que se prevé se cuadruplicará en 1999. En sólo unos pocos años, el comercio por Internet podría dominar el mercado, pero sólo si las empresas logran solucionar los temas relacionados con la seguridad y la confianza. Una empresa debe poder garantizar la privacidad y la seguridad de las transacciones financieras y la única manera de hacerlo es utilizar una codificación potente.

En estos momentos, una compra por Internet se puede proteger con la criptografía de clave pública. Alicia visita la página web de una compañía y selecciona un

artículo. Rellena una hoja de pedido que le pide su nombre, su dirección y los detalles de su tarjeta de crédito. A continuación, Alicia usa la clave pública de la compañía para codificar la hoja de pedido. Transmite la hoja de pedido codificada a la compañía, que son las únicas personas capaces de descifrarla, porque sólo ellos tienen la clave privada necesaria para la descodificación. Todo esto lo hace automáticamente el navegador (p. e., Netscape o Explorer) de Alicia en conjunción con el ordenador de la compañía.

Como siempre, la seguridad de la codificación depende del tamaño de la clave. En Estados Unidos no hay restricciones en el tamaño de las claves, pero a las compañías de *software* de ese país todavía no se les permite exportar productos para la web que ofrezcan codificación potente. Por eso, los navegadores que se exportan al resto del mundo sólo pueden manejar claves cortas, de modo que sólo ofrecen una seguridad moderada. De hecho, si Alicia está en Londres comprando un libro a una compañía de Chicago, su transacción por Internet es un billón de billones de billones de veces menos segura que la transacción de Benito comprando un libro en Nueva York a la misma compañía. La transacción de Benito es absolutamente segura porque su navegador sustenta la codificación con una clave mayor, mientras que la transacción de Alicia podría ser descifrada por un criminal persistente. Afortunadamente, el coste del equipo necesario para descifrar los detalles de la tarjeta de crédito de Alicia es mucho más elevado que el límite típico de las tarjetas de crédito, de forma que semejante ataque no resulta económicamente rentable.

Sin embargo, como la cantidad de dinero que fluye por Internet aumenta, en algún momento a los criminales les resultará rentable descifrar los detalles de las tarjetas de crédito. En resumen, si el comercio por Internet va a crecer rápidamente, los clientes de todo el mundo deben contar con una seguridad apropiada y las empresas no tolerarán la codificación limitada.

Las empresas desean una codificación potente también por otra razón. Las compañías almacenan grandes cantidades de información en bases de datos informáticas, incluidas las descripciones de los productos, los detalles sobre los clientes y la contabilidad. Naturalmente, las empresas quieren proteger esta información contra los piratas informáticos que podrían infiltrarse en el ordenador y robar la información. Esta protección se pude lograr cifrando la información

almacenada, para que sólo sea accesible para los empleados que tienen la clave de descodificación.

Para resumir la situación, está claro que el debate se da entre dos campos: los defensores de los derechos civiles y las empresas están a favor de la codificación potente, mientras que los representantes de la ley están a favor de restricciones severas. En general, la opinión pública parece estar dando un giro en favor de la alianza procodificación, que ha sido ayudada por una prensa favorable y un par de películas de Hollywood. A principios de 1998, *Al rojo vivo* contó la historia de una nueva cifra, supuestamente indescifrable, de la NSA que es descifrada sin querer por un niño autista de nueve años. Alee Baldwin, un agente de la NSA, se propone asesinar al niño, al que se percibe como una amenaza para la seguridad nacional. Por suerte, el chico cuenta con Bruce Willis para protegerlo. También en 1998, Hollywood estrenó *Enemigo público*, que trata de una conspiración de la NSA para asesinar a un político que apoya un proyecto de ley a favor de la codificación potente. Matan al político, pero un abogado, interpretado por Will Smith, y un rebelde de la NSA, encamado por Gene Hackman, logran llevar a los asesinos de la NSA ante la justicia. Ambas películas presentan a la NSA como más siniestra que la CIA, y en muchos aspectos la NSA ha asumido el papel de la amenaza de los poderes establecidos.

Mientras el grupo de presión procodificación presenta argumentos a favor de la libertad criptográfica y el grupo de presión anticodificación lo hace a favor de restricciones criptográficas hay una tercera opción que podría ofrecer un acuerdo. Durante la última década, criptógrafos y políticos han estado investigando los pros y los contras de un plan conocido como «depósito de claves» *(key escrow).* El término «depósito» se relaciona generalmente con un acuerdo en el que alguien da una suma de dinero a un tercero, que luego puede entregar el dinero a una segunda persona si se cumplen ciertas circunstancias. Por ejemplo, un inquilino podría realizar un depósito con un abogado, que luego puede entregárselo al dueño en caso de que se causen daños a la propiedad. En términos criptográficos, depósito significa que Alicia le daría una copia de su clave privada a un agente de depósitos *(escrow agent*), un intermediario independiente y fiable, que está autorizado para entregar la clave privada a la policía si en algún momento hubiera suficiente

evidencia que sugiriese que Alicia estaba involucrada en un delito.

La prueba más famosa de depósito de claves criptográficas fue el American Escrowed Encryption Standard (Estándar Americano de Codificación en Depósito), adoptado en 1994. El objetivo era alentar la adopción de dos sistemas de codificación, denominados *Clipper* y *caps tone,* en las comunicaciones telefónicas y por ordenador, respectivamente. Para utilizar la codificación *Clipper,* Alicia compraría un teléfono con un chip preinstalado que guardaría la información secreta de su clave privada. En el momento mismo en que ella comprara el teléfono *Clipper,* una copia de la clave privada almacenada en el chip se rompería en dos mitades y cada mitad sería enviada a dos autoridades federales diferentes. El gobierno de Estados Unidos alegó que Alicia tendría acceso a una codificación segura, y su privacidad sólo sería invadida si los representantes de la ley podían persuadir a las dos autoridades federales de que existían suficientes argumentos para obtener su clave privada depositada.

El gobierno de Estados Unidos empleó *Clipper* y *capstone* para sus propias comunicaciones y obligó a las compañías vinculadas con los asuntos gubernamentales a adoptar el American Escrowed Encryption Standard. Las demás empresas y los individuos eran libres de utilizar otras formas de codificación, pero el gobierno confiaba en que *Clipper* y *capstone* se convertirían gradualmente en la forma favorita de codificación de la nación. Sin embargo, esa política no funcionó. La idea del depósito de claves consiguió pocos partidarios fuera del gobierno. A los defensores de las libertades civiles no les gustó la idea de que las autoridades federales poseyeran las claves de todo el mundo: establecieron una analogía con las llaves reales y preguntaron cómo se sentiría la gente si el gobierno tuviera las llaves de todas nuestras casas. Los expertos criptográficos señalaron que un solo empleado deshonesto podría socavar todo el sistema vendiendo claves depositadas al mejor postor. Y a las empresas les preocupó la confidencialidad. Por ejemplo, una empresa europea en Estados Unidos podría temer que sus mensajes estuvieran siendo interceptados por oficiales norteamericanos de comercio, en una tentativa de obtener secretos que pudieran dar ventajas competitivas a sus rivales norteamericanos.

A pesar del fracaso de *Clipper* y *capstone,* muchos gobiernos siguen con vencidos

de que se puede hacer que funcione el depósito de claves, siempre que las claves estén lo suficientemente bien protegidas contra los criminales y existan salvaguardias para garantizar al público que el sistema no se presta al abuso por parte del gobierno. Louis J.

Freeh, director del FBI, dijo en 1996: «La comunidad de los representantes de la ley apoya completamente una política equilibrada referente al cifrado... El depósito de claves no es sólo la única solución; es, de hecho, una solución muy buena, porque equilibra eficazmente las preocupaciones sociales fundamentales relacionadas con la privacidad, la seguridad de la información, el comercio electrónico, la seguridad pública y la seguridad nacional». Aunque el gobierno de Estados Unidos ha dado marcha atrás en lo referente a sus propuestas de depósito de claves, muchos sospechan que volverá a intentar introducir una forma alternativa de depósito de claves en el futuro.

Habiendo presenciado el fracaso del depósito opcional, los gobiernos podrían incluso considerar el depósito obligatorio. Mientras tanto, el grupo de presión pro-codificación continúa alegando contra el depósito de claves. Kenneth Neil Cukier, un periodista de temas tecnológicos, ha escrito que: «Los participantes en el debate sobre la criptografía son todos inteligentes, honrados y partidarios del depósito, pero nunca poseen más de dos de estas características a la vez».

Existen varias otras opciones que los gobiernos podrían optar por poner en práctica para intentar equilibrar las preocupaciones de los defensores de las libertades civiles, las empresas y los representantes de la ley. No está nada claro cuál será la opción preferida, porque en la actualidad la política criptográfica cambia constantemente. Un flujo constante de sucesos en todo el mundo está influyendo en el debate sobre la codificación. En noviembre de 1998, el discurso de la reina de Inglaterra anunció que se promulgaría una nueva legislación británica referente al mercado digital. En diciembre de 1998, 33 naciones firmaron el Acuerdo de Wassenaar, que limita la exportación de armas, que incluye también las tecnologías de codificación potente. En enero de 1999, Francia derogó sus leyes anticriptografía, que hasta entonces habían sido las más restrictivas de Europa occidental, probablemente como resultado de la presión del mundo de los negocios. En marzo de 1999, el gobierno británico hizo público un documento de consulta sobre un

proyecto de Ley de Comercio Electrónico.

Para cuando usted lea esto, se habrán producido muchas más vueltas y revueltas en el debate sobre la política criptográfica. Sin embargo, un aspecto de la futura política de codificación parece seguro, a saber, la necesidad de *autoridades certificadoras.* Si Alicia quiere enviar un *e-mail* seguro a un nuevo amigo, Pepe, necesita la clave pública de Pepe. Podría pedir a Pepe que le envíe su clave pública por correo. Desgraciadamente, existe entonces el riesgo de que Eva intercepte la carta de Pepe a Alicia, la destruya y falsifique una nueva carta que incluya la propia clave pública de Eva en vez de la de Pepe. Puede que entonces Alicia envíe un *e-mail* delicado a Pepe, pero sin darse cuenta lo habrá cifrado con la clave pública de Eva. Si Eva puede interceptar este *e-mail*, puede descifrarlo fácilmente y leerlo. En otras palabras, uno de los problemas de la criptografía de clave pública es estar seguro de que tienes la genuina clave pública de la persona con la que deseas comunicarte. Las autoridades certificadoras son organizaciones que verificarán que una clave pública corresponde efectivamente a una persona en particular. Una autoridad certificadora podría solicitar un encuentro cara a cara con Pepe para asegurarse de que han catalogado correctamente su clave pública. Si Alicia confía en la autoridad certificadora puede obtener de ella la clave pública de Pepe y tener confianza en que la clave es válida.

Ya he explicado cómo Alicia podría comprar productos de manera segura en Internet usando la clave pública de una compañía para cifrar la hoja de pedido. En realidad, sólo haría esto si la clave pública estuviera validada por una autoridad certificadora. En 1998, el líder del mercado de la certificación era Verisign, que se ha convertido en una compañía de 30 millones de dólares en sólo cuatro años. Además de garantizar el cifrado fiable certificando claves públicas, las autoridades certificadoras pueden garantizar también la validez de las firmas digitales. En 1998, la compañía irlandesa Baltimore Technologies proveyó la certificación de las firmas digitales del presidente Bill Clinton y el primer ministro Bertie Ahern. Esto permitió que los dos mandatarios firmasen digitalmente un comunicado en Dublín.

Las autoridades certificadoras no suponen ningún riesgo de seguridad. Simplemente se habrían limitado a pedir a Pepe que revelara su clave pública para que ellos pudieran validarla para otras personas que deseen enviarle mensajes cifrados. Sin

embargo, hay otras compañías, conocidas como TTPs *(trusted third parties*, «terceras partes confiables»), que proveen un servicio más polémico conocido como *recuperación de claves.* Imagine que una empresa legal que protege todos sus documentos vitales cifrándolos con su propia clave pública, de modo que sólo ella los pueda descifrar con su propia clave privada. Un sistema semejante es una medida eficaz contra los piratas informáticos y cualquier otra persona que pudiese intentar robar la información. Sin embargo, ¿qué sucede si el empleado que guarda la clave privada la olvida, se fuga o es atropellado por un autobús? Los gobiernos están alentando la formación de TTPs que guarden copias de todas las claves. Una compañía que pierda su clave privada puede entonces recuperarla recurriendo a su TTP.

Las terceras partes confiables (TTPs) son polémicas porque tendrían acceso a las claves privadas de la gente y, por tanto, estarían capacitadas para leer los mensajes de sus clientes. Deben ser dignas de confianza, de otra forma se puede abusar fácilmente del sistema. Algunos afirman que las TTPs son en realidad una reencarnación del depósito de claves, y que los representantes de la ley se sentirán tentados de amedrentar a las TTPs para que les entreguen las claves de un cliente durante una investigación policial. Otras aseguran que las TTPs son una parte necesaria de cualquier infraestructura de clave pública sensata.

Nadie puede predecir qué papel desempeñarán las TTPs en el futuro y nadie puede prever con certeza cómo será la política criptográfica dentro de diez años. Sin embargo, sospecho que en un futuro próximo el grupo de presión pro-codificación ganará inicialmente la discusión, principalmente porque ningún país querrá tener leyes de codificación que prohíban el comercio electrónico *(e-commerce).* Sin embargo, si esta política resulta ser un error, siempre será posible revocar las leyes. Si se produjese una serie de atrocidades terroristas y los representantes de la ley pudieran demostrar que la intervención de líneas las habían impedido, los gobiernos no tardarían en mostrarse partidarios de una política de depósito de claves. Se obligaría a todos los usuarios de una codificación potente a depositar sus claves con un agente de depósito de claves y a partir de entonces cualquiera que enviase un mensaje cifrado con una clave no depositada estaría infringiendo la ley. Si la pena para la codificación no depositada fuera lo suficientemente severa, los

representantes de la ley podrían recuperar el control. Después, si los gobiernos llegaran a abusar de la confianza que conlleva un sistema de depósito de claves, el público pediría la vuelta de la libertad criptográfica y el péndulo volvería a virar en dirección contraria. En resumen, no hay ninguna razón por la que no podamos cambiar nuestra política para que se adapte al ambiente político, económico y social. El factor decisivo será a quién teme más el público, si a los criminales o al gobierno.

2. La rehabilitación de Zimmermann

En 1993 Phil Zimmermann fue objeto de una investigación por parte de un jurado. Según el FBI, había exportado una munición, porque había suministrado a naciones hostiles y a terroristas los útiles que necesitaban para evadir la autoridad del gobierno de

Estados Unidos. Según fueron prolongándose las investigaciones, más y más criptógrafos y defensores de las libertades civiles se apresuraron a apoyar a Zimmermann, creando un fondo internacional para financiar su defensa legal. Al mismo tiempo, el prestigio de ser objeto de una investigación del FBI aumentó la reputación de PGP, y la creación de Zimmermann se expandió por Internet aún más rápidamente; después de todo, éste era el *software* de codificación que era tan seguro que asustaba al FBI.

Inicialmente, *Pretty Good Privacy* se había hecho público con prisas, y como resultado el producto no estaba todo lo pulido que pudiera estar. Pronto se pidió que se desarrollara una versión revisada de PGP, pero era evidente que Zimmermann no estaba en situación de continuar trabajando en el producto. En vez de ello, algunos ingenieros de *software* europeos comenzaron a reconstruir PGP. En general, las actitudes europeas respecto al cifrado eran, y continúan siendo, más liberales, y no habría ninguna restricción para exportar una versión europea de PGP por todo el mundo. Además, la disputa sobre la patente de RSA no tenía relevancia en Europa, porque las patentes de RSA no tenían validez fuera de Estados Unidos.

Después de tres años, la investigación del jurado acusador aún no había llevado a Zimmermann a juicio. El caso lo complicaba la naturaleza de PGP y la manera en que se había distribuido. Si Zimmermann hubiese cargado PGP en un ordenador y

luego lo hubiera enviado a un régimen hostil, el caso contra él sería sencillo, porque obviamente habría sido culpable de exportar un sistema operativo de codificación completo. De manera similar, si hubiese exportado un disco que contuviera el programa PGP, el objeto físico podría ser interpretado como un aparato criptográfico y, de nuevo, el caso contra Zimmermann habría sido bastante sólido. Por otra parte, si hubiera impreso el programa informático y lo hubiese exportado en forma de libro, el caso contra él ya no sería tan claro, porque entonces se consideraría que había exportado conocimientos en vez de un aparato criptográfico. Sin embargo, el material impreso es muy fácil de escanear electrónicamente y pasar la información directamente a un ordenador, lo que significa que un libro es tan peligroso como un disco. Lo que realmente sucedió fue que Zimmermann le dio una copia de PGP a un «amigo», que simplemente la instaló en un ordenador norteamericano, el cual daba la casualidad que estaba conectado a Internet. Después de eso, puede que un régimen hostil lo haya copiado, o puede que no. ¿Era Zimmermann realmente culpable de exportar PGP? Incluso hoy día, los asuntos legales en torno a Internet son objeto de debate e interpretación. A principios de los años noventa, la situación era vaga en extremo.

En 1996, tras tres años de investigación, la Oficina Jurídica del gobierno abandonó su caso contra Zimmermann. El FBI se dio cuenta de que era demasiado tarde: PGP se había escabullido en Internet, y procesar a Zimmermann no serviría para nada.

Existía el problema adicional de que algunas de las instituciones más importantes apoyaban a Zimmermann, como por ejemplo, el Centro de Publicaciones del MIT, que había publicado PGP en un libro de 600 páginas. El libro se estaba distribuyendo por todo el mundo, de modo que procesar a Zimmermann habría significado procesar a MIT Press. El FBI también se mostró reacio a iniciar un proceso porque había una gran posibilidad de que Zimmermann no fuera condenado. Un juicio del FBI podría no conseguir más que un embarazoso debate constitucional sobre el derecho a la privacidad, promoviendo aún más la simpatía pública por la codificación generalizada.

El otro gran problema de Zimmermann también se desvaneció. Finalmente, logró un acuerdo con RSA y obtuvo una licencia que resolvía el asunto de la patente. Por fin, PGP era un producto legítimo y Zimmermann era un hombre libre. La investigación

lo había convertido en un cruzado criptográfico y todos los directores de *marketing* del mundo deben haber envidiado la fama y la publicidad gratuita que el caso dio a PGP. A finales de 1997, Zimmermann vendió PGP a NetWork Associates y se convirtió en uno de sus socios. Aunque ahora PGP se vende a las empresas, todavía está disponible gratuitamente para los individuos que no tienen intenciones de usarlo para ningún fin comercial. En otras palabras, los individuos que simplemente desean ejercer su derecho a la privacidad aún pueden copiar PGP en Internet sin tener que pagar.

Si desea obtener una copia de PGP hay varias páginas en Internet que lo ofrecen, y no le resultará difícil encontrarlas. Probablemente, la fuente más fiable sea http://www.pgpi.com/, la página de PGP International, de donde se pueden copiar las versiones norteamericana e internacional de PGP. Ahora bien, me absuelvo de toda responsabilidad: si decide instalar PGP, le toca a usted comprobar que su ordenador es capaz de hacerlo funcionar, que el *software* no está infectado con un virus, etcétera. Asimismo, debería comprobar que vive en un país que permite el uso del cifrado potente. Finalmente, debería asegurarse de que está copiando la versión apropiada de PGP: los individuos que viven fuera de Estados Unidos no deberían copiar la versión americana de PGP, porque esto violaría las leyes norteamericanas de exportación. La versión internacional de PGP no sufre ninguna restricción de exportación.

Todavía recuerdo la tarde de domingo en que copié PGP en Internet por vez primera. Desde entonces, he podido garantizar mis *e-mails* contra la posibilidad de ser interceptados y leídos, porque ahora puedo cifrar el material delicado dirigido a Alicia, a Benito y a cualquiera que posea el *software* PGP Mi ordenador portátil y su *software* PGP me proporcionan un nivel de seguridad que está fuera del alcance de los esfuerzos combinados de todos los sistemas de desciframiento del mundo.

Capítulo 8
Un salto cuántico al futuro

Contenido:

1. El futuro del criptoanálisis

2. La criptografía cuántica

Durante dos mil años, los creadores de cifras han luchado por preservar secretos, mientras que los descifradores se han esforzado por revelarlos. Ha sido siempre una carrera reñida, en la que los descifradores contraatacaron cuando los creadores de cifras parecían ir en cabeza y los creadores de cifras inventaron nuevas y más potentes formas de cifrado cuando los métodos previos se vieron comprometidos. La invención de la criptografía de clave pública y el debate político en tomo al uso de criptografía potente nos trae al momento presente, y es evidente que los criptógrafos están ganando la guerra de la información. Según Phil Zimmermann, vivimos en una era dorada de la criptografía: «Ahora, en la criptografía moderna es posible crear cifras que están realmente fuera del alcance de todas las formas conocidas de criptoanálisis. Y creo que va a seguir siendo así». El punto de vista de Zimmermann lo comparte el vicedirector de la NSA, William Crowell: «*Si todos los ordenadores personales del mundo — aproximadamente 260 millones— se pusieran a trabajar para descifrar un solo mensaje cifrado con PGP, se calcula que les costaría 12 millones de veces la edad del universo descifrar un solo mensaje*».

Sin embargo, la experiencia anterior nos dice que todas las cifras que se consideraban indescifrables, tarde o temprano han sucumbido al criptoanálisis. La cifra Vegenère era denominada *le chiffre indéchiffrable*, pero Babbage la descifró; la Enigma era considerada invulnerable, hasta que los polacos revelaron sus puntos débiles. Así que, ¿están los criptoanalistas a punto de realizar otro gran avance, o tiene razón Zimmermann? Predecir los avances futuros de cualquier tecnología es siempre una tarea precaria, pero con las cifras es particularmente arriesgada. No sólo tenemos que adivinar qué descubrimientos nos reserva el futuro, sino que también tenemos que adivinar qué descubrimientos nos reserva el presente. La historia de James Ellis y el GCHQ nos advierte que puede que haya ya avances

extraordinarios escondidos tras el velo del secreto gubernamental.

Este capítulo final examina unas pocas de las ideas futuristas que pueden aumentar o destruir la privacidad en el siglo XXI. La sección siguiente considera el futuro del criptoanálisis y una idea en particular que podría permitir que los criptoanalistas descifraran todas las cifras actuales. En cambio, la sección final del libro considera la posibilidad criptográfica más apasionante, un sistema que tiene el potencial de garantizar una privacidad absoluta.

1. El futuro del criptoanálisis

A pesar de la enorme potencia de RSA y otras cifras modernas, los criptoanalistas aún pueden desempeñar un valioso papel a la hora de recoger inteligencia. Su éxito lo demuestra el hecho de que los criptoanalistas están más solicitados que nunca antes en la Historia: la NSA todavía es la organización que más matemáticos emplea del mundo.

Sólo una pequeña fracción de la información que fluye por el mundo está cifrada con seguridad y el resto está mal cifrada o totalmente sin cifrar. Esto se debe a que el número de usuarios de Internet está creciendo rápidamente y, sin embargo, muy pocas de estas personas toman precauciones adecuadas en lo referente a la privacidad. A su vez, esto significa que las organizaciones encargadas de la seguridad nacional, los representantes de la ley y cualquier otra persona con una mente curiosa pueden tener acceso a más información de la que pueden hacer frente.

Incluso si los usuarios emplean la cifra RSA correctamente, los descifradores todavía pueden hacer muchas cosas para obtener información de los mensajes interceptados. Los descifradores continúan utilizando viejas técnicas como el análisis de tráfico; si los descifradores no pueden descifrar el contenido de un mensaje, al menos pueden lograr averiguar quién lo envía, y a quién va dirigido, lo que en sí mismo puede ser revelador. Un avance más reciente es el denominado *ataque de tempestad*, que trata de detectar las diferentes señales electromagnéticas emitidas por un ordenador cada vez que se teclea una letra. Si Eva aparca una furgoneta cerca de la casa de Alicia puede utilizar un equipo sensible a las tormentas para identificar cada pulsación de una tecla que Alicia realiza en su ordenador. Esto

permitiría a Alicia interceptar el mensaje según va siendo escrito en el ordenador, antes de que sea codificado. Para defenderse de los *ataques de tempestad* existen ya compañías que proveen material protector que se puede usar para revestir las paredes de una habitación e impedir el escape de señales electromagnéticas. En Estados Unidos, es necesario obtener una licencia del gobierno antes de usar semejante material protector, lo que sugiere que organizaciones como el FBI utilizan regularmente la vigilancia de tempestad.

Otros ataques incluyen el uso de virus y caballos de Troya. Eva podría diseñar un virus que infecte el *software* PGP y se instale silenciosamente en el ordenador de Alicia. Cuando Alicia utilice su clave privada para descifrar un mensaje, el virus despertaría y la anotaría. La siguiente vez que Alicia conecte con Internet, el virus enviaría subrepticiamente la clave privada a Eva, permitiéndole descifrar todos los mensajes siguientes enviados por Alicia. El caballo de Troya, otro truco de *software*, conlleva que Eva diseñe un programa que aparentemente funcione como un producto de codificación genuino, pero que en realidad traiciona al usuario. Por ejemplo, Alicia podría creer que está copiando (*download)* una versión auténtica de PGP mientras que está copiando una versión que, en realidad, es un caballo de Troya. Esta versión modificada parece ser exactamente igual al programa PGP genuino, pero contiene instrucciones para enviar a Eva copias de texto llano de toda la correspondencia de Alicia. Como dice Phil Zimmermann: «Cualquiera podría modificar el código de origen y producir una lobotomizada imitación zombi de PGP que parezca real pero que cumpla las órdenes de su diabólico dueño. Entonces podría hacer circular por todas partes esta versión caballo de Troya de PGP, afirmando que es la mía. ¡Qué insidioso! Debería usted esforzarse al máximo para obtener su copia de PGP de una fuente fiable, cualquiera que ésta pueda ser».

Una variante del caballo de Troya es un *software* de codificación completamente nuevo que parece seguro, pero que en realidad contiene una *puerta trasera (backdoor*), algo que permite a sus diseñadores descifrar los mensajes de todo el mundo. En 1998, un informe de Wayne Madsen reveló que la compañía criptográfica suiza Crypto AG había construido *puertas traseras* en algunos de sus productos, suministrando al gobierno de Estados Unidos los detalles de cómo sacar partido a estas *puertas traseras.* Como consecuencia de ello, Estados Unidos podía leer las

comunicaciones de varios países. En 1991, los asesinos que mataron a Sapur Bajtiar, el ex primer ministro iraní exiliado, fueron capturados gracias a la interceptación y el desciframiento de *puerta trasera* de mensajes iraníes codificados con un producto de Crypto AG.

Aunque el análisis de tráfico, los ataques de tempestad, los virus y los caballos de Troya son técnicas útiles para recoger información, los criptoanalistas son conscientes de que su verdadero objetivo es encontrar una forma de romper la cifra RSA, la piedra angular de la codificación moderna. La cifra RSA se utiliza para proteger las comunicaciones militares, diplomáticas, comerciales y criminales más importantes, justo los mensajes que las organizaciones de recogida de inteligencia quieren descifrar. Si se proponen desafiar la potente codificación RSA, los criptoanalistas tendrán que realizar un gran avance teórico o tecnológico.

Un gran avance teórico sería una manera fundamentalmente nueva de encontrar la clave privada de Alicia. La clave privada de Alicia consta de p y q, que se encuentran factorizando la clave pública, N. El enfoque normal es probar los números primos uno por uno para ver si dividen a N, pero sabemos que esto cuesta una desmedida cantidad de tiempo. Los criptoanalistas han intentado encontrar un atajo para factorizar, un método que reduzca drásticamente el número de pasos necesarios para encontrar p y q, pero hasta ahora todas las tentativas de desarrollar un método para factorizar rápidamente han terminado en el fracaso. Los matemáticos han estado estudiando la factorización durante siglos y las técnicas modernas de factorización no son considerablemente mejores que las técnicas antiguas. De hecho, podría ser que las leyes de las matemáticas no permitan la existencia de un atajo importante para factorizar.

Sin mucha esperanza de un gran avance teórico, los criptoanalistas se han visto obligados a buscar una innovación tecnológica. Si no existe una manera obvia de reducir el número de pasos necesarios para factorizar, los criptoanalistas necesitan una tecnología que lleve a cabo estos pasos con más rapidez. Los chips de silicona seguirán siendo cada vez más rápidos con el paso de los años, aumentando al doble su velocidad aproximadamente cada dieciocho meses, pero esto no es suficiente para causar un impacto verdadero en la velocidad de la factorización: los criptoanalistas necesitan una tecnología que sea billones de veces más rápida que

los ordenadores actuales. Por consiguiente, los criptoanalistas están anhelando una forma radicalmente nueva de ordenador, el *ordenador cuántico.* Si los científicos pudieran construir un ordenador cuántico, sería capaz de realizar cálculos a una velocidad tan tremenda que haría que un superordenador moderno parezca un ábaco roto.

El resto de esta sección se ocupa del concepto de un ordenador cuántico y, por tanto, introduce algunos de los principios de la física cuántica, a veces denominada mecánica cuántica. Antes de continuar, por favor preste atención a una advertencia formulada originalmente por Niels Bohr, uno de los padres de la mecánica cuántica: «*Cualquiera que pueda contemplar la mecánica cuántica sin sentir vértigo es que no la ha comprendido*». En otras palabras, prepárese para enfrentarse a algunas ideas bastante raras.

Para explicar los principios de la informática cuántica, resulta útil remontarse a finales del siglo XVIII y observar el trabajo de Thomas Young, el polifacético inglés que realizó el primer gran avance en el desciframiento de los jeroglíficos egipcios. Como profesor del Emmanuel College, de la Universidad de Cambridge, a menudo Young pasaba la tarde relajándose junto al estanque de patos de la universidad. Según se cuenta, cierto día se fijó en dos patos que nadaban felices uno junto al otro. Observó que los dos patos dejaban dos rastros de ondas detrás de ellos, que se mezclaban y formaban un patrón particular de partes agitadas y partes en calma. Los dos juegos de ondas se desplegaban detrás de los dos patos, y cuando la cima de la estela de un pato se juntaba con el valle de la del otro pato el resultado era un pequeño trozo de agua en calma: la cima y el valle se cancelaban mutuamente. De manera alternativa, si dos cimas llegaban al mismo punto simultáneamente, el resultado era una cima aún más alta, y si dos valles llegaban al mismo punto simultáneamente, el resultado era un valle aún más profundo. Young se sintió particularmente fascinado, porque los patos le recordaron un experimento sobre la naturaleza de la luz que había realizado en 1799.

En aquel experimento, Young había hecho brillar una luz sobre una mampara en la que había dos estrechas aberturas verticales, tal como se muestra en la Figura 71 (a). En una pantalla situada a cierta distancia detrás de las aberturas, Young esperaba ver dos rayas brillantes, proyecciones de las aberturas. En vez de ello,

observó que la luz se desplegaba desde las dos aberturas y formaba un patrón de varias rayas de luz y rayas oscuras sobre la pantalla. El patrón rayado de luz sobre la pantalla lo había desconcertado, pero ahora creía poder explicarlo completamente en función de lo que había visto en el estanque de los patos.

Young comenzó suponiendo que la luz era un tipo de onda. Si la luz que emanaba de las dos aberturas se comportaba como las ondas, entonces era igual que las estelas que quedaban tras los dos patos. Además, las rayas de luz y oscuridad sobre la pantalla eran causadas por las mismas interacciones que causaban que las olas formaran cimas más altas, valles más profundos y partes en calma. Young imaginó puntos de la pantalla en los que se juntaba un valle con una cima, resultando en cancelación y, por tanto, una raya oscura, y puntos de la pantalla en los que se juntaban dos cimas (o dos valles), resultando en reforzamiento y, por tanto, una raya luminosa, tal como se muestra en la Figura 71 (b). Los patos le habían proporcionado a Young una comprensión más profunda de la verdadera naturaleza de la luz y posteriormente publicaría «La teoría ondulatoria de la luz», un clásico sin antecedentes entre los artículos de física.

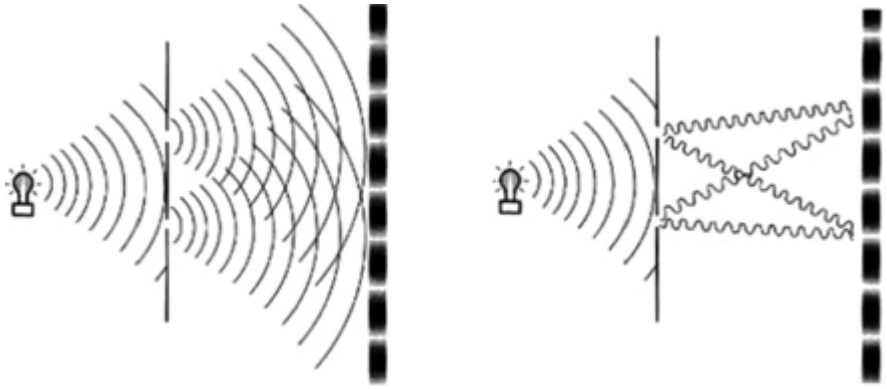


Figura 71. El experimento de Young con las aberturas vistas desde arriba. El diagrama (a) muestra la luz desplegándose desde las dos aberturas de la mampara, mezclándose y creando un patrón rayado sobre la pantalla. El diagrama (b) muestra cómo se mezclan *las ondas individuales. Si un valle se junta con una cima en la pantalla, el resultado es una raya oscura. Si dos valles (o dos cimas) se juntan en la pantalla, el resultado es una raya luminosa.*

Hoy día sabemos que la luz se comporta efectivamente como una onda, pero

sabemos que también puede comportarse como una partícula. Que percibamos la luz como una onda o como una partícula depende de las circunstancias, y esta ambigüedad de la luz se conoce como la dualidad onda- partícula. No necesitamos hablar más de esta dualidad, excepto mencionar que la física moderna considera que un rayo de luz consta de innumerables partículas individuales, conocidas como fotones, que presentan propiedades como de onda. Considerado así, podemos interpretar el experimento de Young en términos de fotones que se desbordan por las aberturas y luego reaccionan entre sí al otro lado de la mampara.

Young comenzó suponiendo que la luz era un tipo de onda. Si la luz que emanaba de las dos aberturas se comportaba como las ondas, entonces era igual que las estelas que quedaban tras los dos patos. Además, las rayas de luz y oscuridad sobre la pantalla eran causadas por las mismas interacciones que causaban que las olas formaran cimas más altas, valles más profundos y partes en calma. Young imaginó puntos de la pantalla en los que se juntaba un valle con una cima, resultando en cancelación y, por tanto, una raya oscura, y puntos de la pantalla en los que se juntaban dos cimas (o dos valles), resultando en reforzamiento y, por tanto, una raya luminosa, tal como se muestra en la Figura 71 (b). Los patos le habían proporcionado a Young una comprensión más profunda de la verdadera naturaleza de la luz y posteriormente publicaría «La teoría ondulatoria de la luz», un clásico sin antecedentes entre los artículos de física.

Hoy día sabemos que la luz se comporta efectivamente como una onda, pero sabemos que también puede comportarse como una partícula. Que percibamos la luz como una onda o como una partícula depende de las circunstancias, y esta ambigüedad de la luz se conoce como la dualidad onda- partícula. No necesitamos hablar más de esta dualidad, excepto mencionar que la física moderna considera que un rayo de luz consta de innumerables partículas individuales, conocidas como fotones, que presentan propiedades como de onda. Considerado así, podemos interpretar el experimento de Young en términos de fotones que se desbordan por las aberturas y luego reaccionan entre sí al otro lado de la mampara.

Hasta ahora, no hay nada de particular en el experimento de Young. Sin embargo, la tecnología moderna permite a los físicos repetir el experimento de Young utilizando un filamento que es tan tenue que emite fotones únicos de luz. Los

fotones son producidos a un ritmo de, pongamos, uno por minuto y cada fotón viaja solo hacia la mampara. A veces, un fotón pasará por una de las aberturas e irá a dar en la pantalla. Aunque nuestros ojos no son lo suficientemente sensibles para ver los fotones individuales, éstos pueden ser observados con ayuda de un detector especial, y en un período de varias horas podríamos obtener una imagen general de dónde están tocando los fotones la pantalla. Con sólo un fotón pasando cada vez por las aberturas no esperaríamos ver el patrón rayado observado por Young, porque ese fenómeno parece depender de que dos fotones atraviesen simultáneamente aberturas diferentes y se mezclen al otro lado. En vez de ello, podríamos esperar ver sólo dos rayas de luz, que serían simplemente la proyección de las aberturas de la mampara. Sin embargo, por alguna razón extraordinaria, incluso con fotones únicos el resultado sobre la pantalla sigue siendo un patrón de rayas de luz y oscuridad, igual que si los fotones hubieran estado mezclándose.

Este extraño resultado desafía el sentido común. No hay manera de explicar el fenómeno en función de las leyes clásicas de la física, es decir, las leyes tradicionales que se formularon para explicar cómo se comportan los objetos cotidianos. La física clásica puede explicar las órbitas de los planetas o la trayectoria de una bala de cañón, pero no puede describir completamente el mundo de lo verdaderamente diminuto, como la trayectoria de un fotón. Para explicar semejantes fenómenos de los fotones, los físicos recurren a la teoría cuántica, una explicación de cómo se comportan los objetos a nivel microscópico. Sin embargo, incluso los físicos cuánticos no se pueden poner de acuerdo sobre cómo interpretar este experimento. Tienden a dividirse en dos bandos opuestos, cada uno con su propia interpretación.

El primer bando propone una idea conocida como *superposición.* Los superposicionistas comienzan afirmando que sólo sabemos con seguridad dos cosas sobre el fotón: que sale del filamento y que va a dar a la pantalla. Todo lo demás es un completo misterio, incluido si el fotón pasó por la abertura izquierda o por la derecha. Como la trayectoria del fotón es desconocida, los superposicionistas adoptan el peculiar punto de vista de que, de alguna forma, el fotón pasa por las dos aberturas simultáneamente, lo que le permite interferir consigo mismo y crear el patrón rayado que se observa en la pantalla. ¿Pero cómo puede un fotón pasar

por las dos aberturas? Los argumentos de los superposicionistas son del siguiente tipo. Si no sabemos lo que está haciendo una partícula, entonces puede hacer cualquier cosa posible simultáneamente. En el caso del fotón, no sabemos si pasó por la abertura izquierda o por la derecha, de modo que asumimos que pasó por las dos aberturas al mismo tiempo. Cada posibilidad se denomina un *estado,* y como el fotón cumple ambas posibilidades, se dice que está en una *superposición de estados.* Sabemos que un fotón salió del filamento y que un fotón tocó la pantalla al otro lado de la mampara, pero entre medio de alguna forma se dividió en dos «fotones fantasmas» que pasaron por ambas aberturas. Puede que la superposición suene ridícula, pero al menos explica el patrón rayado que resulta del experimento de Young realizado con fotones individuales. En cambio, el anticuado punto de vista clásico es que el fotón debe haber pasado por una de las dos aberturas, y simplemente no sabemos por cuál; esto parece mucho más sensato que el punto de vista cuántico, pero por desgracia no puede explicar el resultado final.

Erwin Schrödinger, que obtuvo el premio Nobel de Física en 1933, inventó una parábola conocida como «El gato de Schrödinger», que a menudo se utiliza para ayudar a explicar el concepto de superposición. Imagine un gato en una caja. Hay dos estados posibles en que puede estar el gato, a saber, vivo o muerto. Inicialmente, sabemos que el gato está definitivamente en un estado en particular, porque podemos ver que está vivo. En ese momento, el gato no está en una superposición de estados. A continuación, ponemos un frasco de cianuro en la caja, junto al gato, y tapamos la caja. Ahora entramos en un período de ignorancia, porque no podemos ver o medir el estado del gato. ¿Está todavía vivo, o ha pisado el frasco de cianuro y ha muerto? Tradicionalmente, diríamos que el gato está vivo o muerto, simplemente no sabemos cuál de los dos. Sin embargo, la teoría cuántica dice que el gato está en una superposición de dos estados: está tanto vivo como muerto, reúne todas las posibilidades. La superposición sucede sólo cuando perdemos de vista un objeto y es una manera de describir un objeto durante un período de ambigüedad. La acción de mirar al gato lo obliga a estar en un estado en particular, y en ese mismo momento la superposición desaparece.

Para los lectores que se sientan incómodos con la superposición está el segundo bando cuántico, a favor de una interpretación diferente del experimento de Young.

Desgraciadamente, este punto de vista alternativo es igual de extraño. *La interpretación de los mundos múltiples* afirma que al salir del filamento el fotón tiene dos opciones — pasar por la abertura izquierda o por la derecha— y en ese momento el universo se divide en dos universos, y en un universo el fotón pasa por la abertura izquierda y en el otro el fotón pasa por la abertura derecha. Estos dos universos interfieren de alguna forma entre sí, lo que explica el patrón rayado. Los seguidores de la interpretación de los mundos múltiples creen que cada vez que un objeto tiene el potencial de entrar en uno entre varios estados posibles, el universo se divide en muchos universos, de modo que cada potencial se realiza en un universo diferente. Esta proliferación de universos se denomina el *multiverso.*

Adoptemos la interpretación de la superposición o la de los mundos múltiples, la teoría cuántica es una filosofía desconcertante. Sin embargo, ha demostrado ser la teoría científica más práctica y con más éxito jamás concebida. Además de su capacidad única para explicar el resultado del experimento de Young, la teoría cuántica explica satisfactoriamente muchos otros fenómenos. Sólo la teoría cuántica permite a los físicos calcular las consecuencias de las reacciones nucleares en las centrales eléctricas; sólo la teoría cuántica puede explicar el milagro del ADN; sólo la teoría cuántica puede explicar cómo brilla el sol; sólo la teoría cuántica se puede utilizar para diseñar el láser que lee los CD en su estéreo. Así que, nos guste o no, vivimos en un mundo cuántico.

De todas las consecuencias de la teoría cuántica, la más importante tecnológicamente es potencialmente el ordenador cuántico. Además de eliminar la seguridad de todas las cifras modernas, el ordenador cuántico anunciaría una nueva era de potencia informática. Uno de los pioneros de la informática cuántica es David Deutsch, un físico inglés que comenzó a trabajar con ese concepto en 1984, cuando asistió a un congreso sobre la teoría de la computación. Mientras escuchaba una ponencia del congreso, Deutsch vio algo que hasta entonces se había pasado por alto. La suposición tácita era que todos los ordenadores funcionaban esencialmente según las leyes de la física clásica, pero Deutsch estaba convencido de que en vez de ello los ordenadores deberían obedecer las leyes de la física cuántica, porque las leyes cuánticas son más fundamentales.

Figura 72. David Deutsch

Los ordenadores corrientes funcionan en un nivel relativamente macroscópico, y en ese nivel las leyes cuánticas y las leyes clásicas son casi indistinguibles. Por tanto, no importaba que los científicos generalmente hubiesen considerado los ordenadores corrientes desde el punto de vista de la física clásica. Sin embargo, a nivel microscópico, los dos conjuntos de leyes divergen, y en ese nivel sólo las leyes de la física cuántica siguen siendo válidas. En el nivel microscópico, las leyes cuánticas se nos muestran en su verdadero misterio y un ordenador construido para sacar partido a estas leyes se comportaría de una manera drásticamente nueva. Después del congreso, Deutsch volvió a casa y comenzó a rehacer la teoría de los ordenadores a la luz de la física cuántica. En un artículo publicado en 1985 describió su visión de un ordenador cuántico que funcionara de acuerdo a las leyes de la física cuántica. En particular, explicó en qué se diferenciaba su ordenador cuántico de un ordenador corriente.

Imagine que tiene usted dos versiones de una pregunta. Para responder ambas preguntas utilizando un ordenador corriente, primero tendría que introducir la primera versión y esperar la respuesta y luego introducir la segunda versión y esperar la respuesta. En otras palabras, un ordenador corriente sólo puede tratar una pregunta cada vez, y si hay varias preguntas tiene que tratarlas secuencialmente. Sin embargo, con un ordenador cuántico, las dos preguntas se pueden combinar como una superposición de dos estados e introducirse simultáneamente: la máquina misma entraría entonces en una superposición de dos estados, uno para cada pregunta. O, según la interpretación de los mundos múltiples, la máquina entraría en dos universos diferentes y respondería cada pregunta en un universo diferente. Sea cual sea la interpretación, el ordenador cuántico puede tratar dos preguntas al mismo tiempo sacando partido a las leyes de la física cuántica.

Para hacernos alguna idea de la potencia de un ordenador cuántico, podemos comparar su rendimiento con el de un ordenador tradicional observando lo que sucede cuando usamos ambos para abordar un problema en particular. Por ejemplo, los dos tipos de ordenador podrían abordar el problema de encontrar un número cuyo cuadrado y cubo juntos utilicen todos los dígitos del 0 al 9 una sola vez. Si probamos el número 19, encontramos que $19^2 = 361$, y $19^3 = 6.859$. El número 19 no cumple el requisito, porque su cuadrado y su cubo sólo incluyen los dígitos: 1, 3, 5, 6, 6, 8, 9, es decir, faltan los dígitos 0, 2, 4 y 7, y además se repite el dígito 6.

Para resolver este problema con un ordenador tradicional, el operador tendría que adoptar el siguiente enfoque. El operador introduce el número 1 y deja que el ordenador lo pruebe. Una vez que el ordenador ha realizado los cálculos necesarios declara si el número satisface o no el criterio. El número 1 no satisface el criterio, de modo que el operador introduce el número 2 y deja que el ordenador realice otra prueba, y así sucesivamente, hasta que finalmente se encuentre el número apropiado. Resulta que la respuesta es 69, porque $69^2 = 4.761$, y $69^3 = 328.509$, y estos números incluyen efectivamente cada uno de los diez dígitos y sólo una vez. De hecho, 69 es el único número que satisface este requisito. Es evidente que este proceso requiere mucho tiempo, porque un ordenador tradicional sólo puede probar un número cada vez. Si al ordenador le cuesta un segundo probar cada número le

habría costado 69 segundos encontrar la respuesta. En cambio, un ordenador cuántico encontraría la respuesta en sólo 1 segundo.

El operador comienza representando los números de una manera especial para sacar partido al poder del ordenador cuántico. Una forma de representar los números es en términos de partículas giratorias, puesto que muchas partículas fundamentales poseen un giro inherente, y pueden girar hacia el este o hacia el oeste, como una pelota de tenis que gira en el extremo de un dedo. Cuando una partícula está girando hacia el este representa el 1, y cuando está girando hacia el oeste representa el 0. Por tanto, una secuencia de partículas giratorias representa una secuencia de unos y de ceros, o un número binario. Por ejemplo, siete partículas, girando este, este, oeste, este, oeste, oeste, oeste respectivamente, juntas representan el número binario 1101000, que equivale al número decimal 104. Dependiendo de sus giros, una combinación de siete partículas puede representar cualquier número entre 0 y 127.

Con un ordenador tradicional, el operador introduciría una secuencia particular de giros, como oeste, oeste, oeste, oeste, oeste, oeste, este, que representa 0000001, que es simplemente el número digital 1. El operador esperaría entonces a que el ordenador probase el número para ver si cumplía el criterio mencionado. A continuación, el operador introduciría 0000010, que sería una secuencia de partículas giratorias que representan el 2, y así sucesivamente. Como antes, los números tendrían que ser introducidos uno cada vez, lo que ya sabemos que requiere mucho tiempo. Sin embargo, si se trata de un ordenador cuántico, el operador cuenta con una manera alternativa de introducir los números que es mucho más rápida. Como cada partícula es fundamental obedece las leyes de la física cuántica. Por consiguiente, cuando una partícula no está siendo observada puede entrar en una superposición de estados, lo que significa que está girando en ambas direcciones al mismo tiempo, de modo que está representado 0 y 1 al mismo tiempo. De manera alternativa, podemos considerar que la partícula entra en dos universos diferentes: en un universo gira hacia el este y representa el 1 mientras que en el otro gira hacia el oeste y representa el 0.

La superposición se logra de la siguiente manera. Imagine que podemos observar una de las partículas y está girando hacia el oeste. Para cambiar su giro lanzaríamos

una pulsación de energía lo suficientemente poderosa como para hacer que la partícula gire hacia el este. Si lanzásemos una pulsación más débil, unas veces tendríamos suerte y la partícula modificaría su giro, y otras veces no tendríamos suerte y la partícula seguiría girando hacia el oeste. Hasta ahora, la partícula estaba claramente a la vista y hemos podido seguir sus movimientos. Sin embargo, si la partícula está girando hacia el oeste y está en una caja donde no la podemos ver, y le lanzamos una pulsación de energía débil, entonces no tenemos ni idea de si su giro ha cambiado. La partícula entra en una superposición de giros hacia el este y hacia el oeste, igual que el gato entraba en una superposición de estar muerto y estar vivo. Si tomamos siete partículas que giren hacia el oeste, las ponemos en una caja y les lanzamos siete pulsaciones de energía débiles las siete partículas entran en una superposición.

Al estar las siete partículas en superposición representan de hecho todas las combinaciones posibles de giros hacia el este y hacia el oeste. Las siete partículas representan simultáneamente 128 estados diferentes o 128 números diferentes. El operador introduce las siete partículas, mientras están aún en una superposición de estados, en el ordenador cuántico, que realiza entonces sus cálculos como si estuviera probando los 128 números simultáneamente. Después de un segundo, el ordenador ofrece el número, 69, que cumple el criterio requerido. El operador obtiene 128 cálculos por el precio de uno.

Un ordenador cuántico desafía el sentido común. Ignorando los detalles por un momento, un ordenador cuántico se puede considerar de dos maneras diferentes, dependiendo de qué interpretación cuántica se prefiera. Algunos físicos consideran el ordenador cuántico como una única entidad que realiza el mismo cálculo simultáneamente con 128 números. Otros lo consideran como 128 entidades, cada una de ellas en un universo diferente y cada una realizando sólo un cálculo. La informática cuántica es tecnología de *La zona oscura (Twilight Zone).*

Cuando los ordenadores tradicionales funcionan con 1s y 0s, los 1s y 0s se denominan bits, que es una abreviatura de «dígitos binarios». Como un ordenador cuántico funciona con 1s y 0s que están en una superposición cuántica se denominan bits cuánticos, o *qubits* [26]. La ventaja de los qubits queda aún más de

[26] Qubit: término creado por Schumacher en 1995, como abreviatura de quantum bit (bit cuántico).

manifiesto cuando consideramos más partículas. Con 250 partículas giratorias, o 250 qubits, es posible representar aproximadamente 10^{75} combinaciones, que es un número mayor que el de los átomos del universo. Si fuera posible lograr la superposición apropiada con 250 partículas, un ordenador cuántico podría realizar 10^{75} computaciones simultáneas, completándolas todas en un solo segundo.

Sacar partido a los efectos cuánticos podría dar lugar a ordenadores cuánticos de una potencia inimaginable. Por desgracia, cuando Deutsch creó su visión de un ordenador cuántico a mediados de los años ochenta, nadie podía imaginar cómo construir una máquina sólida, práctica, con esas características. Por ejemplo, los científicos no podían construir nada que pudiera calcular con partículas giratorias en una superposición de estados. Uno de los mayores obstáculos era mantener una superposición de estados a lo largo de todo el cálculo. Una superposición existe sólo cuando no está siendo observada, pero una observación en el sentido más general incluye cualquier interacción con cualquier cosa externa a la superposición. Un solo átomo disperso que interfiriese con una de las partículas giratorias rompería la superposición llevándola a un solo estado, haciendo que fracasara el cálculo cuántico.

Otro problema era que los científicos no sabían cómo programar un ordenador cuántico y, por tanto, no estaban seguros de qué tipo de cómputos podría ser capaz de realizar. Sin embargo, en 1994, Peter Shor, de los laboratorios AT&T Bell en Nueva Jersey, logró definir un programa útil para un ordenador cuántico. La noticia extraordinaria para los criptoanalistas era que el programa de Shor definía una serie de pasos que un ordenador cuántico podía seguir para factorizar un número gigante, justo lo que se requería para romper la cifra RSA. Cuando Martin Gardner planteó su desafío RSA en la revista *Scientific American,* seiscientos ordenadores necesitaron varios meses para factorizar un número de 129 dígitos. En cambio, el programa de Shor podía factorizar un número un millón de veces mayor en una millonésima del tiempo.

Desgraciadamente, Shor no podía demostrar su programa de factorización porque todavía no existía nada parecido a un ordenador cuántico.

Después, en 1996, Lov Grover, también de los laboratorios Bell, descubrió otro poderoso programa. El programa de Grover es una forma de buscar una lista a una

velocidad increíblemente alta, lo que puede que no suene particularmente interesante hasta que uno se da cuenta de que eso es exactamente lo que se requiere para descifrar una cifra DES. Para romper una cifra DES es necesario buscar una lista de todas las claves posibles para encontrar la correcta. Si un ordenador convencional puede probar un millón de claves por segundo le costará más de mil años romper una cifra DES, mientras que un ordenador cuántico que utilice el programa de Grover podría encontrar la clave en menos de cuatro minutos. Es una mera coincidencia que los dos primeros programas para ordenador cuántico que se han inventado hayan sido exactamente lo que los criptoanalistas habrían puesto en primer lugar en su lista de deseos. Aunque los programas de Shor y Grover produjeron un optimismo enorme entre los descifradores, hubo también una inmensa frustración, porque todavía no existía tal cosa como un ordenador cuántico operativo que pudiera hacer funcionar estos programas. No sorprenderá que el potencial de esta arma suprema de la tecnología de descodificación haya estimulado el apetito de organizaciones como las norteamericanas DARPA (Defense Advanced Research Projects Agency, Agencia de proyectos avanzados de investigación de defensa) y el Laboratorio Nacional de Los Álamos, que están tratando desesperadamente de construir aparatos que puedan manejar qubits, de la misma manera que los chips de silicona pueden manejar bits. Aunque varios avances recientes han subido la moral de los investigadores, puede decirse que la tecnología sigue siendo notablemente primitiva. En 1998, Serge Haroche, de la Universidad de París VI, puso en su perspectiva correcta la propaganda exagerada que rodeaba a los avances cuando disipó las afirmaciones de que un ordenador cuántico real estaba sólo a unos pocos años de distancia. Haroche dijo que esto era como montar concienzudamente el primer nivel de un castillo de naipes y jactarse de que los siguientes 15.000 niveles son una mera formalidad.

Sólo el tiempo dirá si se pueden superar los problemas de construir un ordenador cuántico, y de ser así, cuándo. Mientras tanto, lo único que podemos hacer es especular sobre el impacto que tendría en el mundo de la criptografía. Desde los años setenta, los creadores de cifras han llevado una clara delantera en la carrera contra los descifradores, gracias a cifras como DES y RSA. Estos tipos de cifras son un recurso muy valioso, porque hemos llegado a confiar en ellas para codificar

nuestros *e-mails* y proteger nuestra privacidad. De manera similar, según entramos en el siglo XXI, más y más comercio se llevará a cabo en Internet, y el mercado electrónico dependerá de cifras fuertes para proteger y verificar las transacciones financieras. Según la información se convierte en la mercancía más valiosa del mundo, el destino económico, político y militar de las naciones dependerá de la fortaleza de las cifras.

Por consiguiente, el desarrollo de un ordenador cuántico totalmente operativo pondría en peligro nuestra privacidad personal, destruiría el comercio electrónico y demolería el concepto de la seguridad nacional. Un ordenador cuántico haría peligrar la estabilidad del mundo. El país que primero lo consiga podrá vigilar las comunicaciones de sus ciudadanos, leer la mente de sus rivales comerciales y enterarse de los planes de sus enemigos. Aunque aún está en pañales, la informática cuántica presenta una amenaza potencial al individuo, los negocios internacionales y la seguridad global.

2. La criptografía cuántica

Mientras los criptoanalistas esperan la llegada de los ordenadores cuánticos, los criptógrafos están ocupándose de su propio milagro tecnológico: un sistema de cifrado que restablecería la privacidad, incluso si tuviera que hacer frente a la fuerza de un ordenador cuántico. Esta nueva forma de codificación es fundamentalmente diferente a cualquiera de las que hemos visto anteriormente, ya que ofrece la esperanza de una privacidad perfecta. En otras palabras, este sistema no tendría ningún defecto y garantizaría una seguridad absoluta para toda la eternidad. Además, se basa en la teoría cuántica, la misma que constituye el fundamento de los ordenadores cuánticos. De modo que mientras la teoría cuántica constituye la inspiración para un ordenador que podría descifrar todas las cifras actuales está también en el centro de una nueva cifra indescifrable denominada *criptografía cuántica.*

La historia de la criptografía cuántica se remonta a una curiosa idea desarrollada a finales de los años sesenta por Stephen Wiesner, que en aquellos momentos era un estudiante graduado en la Universidad de Columbia (Nueva York).

Lamentablemente, la desgracia de Wiesner fue inventar una idea que se anticipaba

tanto a su tiempo que nadie se la tomó en serio. Todavía recuerda la reacción de sus superiores: «*No obtuve ningún apoyo del director de mi tesis doctoral —no mostró ningún interés en absoluto—. Se la mostré a varias otras personas y todos pusieron una cara rara, volviendo inmediatamente a lo que estaban haciendo*». Wiesner estaba proponiendo el extraño concepto del dinero cuántico, que tenía la gran ventaja de ser imposible de falsificar.

El dinero cuántico de Wiesner se basaba enormemente en la física de los fotones. Cuando un fotón viaja por el espacio, vibra, como se muestra en la Figura 73 (a). Los cuatro fotones viajan en la misma dirección, pero el ángulo de vibración es diferente en cada caso. El ángulo de vibración se conoce como la polarización del fotón, y una bombilla genera fotones con todas las polarizaciones, lo que significa que algunos fotones vibrarán hacia arriba y abajo, otros de un lado al otro y otros en ángulos intermedios. Para simplificar, supondremos que los fotones sólo tienen cuatro polarizaciones posibles, que denominaremos ↕, ↔, ↘, y ↙.

Colocando un filtro, conocido como un Polaroid, en la trayectoria de los fotones, es posible asegurar que el rayo de luz que sale se compone de fotones que vibran en una dirección particular; en otras palabras, todos los fotones tienen la misma polarización. Hasta cierto punto, podemos considerar el filtro Polaroid como un enrejado y los fotones como cerillas esparcidas al azar sobre el enrejado. Las cerillas sólo pasarán por el enrejado si están en el ángulo correcto. Cualquier fotón que ya esté polarizado en la misma dirección del filtro Polaroid pasará automáticamente por él sin modificarse y los fotones que estén polarizados perpendicularmente al filtro quedarán bloqueados.

Desgraciadamente, la analogía de las cerillas se viene abajo cuando consideramos los fotones polarizados diagonalmente que se acercan a un filtro Polaroid vertical. Aunque las cerillas orientadas diagonalmente quedarían bloqueadas por un enrejado vertical, esto no es necesariamente así en el caso de los fotones polarizados diagonalmente que se acercan a un filtro Polaroid vertical. De hecho, los fotones polarizados diagonalmente están en un dilema cuántico cuando afrontan un filtro Polaroid vertical. Lo que sucede es que, al azar, la mitad de ellos quedará bloqueada y la otra mitad pasará, y los que pasen estarán reorientados con una polarización vertical. La Figura 73(b) muestra ocho fotones que se aproximan a un filtro Polaroid

vertical y la Figura 73(c) muestra que sólo cuatro de ellos han logrado pasar por el filtro. Todos los fotones polarizados verticalmente han pasado, todos los fotones polarizados horizontalmente han quedado bloqueados y la mitad de los fotones polarizados diagonalmente ha pasado.

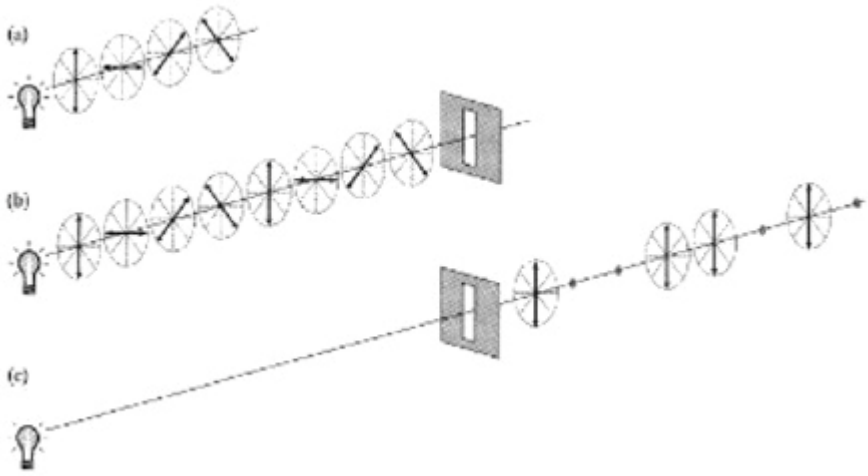


Figura 73. (a) Aunque los fotones de luz vibran en todas las direcciones, para simplificar suponemos que sólo hay cuatro direcciones, como se muestra e» este diagrama, (b) La lámpara ha emitido ocho fotones, que vibran en varias direcciones. Se dice que cada fotón tiene una polarización, Los fotones se dirigen hacia un filtro Polaroid vertical, (e) Al otro lado del filtro, sólo la mitad de los fotones ha sobrevivido. Los fotones polarizados verticalmente han pasado y los fotones polarizados horizontal mente no. La mitad de los fotones polarizados diagonalmente han pasado y a partir de entonces están polarizados verticalmente.

Es esta habilidad para bloquear ciertos fotones lo que explica cómo funcionan las gafas de sol Polaroid. De hecho, usted mismo puede demostrar el efecto de los filtros Polaroid experimentando con unas gafas de sol Polaroid.

Primero, retire una de las lentes, y cierre ese ojo, de modo que sólo mire con el otro ojo por la lente que queda. Naturalmente, el mundo parece bastante oscuro, porque la lente bloquea muchos de los fotones que de otra forma llegarían a su ojo. En ese momento, todos los fotones que llegan a su ojo tienen la misma polarización. A continuación, ponga la otra lente delante de la lente por la que está mirando y hágala girar lentamente. En un momento dado de la rotación, la lente suelta no

tendrá ningún efecto sobre la cantidad de luz que llega a su ojo, porque su orientación es la misma que la de la lente fija; todos los fotones que pasan por la lente suelta pasan también por la lente fija. Si gira ahora la lente en un ángulo de 90° todo se volverá completamente oscuro. En esta configuración, la polarización de la lente suelta es perpendicular a la polarización de la lente fija, de modo que los fotones que pasan por la lente suelta son bloqueados por la lente fija. Si entonces gira la lente en un ángulo de 45° llegará a una fase intermedia en la que las lentes se bloquean parcialmente y la mitad de los fotones que pasan por la lente suelta logran pasar por la lente fija.

Wiesner planeó usar la polarización de los fotones para crear billetes de dólar que nunca pudieran ser falsificados. Su idea era que los billetes de dólar contuvieran 20 trampas de luz, diminutos aparatos que son capaces de capturar y retener un fotón.

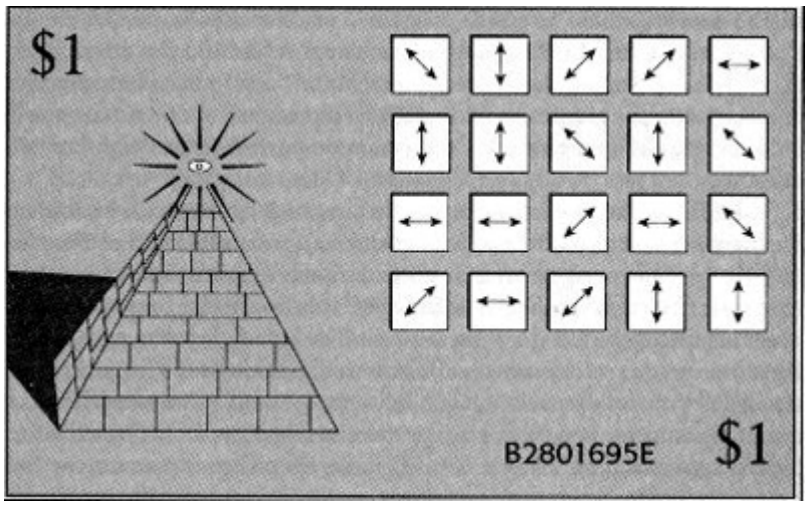
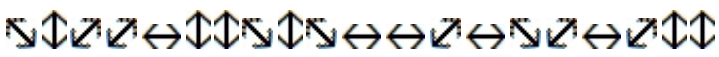


Figura 74. El dinero cuántico de Stephen Wiesner. Cada billete es único a causa de su número de serie, que puede verse fácilmente, y las 20 trampas de luz, cuyo contenido es un misterio. Las trampas de luz contienen fotones de varias polarizaciones. El banco conoce la secuencia de polarizaciones que corresponde a cada número de serie, pero un falsificador, no.

Wiesner sugirió que los bancos podrían utilizar cuatro filtros Polaroid orientados de cuatro maneras diferentes (↕, ↔, ↘ y ↙) para llenar las 20 trampas de luz con una secuencia de 20 fotones polarizados, usando una frecuencia diferente para cada billete. Por ejemplo, la Figura 74 muestra un billete con la secuencia de polarización



Aunque las polarizaciones se muestran explícitamente en la Figura 74, en realidad quedarían ocultas a la vista. Cada billete lleva también un número de serie convencional, que en el billete mostrado es B2801695E. El banco emisor puede identificar cada billete según su secuencia de polarización y su número de serie impreso, y guardaría una lista maestra de los números de serie y las correspondientes secuencias de polarización.

Un falsificador se enfrenta a un problema; no puede simplemente falsificar un billete que lleve un número de serie arbitrario y una secuencia de polarización aleatoria en las trampas de luz, porque este emparejamiento no aparece en la lista maestra del banco, y el banco descubrirá que el billete es falso. Para crear una falsificación eficaz, el falsificador debe usar un billete genuino como muestra, precisar de alguna manera sus 20 polarizaciones y luego duplicar el billete, reproduciendo el número de serie y cargando las trampas de luz de la forma apropiada. Sin embargo, precisar las polarizaciones de los fotones es una tarea notoriamente difícil, y si el falsificador no puede precisarlas exactamente en el billete de muestra no puede esperar duplicarlas.

Para comprender la dificultad de precisar la polarización de los fotones necesitamos considerar qué tendríamos que hacer para intentar realizar semejante medición. La única manera de aprender algo sobre la polarización de un fotón es utilizando un filtro Polaroid. Para precisar la polarización del fotón en una trampa de luz en particular, el falsificador selecciona un filtro Polaroid y lo orienta de un modo en particular, pongamos verticalmente, ↕. Si da la casualidad de que el fotón que sale de la trampa de luz está polarizado verticalmente pasará por el filtro Polaroid vertical y el falsificador supondrá acertadamente que se trata de un fotón polarizado verticalmente. Si el fotón que sale está polarizado horizontalmente no pasará por el filtro Polaroid vertical y el falsificador supondrá correctamente que se trata de un fotón polarizado horizontalmente. Sin embargo, si el fotón que sale está polarizado diagonalmente (↘ o ↗) podría pasar por el filtro o podría no hacerlo, y en ambos casos el falsificador no podrá identificar su verdadera naturaleza. Un fotón ↘ podría

pasar por el filtro Polaroid vertical, en cuyo caso el falsificador supondría erróneamente que se trata de un fotón polarizado verticalmente, o el mismo fotón podría no pasar por el filtro, en cuyo caso el falsificador supondría erróneamente que se trata de un fotón polarizado horizontalmente. De manera alternativa, si el falsificador decide precisar el fotón en otra trampa de luz orientando el filtro diagonalmente, pongamos esto identificaría correctamente la naturaleza de un fotón polarizado diagonalmente, pero no podría identificar con exactitud un fotón polarizado vertical u horizontalmente.

El problema del falsificador es que debe utilizar la orientación correcta del filtro Polaroid para identificar la polarización de un fotón, pero no sabe qué orientación usar porque no conoce la polarización del fotón. Este círculo vicioso es una parte inherente de la física de los fotones. Imagine que el falsificador elige un filtro ↘ para precisar el fotón que sale de la segunda trampa de luz y que el fotón no pasa por el filtro. El falsificador puede estar seguro de que el fotón no estaba polarizado en dirección ↘ porque ese tipo de fotón habría pasado por el filtro. Sin embargo, el falsificador no puede decir si el fotón estaba polarizado en dirección ↗, con lo que ciertamente no habría pasado por el filtro, o si lo estaba en dirección ↕ o en ↔, cada una de las cuales le daba un cincuenta por ciento de posibilidades de quedar bloqueado.

La dificultad de precisar fotones es un aspecto del principio de incertidumbre (también denominado «de indeterminación»), desarrollado por el físico alemán Werner Heisenberg en los años veinte. Heisenberg sintetizó esta proposición altamente técnica en una simple declaración: «*Como principio, no podemos conocer el presente en todos sus detalles*». Esto no significa que no podamos saberlo todo porque no tenemos el suficiente equipo de medición, o porque nuestro equipo esté mal diseñado. Lo que Heisenberg estaba realmente diciendo es que es lógicamente imposible precisar todos los aspectos de un objeto particular con toda exactitud. En este caso concreto, no podemos precisar con toda exactitud todos los aspectos de los fotones que hay en las trampas de luz. El principio de incertidumbre es otra extraña consecuencia de la teoría cuántica.

El dinero cuántico de Wiesner se basaba en el hecho de que falsificar es un proceso de dos fases: primero, el falsificador necesita precisar el billete original con gran

exactitud y luego tiene que duplicarlo. Al incorporar fotones en el diseño del billete, Wiesner estaba imposibilitando la medición exacta del billete y, por tanto, creando un obstáculo para la falsificación.

Un falsificador ingenuo podría pensar que si él no podía precisar las polarizaciones de los fotones de las trampas de luz, entonces tampoco podría hacerlo el banco. Podría tratar de fabricar billetes llenando las trampas de luz con una secuencia arbitraria de polarizaciones. Sin embargo, el banco puede verificar si todos los billetes son genuinos. El banco mira el número de serie y consulta su lista maestra confidencial para ver qué fotón debería haber en cada trampa de luz. Como el banco sabe qué polarizaciones esperar en cada trampa de luz, puede orientar correctamente el filtro Polaroid para cada trampa de luz y realizar una medición exacta. Si el billete está falsificado, las polarizaciones arbitrarias del falsificador producirán unas mediciones incorrectas y se notará que el billete es una falsificación. Por ejemplo, si el banco utiliza un filtro ↕ para precisar lo que debería ser un fotón polarizado en ↕, pero encuentra que el filtro bloquea el fotón, sabe que un falsificador ha llenado la trampa de luz con un fotón erróneo. Sin embargo, si resulta que el billete es genuino, el banco vuelve a llenar las trampas de luz con los fotones apropiados y lo vuelve a poner en circulación.

Resumiendo, el falsificador no puede precisar las polarizaciones de un billete genuino porque no sabe qué tipo de fotón hay en cada trampa de luz y, por tanto, no puede saber cómo debe orientar el filtro Polaroid para precisarlo correctamente. Por otra parte, el banco puede examinar las polarizaciones de un billete genuino porque fue él quien eligió esas polarizaciones, de modo que sabe cómo orientar el filtro Polaroid para cada una de ellas.

El dinero cuántico es una idea brillante. Es también una idea totalmente inviable. Para empezar, los ingenieros todavía no han creado la tecnología para atrapar fotones en un estado polarizado particular durante un período de tiempo lo suficientemente largo. Incluso si existiera la tecnología resultaría demasiado caro ponerla en práctica. Costaría alrededor de 1 millón de dólares proteger cada billete de 1 dólar. A pesar de su inviabilidad, el dinero cuántico aplicaba la teoría cuántica de una manera fascinante e imaginativa, por lo que, a pesar de la falta de apoyo del director de su tesis doctoral, Wiesner envió un artículo a una revista científica. Se lo

rechazaron. Lo envió a otras tres revistas y fue rechazado otras tres veces. Wiesner afirma que simplemente no comprendían la física.

Parecía que sólo había una persona que compartía el entusiasmo de Wiesner por el dinero cuántico. Se trataba de un viejo amigo llamado Charles Bennett, que varios años antes había estudiado con él en la Universidad Brandeis. La curiosidad de Bennett por todos los aspectos de la ciencia es uno de los rasgos más notables de su personalidad. Dice que a los tres años ya sabía que quería ser científico, y su entusiasmo infantil por la materia no le pasó desapercibido a su madre. Un día, ella llegó a casa y encontró una olla con un extraño guiso hirviendo en la cocina. Por suerte, no se le ocurrió probarlo, ya que resultó contener los restos de una tortuga que el joven Bennett estaba cociendo en álcali para retirar la carne de los huesos y obtener así un espécimen perfecto de esqueleto de tortuga.

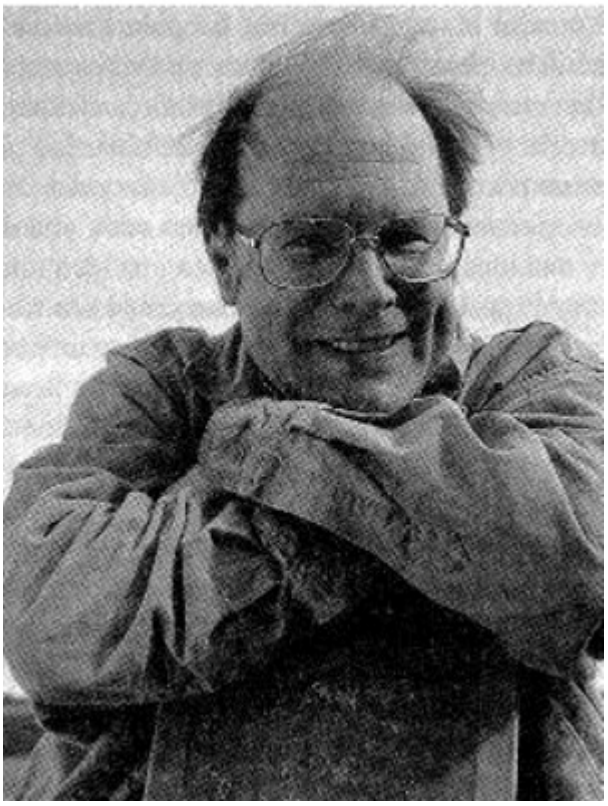


Figura 75. Charles Bennett

Durante su adolescencia, la curiosidad de Bennett pasó de la biología a la bioquímica, y para cuando llegó a la Universidad Brandeis había decidido

especializarse en química. En sus estudios de doctorado se centró en la química física y luego pasó a realizar investigación en física, matemáticas, lógica y, finalmente, informática.

Consciente de la amplia gama de intereses de Bennett, Wiesner confió en que él apreciaría el dinero cuántico y le entregó una copia de su manuscrito rechazado. A Bennett le fascinó inmediatamente el concepto y lo consideró una de las ideas más bellas que había visto. Durante la década siguiente releyó el manuscrito de vez en cuando, preguntándose si habría alguna manera de convertir algo tan ingenioso en algo que fuera también útil. Incluso cuando fue nombrado profesor investigador de los Laboratorios Thomas J. Watson de la IBM, Bennett aún no podía dejar de pensar en la idea de Wiesner. Puede que las revistas no quisieran publicarla, pero Bennett estaba obsesionado con ella.

Un día, Bennett le explicó el concepto del dinero cuántico a Gilies Brassard, un científico de la informática de la Universidad de Montreal. Bennett y Brassard, que habían colaborado en diversos proyectos de investigación, discutieron los detalles del artículo de Wiesner una y otra vez. Poco a poco empezaron a ver que la idea de Wiesner podría tener una aplicación en criptografía. Para que Eva descifre un mensaje cifrado entre Alicia y Benito, primero debe interceptarlo, lo que significa que de alguna manera debe percibir con exactitud el contenido de la transmisión. El dinero cuántico de Wiesner era seguro, porque resultaba imposible percibir con exactitud las polarizaciones de los fotones atrapados en los billetes. Bennett y Brassard se preguntaron qué sucedería si un mensaje cifrado fuera representado y transmitido mediante una serie de fotones polarizados. En teoría, parecía que Eva no podría leer con exactitud el mensaje cifrado y si no podía leer el mensaje cifrado, entonces no podría descifrarlo.

Bennett y Brassard comenzaron a crear un sistema basado en el siguiente principio. Imagine que Alicia quiere enviar a Benito un mensaje cifrado, que se compone de una serie de 1s y 0s. Alicia representa los 1s y los 0s enviando fotones con ciertas polarizaciones. Alicia tiene dos esquemas posibles para asociar las polarizaciones de los fotones con 1 o 0. En el primer esquema, denominado esquema *rectilíneo* o esquema +, Alicia envía ↕ para representar 1 y ↔ para representar 0. En el otro esquema, denominado esquema *diagonal* o esquema x, envía ⤢ para representar 1,

y ⤡ para representar 0. Para enviar un mensaje binario, pasa de un esquema al otro de manera imprevisible. Por tanto, el mensaje binario 1101101001 podría ser transmitido de la siguiente manera:

Mensaje	1	1	0	1	1	0	1	0	0	1
Esquema	+	×	+	×	×	×	+	+	×	×
Transmisión	↕	⤢	↔	⤢	⤢	⤡	↕	↔	⤡	⤢

Alicia transmite el primer 1 utilizando el esquema + y el segundo 1 utilizando el esquema x. Por consiguiente, en ambos casos se está transmitiendo 1, pero cada vez es representado por fotones polarizados de manera diferente.

Si Eva quiere interceptar este mensaje necesita identificar la polarización de cada fotón, igual que el falsificador necesitaba identificar la polarización de cada fotón en las trampas de luz del billete. Para precisar la polarización de cada fotón, Eva debe decidir cómo orientar su filtro Polaroid según se aproxima cada uno de ellos. No puede saber con seguridad qué esquema estará usando Alicia para cada fotón, de modo que su elección de filtro Polaroid será fortuita y, en la mitad de los casos, errónea. Por consiguiente, no puede tener un conocimiento completo de la transmisión Una manera más fácil de considerar el dilema de Eva es suponer que tiene dos tipos de detectores Polaroid a su disposición. El detector + es capaz de precisar con toda exactitud los fotones polarizados horizontal y verticalmente, pero no es capaz de precisar con certeza los fotones polarizados diagonalmente, y meramente los interpreta erróneamente como fotones polarizados vertical u horizontalmente. Por otra parte, el detector x puede precisar con toda exactitud los fotones polarizados diagonalmente, pero no es capaz de precisar con certeza los fotones polarizados horizontal y vertical mente y meramente los interpreta erróneamente como fotones polarizados diagonalmente. Por ejemplo, si utiliza el detector x para precisar el primer fotón, que es ↕, lo interpretará erróneamente como ⤡ o ⤢ Si lo interpreta erróneamente como ⤢, entonces no es problema, porque éste también representa 1, pero si lo interpreta erróneamente como ⤡ estará en dificultades, porque éste representa 0.

Para empeorar aún las cosas para Eva, sólo tiene una oportunidad para precisar con exactitud cada fotón Un fotón es indivisible, de modo que Eva no puede dividirlo en dos fotones y precisarlos utilizando ambos esquemas.

Este sistema parece tener algunos rasgos agradables. Eva no puede estar segura de estar interceptando con exactitud el mensaje cifrado, de modo que no puede tener esperanzas de descifrarlo. Sin embargo, el sistema tiene un problema grave y aparentemente insuperable: Benito se encuentra en la misma situación que Eva, en cuanto que no tiene ninguna manera de saber qué esquema de polarización está utilizando Alicia para cada fotón, de modo que también él interpretará erróneamente el mensaje. La solución obvia al problema es que Alicia y Benito se pongan de acuerdo sobre el esquema de polarización que usarán para cada fotón. Para el ejemplo anterior, Alicia y Benito compartirían una lista, o clave, que es

+x+xxx++xx

Sin embargo, volvemos al mismo viejo problema de la distribución de claves: de alguna forma, Alicia tiene que hacer llegar de manera segura a Benito la lista de los esquemas de polarización.

Por supuesto, Alicia podría cifrar la lista de esquemas utilizando una cifra de clave pública como RSA y luego transmitírsela a Benito. Sin embargo, imagine que ahora estamos en una era en la que RSA ha sido descifrada quizá a raíz del desarrollo de poderosos ordenadores cuánticos. El sistema de Bennett y Brassard tiene que ser autosuficiente y no depender de RSA. Durante meses, Bennett y Brassard trataron de pensar una forma de superar el problema de la distribución de la clave. Entonces, en 1984, un día estaban los dos en el andén de la estación Croton-Harmon, cerca de los Laboratorios Thomas J. Watson de la IBM. Estaban esperando el tren que llevaría a Brassard a Montreal y pasaban el tiempo charlando sobre las dificultades de Alicia, Benito y Eva. Si el tren hubiera llegado con unos minutos de antelación se habrían despedido sin realizar ningún avance en el problema de la distribución de claves. En vez de ello, en un momento de *¡eureka!* crearon la criptografía cuántica, la forma más segura de criptografía jamás concebida.

Su receta para la criptografía cuántica requiere tres fases preparatorias. Aunque

estas fases no conllevan enviar un mensaje cifrado sí permiten el intercambio seguro de una clave que luego se puede usar para cifrar un mensaje.

Fase 1. *Alicia comienza por transmitir una secuencia aleatoria de 1s y 0s (bits), utilizando una elección aleatoria de esquemas de polarización rectilíneos (horizontal y vertical) y diagonales. La Figura 76 muestra semejante secuencia de fotones en camino hacia Benito.*

Fase 2. *Benito tiene que precisar las polarizaciones de estos fotones. Como no tiene ni idea de qué esquema de polarización ha usado Alicia para cada uno de ellos alterna aleatoriamente entre su detector + y su detector x. Algunas veces, Benito elige el detector correcto y otras elige el erróneo. Si Benito usa el detector erróneo puede interpretar erróneamente el fotón de Alicia. La Tabla 27 cubre todas las posibilidades. Por ejemplo, en la línea superior, Alicia utiliza el esquema rectilíneo para enviar 1, por lo que transmite* ↕*; entonces Benito usa el detector correcto, por lo que detecta* ↕*, y anota correctamente 1 como primer bit de la secuencia. En la línea siguiente, Alicia hace lo mismo, pero Benito utiliza el detector incorrecto, de modo que podría detectar* ⤢ *o* ⤡ *lo que significa que podría anotar correctamente 1 o anotar erróneamente 0.*

Fase 3. *Hasta ese momento, Alicia ha enviado una serie de 1s y 0s, y Benito ha detectado algunos de ellos correctamente y otros erróneamente. Para aclarar la situación, Alicia llama por teléfono a Benito en una línea corriente y poco segura y le dice qué esquemas de polarización utilizó para cada fotón —pero no le dice cómo polarizó cada fotón —. De modo que podría decir que el primer fotón fue enviado usando el esquema rectilíneo, pero no dirá si lo envió* ↕ *o* ↔*. Benito le dice entonces en qué ocasiones ha adivinado el esquema de polarización correcto. En estas ocasiones precisó definitivamente la polarización correcta y anotó correctamente 1 o 0. Finalmente, Alicia y Benito ignoran todos los fotones para los que Benito utilizó el esquema*

erróneo y se centran tan sólo en aquellos para los que adivinó el esquema correcto. De hecho, han generado una secuencia más corta de bits, que se compone solamente de las mediciones correctas de Benito. Esta fase se ilustra en la Tabla que se incluye en la Figura 76.

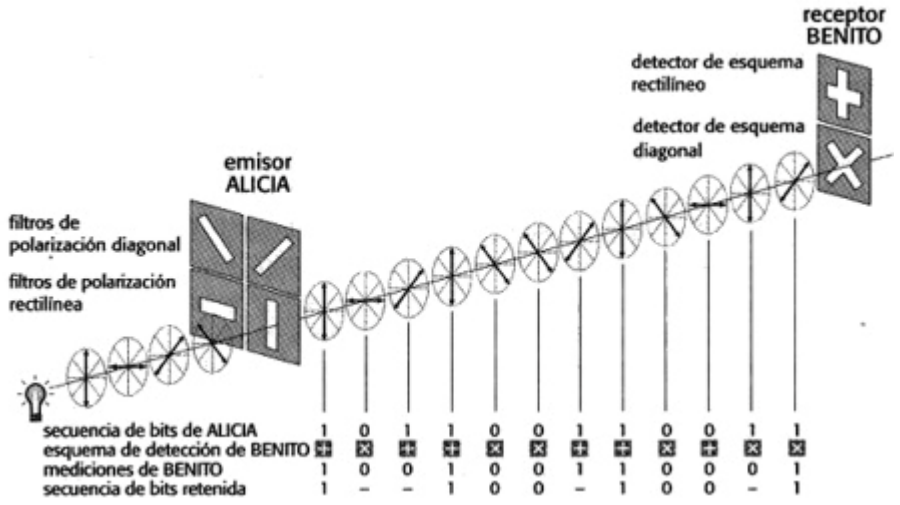


Figura 76. Alicia transmite una serie de 1s y 0s a Benito. Cada 1 y cada 0 es representado por un fotón polarizado, según el esquema de polarización rectilíneo (horizontal/vertical) o el esquema de polarización diagonal. Benito precisa cada fotón utilizando, bien su detector rectilíneo, bien su receptor diagonal. Elige el detector correcto para el fotón del extremo izquierdo y lo interpreta correctamente como 1. Sin embargo, elige el detector incorrecto para el siguiente fotón. Casualmente, lo interpreta correctamente como 0, pero, sin embargo, este bit es desechado posteriormente porque Benito no puede estar seguro de si lo ha medido correctamente.

Estas tres fases han permitido a Alicia y Benito establecer una serie común de dígitos, como la secuencia 11001001 acordada en la Figura 76. La propiedad crucial de esta secuencia es que es aleatoria, porque se deriva de la secuencia inicial de Alicia, que es en sí misma aleatoria. Además, las ocasiones en que Benito utiliza el detector correcto son también aleatorias. La secuencia acordada no constituye, por tanto, ningún mensaje, pero podría servir como clave aleatoria. Por fin, puede comenzar el verdadero proceso de cifrado seguro.

Tabla 27

Las diversas posibilidades del intercambio de fotones entre Alicia y Benito en la Fase 2

Esquema de Alicia	Bit de Alicia	Alicia envía	Detector de Benito	¿Detector correcto?	Benito detecta	Bit de Benito	¿Es correcto el bit de Benito?
Rectilíneo	1	↕	+	Sí	↕	1	Sí
			×	No	⤢	1	Sí
					⤡	0	No
	0	↔	+	Sí	↔	0	Sí
			×	No	⤢	1	No
					⤡	0	Sí
Diagonal	1	⤢	+	No	↕	1	Sí
					↔	0	No
			×	Sí	⤢	1	Sí
	0	⤡	+	No	↕	1	No
					↔	0	Sí
			×	Sí	⤡	0	Sí

Esta secuencia aleatoria acordada puede utilizarse como clave para una cifra de cuaderno de uso único. En el Capítulo 3 describí cómo una serie aleatoria de letras o números, el cuaderno de uso único, puede dar lugar a una cifra indescifrable; no sólo prácticamente indescifrable, sino absolutamente indescifrable.

Previamente, el único problema con la cifra de cuaderno de uso único era la dificultad de distribuir de una manera segura las series aleatorias, pero el plan de Bennett y Brassard resuelve este problema. Alicia y Benito han acordado un cuaderno de uso único y las leyes de la física cuántica no permiten que Eva lo intercepte con éxito. Éste es el momento de que nos pongamos en la situación de Eva y entonces veremos por qué no puede interceptar la clave.

Cuando Alicia transmite los fotones polarizados, Eva trata de precisarlos, pero no sabe si utilizar el detector + o el detector x. La mitad de las veces elegirá el detector erróneo. Esta es exactamente la misma situación en que se encuentra Benito, porque también él elige el detector erróneo la mitad de las veces. Sin embargo, después de la transmisión Alicia le dice a Benito qué esquema debería haber utilizado para cada fotón y acuerdan usar sólo los fotones que fueron medidos cuando Benito empleó el detector correcto. Sin embargo, esto no ayuda a Eva, porque ella habrá precisado la mitad de esos fotones usando el detector erróneo, de modo que habrá precisado erróneamente algunos de los fotones que constituyen la clave final.

Otra manera de entender la criptografía cuántica es considerándola desde el punto de vista de una baraja de cartas en vez de fotones polarizados. Cada carta tiene un valor y un palo, como la sota de copas o el seis de bastos, y normalmente podemos mirar una carta y ver tanto el valor como el palo al mismo tiempo. Sin embargo, imagine que sólo es posible precisar el valor o el palo, pero no ambos. Alicia toma una carta de la baraja y debe decidir si quiere precisar el valor o el palo. Supongamos que elige precisar el palo, que es «espadas», y lo anota. La carta es el cuatro de espadas, pero Alicia sólo sabe que es una espada. Entonces transmite la carta a Benito por una línea telefónica. Mientras esto está sucediendo, Eva trata de precisar la carta, pero por desgracia ella elige precisar el valor, que es «cuatro». Cuando la carta llega a Benito, éste decide precisar su palo, que es «espadas», y lo anota. Después, Alicia llama a Benito y le pregunta si ha precisado el palo, y lo hizo, de modo que Alicia y Benito saben ahora que comparten el mismo conocimiento común: ambos han escrito «espadas» en su cuaderno. Sin embargo, Eva ha escrito «cuatro», lo que no le sirve para nada.

A continuación, Alicia toma otra carta de la baraja, pongamos el rey de oros, pero de nuevo sólo puede precisar una propiedad. Esta vez elige precisar el valor, que es «rey», y transmite la carta a Benito por una línea telefónica. Eva intenta precisar la carta, y también ella elige precisar su valor, «rey». Cuando la carta llega a Benito, éste decide precisar el palo, que es «oros». Después, Alicia llama a Benito y le pregunta si ha precisado el valor de la carta y él tiene que admitir que adivinó erróneamente y precisó el palo. Esto no preocupa a Alicia y Benito, porque pueden

ignorar esta carta completamente e intentarlo de nuevo con otra carta elegida al azar. En esta última ocasión, Eva eligió correctamente, y precisó lo mismo que Alicia, «rey», pero la carta fue desechada porque Benito no la precisó correctamente. De modo que Benito no tiene que preocuparse por sus errores, porque Alicia y él pueden acordar ignorarlos, pero Eva está estancada con sus errores. Enviando varias cartas, Alicia y Benito pueden acordar una secuencia de palos y valores que luego pueden utilizar como base de algún tipo de clave.

La criptografía cuántica permite que Alicia y Benito acuerden una clave, y Eva no puede interceptar esta clave sin cometer errores. Además, la criptografía cuántica tiene una ventaja adicional: ofrece a Alicia y Benito una manera de descubrir si Eva está escuchando subrepticiamente. La presencia de Eva en la línea se evidencia porque cada vez que mide un fotón se arriesga a alterarlo, y estas alteraciones les resultan obvias a Alicia y Benito.

Imagine que Alicia envía ↘ y Eva lo precisa con el detector erróneo, el detector +. De hecho, el detector + fuerza al fotón entrante ↘ a salir como fotón ↕ o ↔ porque ésta es la única manera en que el fotón puede pasar por el detector de Eva. Si al recibir el fotón transformado Benito lo precisa con su detector x, entonces podría detectar ↘ que es lo que envió Alicia, o podría detectar ↗ que sería una medición errónea. Esto es un problema para Alicia y Benito, porque Alicia envió un fotón polarizado diagonalmente y Benito lo midió con el detector correcto, y, sin embargo, podría haberlo medido erróneamente. Resumiendo, cuando Eva elige el detector erróneo, «torcerá» algunos de los fotones y esto hará que Benito sea propenso a cometer errores, incluso cuando esté utilizando el detector correcto. Estos errores se pueden descubrir si Alicia y Benito realizan un breve proceso de revisión de errores.

La revisión de errores se lleva a cabo después de las tres fases preliminares, y para entonces Alicia y Benito deberían tener secuencias idénticas de 1s y 0s. Imagine que han establecido una secuencia que contiene 1.075 dígitos binarios. Una manera en que Alicia y Benito pueden revisar si sus respectivas secuencias coinciden sería que Alicia llame a Benito y le lea su propia secuencia completa. Por desgracia, si Eva está espiando podría interceptar la clave entera. Revisar la secuencia completa es obviamente poco aconsejable, y además es innecesario. En vez de ello, Alicia

simplemente tiene que elegir al azar 75 de los dígitos y revisar solamente éstos. Si los 75 dígitos coinciden con los de Benito, es muy improbable que Eva haya estado espiando durante la transmisión original de los fotones. De hecho, las posibilidades de que Eva esté en la línea y no afecte las mediciones de Benito de estos 75 dígitos son de menos de una en un billón Como Alicia y Benito han hablado abiertamente de estos 75 dígitos deben desecharlos, por lo que su cuaderno de uso único queda reducido de 1.075 a 1.000 dígitos binarios. Por otra parte, si Alicia y Benito encuentran una discrepancia entre los 75 dígitos sabrán que Eva ha estado espiando y tendrán que abandonar todo el cuaderno de uso único, cambiar a una nueva línea y empezar otra vez desde el principio.

Para resumir, la criptografía cuántica es un sistema que garantiza la seguridad de un mensaje dificultando que Eva pueda leer con exactitud una comunicación entre Alicia y Benito. Además, si Eva intenta escuchar subrepticiamente, Alicia y Benito podrán detectar su presencia. Por tanto, la criptografía cuántica permite que Alicia y Benito intercambien y acuerden un cuaderno de uso único con completa privacidad y luego pueden utilizarlo como clave para cifrar un mensaje. El procedimiento tiene cinco fases básicas:

1. Alicia envía a Benito una serie de fotones y Benito los precisa.
2. Alicia le dice a Benito en qué ocasiones los midió correctamente. (Aunque Alicia le esté diciendo a Benito cuando éste realizó la medición correcta, no le está diciendo cuál debería haber sido el resultado correcto, de modo que esta conversación puede ser «pinchada» sin que esto suponga ningún riesgo para la seguridad).
3. Alicia y Benito desechan las mediciones que Benito realizó erróneamente y se centran en las mediciones que hizo correctamente para crear un par idéntico de cuadernos de uso único.
4. Alicia y Benito prueban la integridad de sus cuadernos de uso único revisando algunos de los dígitos.
5. Si el proceso de verificación es satisfactorio pueden usar el cuaderno de uso único para cifrar un mensaje; si la verificación revela errores saben que los fotones estaban siendo interceptados por Eva y necesitan empezar de nuevo desde el principio.

Catorce años después de que el artículo de Wiesner sobre el dinero cuántico hubiera sido rechazado por las revistas científicas había inspirado un sistema de comunicación absolutamente seguro. Wiesner, que ahora vive en Israel, se siente aliviado de que, por fin, su trabajo esté siendo reconocido:

> *«Al mirar atrás, me pregunto si no hubiera podido sacarle más partido. Me han acusado de haberme rendido demasiado pronto, por no haber seguido intentando que publicaran mi idea —supongo que en cierta forma tienen razón—, pero entonces era un joven estudiante graduado, y no tenía demasiada confianza. De todas formas, nadie parecía estar interesado en el dinero cuántico».*

Los criptógrafos recibieron la criptografía cuántica de Bennett y Brassard con entusiasmo. Sin embargo, muchos experimentadores alegaron que el sistema funcionaba bien en teoría, pero que fracasaría en la práctica. Creían que la dificultad de tratar con fotones individuales haría que el sistema resultara imposible de poner en práctica. A pesar de las críticas, Bennett y Brassard estaban convencidos de que se podría hacer que la criptografía cuántica funcionara. De hecho, tenían tanta fe en su sistema que no se molestaron en construir el aparato. Como Bennett dijo una vez, «*no tiene sentido ir al polo norte si ya sabes que está ahí*».

Sin embargo, llegó un momento en que Bennett ya no aguantó más el creciente escepticismo y decidió demostrar que el sistema podía funcionar realmente. En 1988 comenzó a reunir los componentes que necesitaría para un sistema criptográfico cuántico y tomó un estudiante de investigación, John Smolin, para que lo ayudara a montar el aparato. Tras un año de esfuerzo, estaban listos para intentar enviar el primer mensaje protegido por la criptografía cuántica de la Historia. Un día, a última hora de la tarde, se retiraron a su laboratorio a prueba de luz, un ambiente completamente oscuro, protegido de fotones perdidos que pudieran interferir con el experimento. Como habían cenado abundantemente, estaban bien preparados para una larga noche haciendo ajustes al aparato. Se propusieron la tarea de intentar enviar fotones polarizados de un lado al otro de la habitación, para luego precisarlos utilizando un detector + y un detector x. Un

ordenador denominado Alicia controlaba la transmisión de fotones y un ordenador denominado Benito decidía qué detector debía utilizarse para precisar cada fotón.

Tras horas de ajustes, hacia las 3 de la mañana, Bennett presenció el primer intercambio criptográfico cuántico. Alicia y Benito lograron enviar y recibir fotones, discutieron los esquemas de polarización que había usado Alicia, desecharon los fotones que Benito había precisado utilizando el detector erróneo y acordaron un cuaderno de uso único consistente en los fotones restantes.

«Nunca tuve la menor duda de que funcionaría», recuerda Bennett, «lo único de lo que no estaba seguro es de si nuestros dedos podrían ser demasiado torpes para construirlo». El experimento de Bennett había demostrado que dos ordenadores, Alicia y Benito, se podían comunicar en absoluto secreto. Fue un experimento histórico, a pesar del hecho de que los dos ordenadores estuvieran a una distancia de sólo 30 cm Desde el experimento de Bennett, el desafío ha sido construir un sistema criptográfico cuántico que opere entre distancias útiles. Ésta no es una tarea insignificante, porque los fotones no viajan bien. Si Alicia transmite un fotón con una polarización particular por el aire, las moléculas del aire interferirán con él, causando un cambio en su polarización, lo que no puede ser tolerado. Un medio más eficaz para transmitir fotones es a través de una fibra óptica y recientemente los investigadores han logrado utilizar esta técnica para construir sistemas criptográficos cuánticos que operan a través de grandes distancias. En 1995, investigadores de la Universidad de Ginebra lograron poner en práctica la criptografía cuántica en una fibra óptica que se extendía 23 km, de Ginebra a la ciudad de Nyon.

Más recientemente, un grupo de científicos del Laboratorio Nacional de Los Álamos, en Nuevo México, han comenzado de nuevo a experimentar con la criptografía cuántica a través del aire. Su objetivo final es crear un sistema criptográfico cuántico que pueda operar a través de satélites. Si esto se pudiera conseguir permitiría la comunicación global absolutamente segura. Hasta ahora, el grupo de Los Álamos ha logrado transmitir una clave cuántica a través del aire a una distancia de 1 km Los expertos en seguridad se preguntan ahora cuánto se tardará en convertir la criptografía cuántica en una tecnología práctica. En estos momentos, contar con la criptografía cuántica no supondría una ventaja, porque la cifra RSA ya

nos da acceso a una codificación de hecho indescifrable. Sin embargo, si los ordenadores cuánticos se convierten en realidad, RSA y todas las demás cifras modernas serán inútiles, y la criptografía cuántica se convertiría en una necesidad. De modo que la carrera está en marcha. La cuestión realmente importante es si la criptografía cuántica llegará a tiempo de salvamos de la amenaza de los ordenadores cuánticos, o si habrá un intervalo sin privacidad, un período entre el desarrollo de los ordenadores cuánticos y la llegada de la criptografía cuántica. Hasta ahora, la criptografía cuántica es la tecnología más avanzada. El experimento suizo con fibras ópticas demuestra que sería viable construir un sistema que permita la comunicación segura entre instituciones financieras dentro de una misma ciudad. Efectivamente, ahora mismo es posible construir un enlace de criptografía cuántica entre la Casa Blanca y el Pentágono. Quizá ya haya uno.

La criptografía cuántica marcaría el fin de la batalla entre los creadores de cifras y los descifradores, y los creadores de cifras serían los vencedores. La criptografía cuántica es un sistema de cifrado indescifrable. Puede que esto parezca una afirmación bastante exagerada, sobre todo a la luz de anteriores afirmaciones similares. En diferentes momentos de los últimos dos mil años, los criptógrafos han creído que la cifra monoalfabética, la cifra polialfabética y las cifras de máquina como la Enigma eran indescifrables. En cada uno de estos casos se demostró posteriormente que los criptógrafos estaban equivocados porque sus afirmaciones se basaban meramente en el hecho de que la complejidad de las cifras superaba el ingenio y la tecnología de los criptoanalistas en un determinado momento de la Historia. Con la perspectiva del tiempo, podemos ver que los criptoanalistas descubrirían inevitablemente una forma de descifrar cada cifra o de desarrollar la tecnología que la descifraría.

Sin embargo, la afirmación de que la criptografía cuántica es segura es cualitativamente diferente de todas las afirmaciones anteriores. La criptografía cuántica no es sólo de hecho indescifrable, es absolutamente indescifrable. La teoría cuántica, la teoría de más éxito en la historia de la física, significa que es imposible que Eva intercepte con exactitud la clave de cuaderno de uso único establecida entre Alicia y Benito. Eva ni siquiera puede tratar de interceptar la clave de cuaderno de uso único sin que Alicia y Benito adviertan su espionaje. En realidad, si

un mensaje protegido por la criptografía cuántica fuese descifrado alguna vez, esto significaría que la teoría cuántica es errónea, lo que tendría implicaciones desastrosas para los físicos; se verían obligados a reconsiderar su compresión de cómo funciona el universo en su nivel más fundamental.

Si se pueden construir sistemas criptográficos cuánticos que operen entre grandes distancias, la evolución de las cifras se detendrá. La búsqueda de la privacidad habrá llegado a su fin. Habrá disponible una tecnología que garantice las comunicaciones seguras a los gobiernos, el ejército, las empresas y el público. La única cuestión que queda es si los gobiernos nos permitirían usar esa tecnología. ¿Cómo regularían los gobiernos la criptografía cuántica para que enriquezca la Era de la Información sin proteger a los criminales?

Apéndice A
El llamado «Código de la Biblia»

En 1997, el libro *The Bible Code*, de Michael Drosnin, provocó titulares en todo el mundo. Drosnin afirmaba que la Biblia contiene mensajes ocultos que se podían descubrir buscando las secuencias de letras equidistantes *(equidistant letters sequences*: EDLS). Un EDLS se encuentra tomando cualquier texto, eligiendo una letra inicial particular, y luego avanzando un número determinado de letras cada vez.

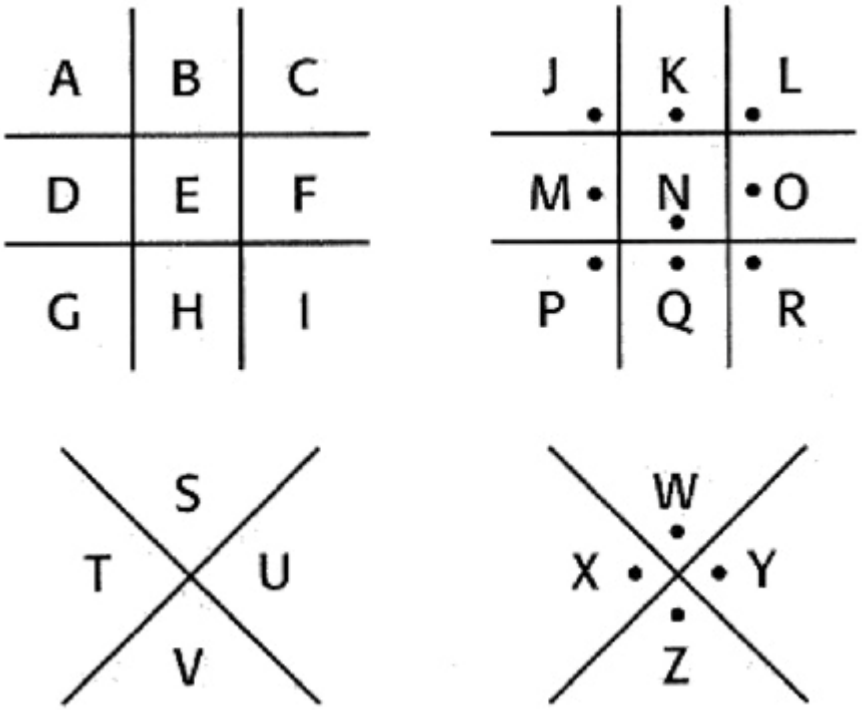
Así, por ejemplo, con este párrafo podríamos empezar con la letra «M» de Michael y avanzar, pongamos, cinco espacios cada vez. Si anotásemos cada quinta letra, generaríamos el EDLS mesroleo...

Aunque este EDLS en particular no contiene ninguna palabra con sentido, Drosnin describió el descubrimiento de un número sorprendente de EDLS bíblicos que no solamente forman palabras con sentido, sino que resultan frases completas. Según Drosnin, estas secuencias son predicciones bíblicas. Por ejemplo, asegura haber encontrado referencias a los asesinatos de John F. Kennedy, Robert Kennedy y Anuar El Sadat. En un EDLS se menciona el nombre Newton junto a la gravedad, y en otro se asocia a Edison con la bombilla. Aunque el libro de Drosnin se basa en un artículo publicado por Doron Witzum, Eliyahu Rips y Yoav Rosenberg, sus afirmaciones son muchísimo más ambiciosas y ha provocado muchas críticas. La mayor causa de aprensión es que el texto que se estudia es enorme: en un texto suficientemente extenso, no es de extrañar que variando tanto el lugar inicial y el tamaño de los avances se puedan hacer aparecer frases con sentido.

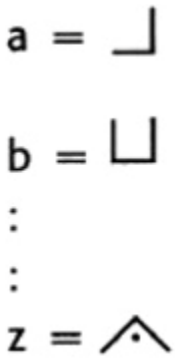
Brendan McKay, de la Universidad Nacional Australiana, trató de demostrar la debilidad del enfoque de Drosnin buscando EDLS en *Moby Dick* y descubrió trece afirmaciones relacionadas con los asesinatos de personas famosas, incluidos Trotski, Gandhi y Robert Kennedy. Además, los textos hebreos tienden a ser particularmente ricos en EDLS, porque están en gran medida desprovistos de vocales. Esto significa que los intérpretes pueden insertar vocales según lo crean conveniente, lo que hace que resulte más fácil extraer predicciones.

Apéndice B
La cifra Pigpen

La cifra de sustitución monoaltabética perduró a través de los siglos en formas diversas. Por ejemplo, la cifra Pigpen fue utilizada por los masones en el siglo XVIII para preservar la privacidad de sus archivos, y todavía la usan los niños hoy en día. La cifra no sustituye una letra por otra, sino que sustituye cada letra por un símbolo de acuerdo al siguiente modelo.



Para codificar una letra particular, encuentre su posición en una de las cuatro cuadrículas y luego dibuje esa porción de la cuadrícula para representar esa letra. Por tanto:



Si conoce la clave, la cifra Pigpen es fácil de descifrar. Si no, se puede descifrar fácilmente con el:

Apéndice C
La cifra Playfair

La cifra Playfair fue popularizada por Lyon Playfair, primer barón Playfair de St. Andrews, pero fue inventada por sir Charles Wheatstone, uno de los pioneros del telégrafo eléctrico. Los dos hombres vivían cerca, cada uno a un lado del puente de Hammersmith, y se reunían a menudo para hablar de sus ideas sobre la criptografía.

La cifra sustituye cada par de letras de texto llano con otro par de letras. Para codificar y transmitir un mensaje, el emisor y el receptor deben acordar primero una palabra clave. Por ejemplo, podemos utilizar el propio nombre de Wheatstone, CHARLES, como clave. A continuación, antes de codificar, las letras del alfabeto se escriben en un cuadrado de 5 x 5, comenzando con la palabra clave, y combinando las letras I y J en un solo elemento:

C	H	A	R	L
E	S	B	D	F
G	I/J	K	M	N
O	P	Q	T	U
V	W	X	Y	Z

A continuación, se divide el mensaje en pares de letras, o dígrafos. Las dos letras de todos los dígrafos deben ser diferentes, lo que se consigue en el ejemplo siguiente insertando una x adicional entre las dos m de hammersmith, y se añade una x adicional al final para convertir en un dígrafo la letra final que quedaba sola:

Texto llano	meet me at hammersmith bridge tonight*
Texto llano en dígrafos	me-et-me-at-ha-mx-me-rs-mi-th-br-id-ge-to-ni-gh-tx

«Reúnete conmigo en el puente de Hammersmith esta noche».

Ahora puede comenzar la codificación. Todos los dígrafos caen en una de estas tres categorías: ambas letras están en la misma línea, o en la misma columna, o en ninguna de las dos. Si ambas letras están en la misma línea, son reemplazadas por la letra que queda a la derecha de cada una de ellas; igualmente, mi se convierte en NK Si una de las letras está al final de la línea, es reemplazada por la letra que hay al principio de la línea; por último, ni se convierte en GK Si ambas letras están en la misma columna, son reemplazadas por la letra que hay debajo de cada una de ellas; así pues, ge se convierte en OG. Si una de las letras está en la parte inferior de la columna, es reemplazada por la letra de la parte superior de la columna; así pues, ve se convierte en CG

Si las letras del dígrafo no están ni en la misma línea ni en la misma columna, la codificación se rige por una regla diferente. Para codificar la primera letra, mire en su línea hasta llegar a la columna que contiene la segunda letra; la letra que hay en esa intersección reemplaza a la primera letra. Para codificar la segunda letra, mire en su línea hasta llegar la columna que contiene la primera letra; la letra que hay en esa intersección reemplaza a la segunda letra. Por tanto, me se convierte en GD y et se convierte en DO. La codificación completa es:

Texto llano															
en dígrafos	me	et	me	at	ha	mx	me	rs	mi	th	br	id	ge	to	ni	gh	tx
texto cifrado	GD	DO	GD	RQ	AR	KY	GD	HD	NK	PR	DA	MS	OG	UP	GK	IC	QY

El receptor, que también conoce la palabra clave, puede descifrar fácilmente el texto cifrado simplemente invirtiendo el proceso: por ejemplo, las letras cifradas que estén en la misma línea se descifran reemplazándolas por la letra que haya a la izquierda de cada una de ellas.

Además de ser científico, Playfair era también una notable figura pública (vicepresidente de la Cámara de los Comunes, director general de correos, y el comisario de la salud pública que contribuyó a desarrollar la base moderna de la sanidad) y estaba decidido a promover la idea de Wheatstone entre los políticos con cargos más elevados. Primero lo comentó en una cena en 1854 delante del príncipe Alberto y del futuro primer ministro, lord Palmerston, y luego presentó a Wheatstone al vicesecretario del Ministerio de Asuntos Exteriores.

Desgraciadamente, el vicesecretario alegó que el sistema era demasiado complicado para ser usado en condiciones de batalla, a lo que Wheatstone adujo que él podría enseñar el método en un cuarto de hora a los niños de la escuela primaria más cercana. «Eso es muy posible», replicó el vicesecretario, «pero nunca podría enseñárselo a los agregados diplomáticos».

Playfair persistió, y finalmente el secretario de la Oficina de Guerra británica adoptó la técnica, utilizándola probablemente por vez primera en la guerra de los bóers. Aunque resultó eficaz durante un tiempo, la cifra Playfair estaba muy lejos de ser inexpugnable. Se puede atacar buscando los dígrafos que aparezcan con más frecuencia en el texto cifrado, y suponiendo que representan los dígrafos más corrientes en inglés: th, he, an, in, er, re, es.

Apéndice D
La cifra ADFGVX

n la cifra ADFGVX hay sustitución y trasposición. La codificación comienza dibujando una cuadrícula de 6 x 6, y llenando los 36 cuadrados con una disposición aleatoria de las 26 letras y los 10 dígitos. Cada línea y cada columna de la cuadrícula se identifica con una de las seis letras A, D, F, G, V o X. La disposición de los elementos en la cuadrícula funciona como parte de la clave, de modo que el receptor necesita conocer los detalles de la cuadrícula

	A	D	F	G	V	X
A	8	p	3	d	1	n
D	l	t	4	o	a	h
F	7	k	b	c	5	z
G	j	u	6	w	g	m
V	x	s	v	i	r	2
X	9	e	y	0	f	q

La primera fase de la codificación es tomar cada letra del mensaje, localizar su posición en la cuadrícula y sustituirla con las letras que dan nombre a su línea y su columna. Por ejemplo, 8 sería sustituido por A A, y p sería reemplazado por AD. Veamos un mensaje corto codificado según este sistema.

Mensaje	ven a las 10 de la noche
Texto llano	v e n a l a s 1 0 d e l a n o c h e
Texto cifrado fase 1	VF XD AX DV DA DV VD AV XG AG XD DA DV AX DG FG DX XD

Hasta ahora, es una simple cifra de sustitución monoalfabética, y bastaría un análisis de frecuencia para descifrarla. Sin embargo, la segunda fase de ADFGVX es una trasposición, lo que dificulta muchísimo más el criptoanálisis. La trasposición depende de una palabra clave, que en este caso es la palabra PACO, y que debe compartirse con el receptor. La trasposición se lleva a cabo de la siguiente manera.

Primero, las letras de la palabra clave se escriben en la línea superior de una nueva cuadrícula. Luego, el texto cifrado fase 1 se escribe debajo en una serie de líneas, tal como se muestra a continuación. Después, las columnas de la cuadrícula se cambian de posición de modo que las letras de la palabra clave queden en orden alfabético. El texto cifrado final se logra descendiendo cada columna y escribiendo las letras en este nuevo orden

P	A	C	O		A	C	O	P
V	F	X	D		F	X	D	V
A	X	D	V		X	D	V	A
D	A	D	V	Cambie la posición de las	A	D	V	D
V	D	A	V	columnas de modo que las	D	A	V	V
X	G	A	G	letras de la palabra clave	G	A	G	X
X	D	D	A	queden en orden alfabético	D	D	A	X
D	V	A	X		V	A	X	D
D	C	F	G		C	F	C	D
D	X	X	D		X	X	D	D

Texto cifrado final FXADGDVGXXDDAADAFXDVVVGAXGDVADVXXDDD

El texto cifrado final se transmitiría entonces en código Morse, y el receptor invertiría el proceso de codificación para obtener el texto original. Todo el texto cifrado se compone con sólo seis letras (esto es, A, D, F, G, V, X), porque éstas son las que dan nombre a las líneas y las columnas de la cuadrícula inicial de 6 x 6. A menudo, la gente se pregunta

por qué se eligieron estas letras, en vez de, pongamos, A, B, C, D, E y F. La respuesta es que A, D, F, G, V y X son muy diferentes entre sí cuando se convierten en las líneas y puntos del Morse, de modo que esta elección de letras reduce al mínimo el riesgo de errores durante la transmisión.

Apéndice E

Los problemas de reciclar un cuaderno de uso único

Por las razones explicadas en el Capítulo 3, los textos cifrados codificados según una cifra de cuaderno de uso único son indescifrables. Sin embargo, esto depende de que cada cuaderno de uso único se utilice una sola vez. Si interceptásemos dos textos cifrados distintos que hubieran sido codificados con el mismo cuaderno de uso único, podríamos descifrarlos de la siguiente manera.

Probablemente estaríamos en lo cierto al suponer que el primer texto cifrado contiene en alguna parte la palabra the, de modo que el criptoanálisis comienza suponiendo que el mensaje entero consiste en una serie de thes. A continuación, calculamos el cuaderno de uso único que se requeriría para convertir toda una serie de thes en el primer texto cifrado. Ésta se vuelve nuestra primera suposición del cuaderno de uso único. ¿Cómo averiguamos qué partes de este cuaderno de uso único son correctas?

Podemos aplicar nuestra primera suposición del cuaderno de uso único al segundo texto cifrado, y ver si el texto llano resultante tiene algún sentido. Si tenemos suerte, podremos discernir unos pocos fragmentos de palabras en el segundo texto cifrado, lo que indica que las partes correspondientes del cuaderno de uso único son correctas. A su vez, esto nos muestra que partes del primer mensaje debería ser the.

Expandiendo los fragmentos que hemos encontrado en el segundo texto llano, podemos calcular más partes del cuaderno de uso único y deducir así nuevos fragmentos del primer texto llano. Expandiendo estos fragmentos en el primer texto llano, podemos calcular más partes del cuaderno de uso único para luego deducir nuevos fragmentos en el segundo texto llano. Podemos continuar este proceso hasta que hayamos descifrado los dos textos llanos.

Este proceso es muy similar al desciframiento de un mensaje codificado con una cifra Vegenère que utilice una clave que consista en una serie de palabras, como en el ejemplo del Capítulo 3, en el que la clave era CANADABRAZILEGYPTCUBA.

Apéndice F
Ejercicios para el lector interesado

Algunos de los desciframientos más importantes de la Historia han sido realizados por aficionados. Por ejemplo, Georg Grotefend, que realizó el primer gran avance en la interpretación del cuneiforme, era un maestro de escuela. Para aquellos lectores que sientan el deseo de seguir sus pasos aún quedan varias escrituras que continúan siendo un misterio. El Lineal A, una escritura minoica, se ha resistido a todas las tentativas de desciframiento, debido en parte a la escasez de material. El etrusco no ofrece este problema, pues hay más de 10.000 inscripciones disponibles para el estudio, pero también ha desconcertado a los eruditos más importantes del mundo. El ibérico, otra escritura prerromana, y las runas futhark de Escandinavia son igualmente insondables.

La escritura europea antigua más fascinante aparece en el disco de Faistos, un ejemplar único descubierto en el sur de Creta en 1908. Es una tablilla circular que data de alrededor de 1700 a. C. y lleva un texto escrito en forma de dos espirales, una en cada lado. Los signos no son impresiones hechas a mano, sino que fueron hechos utilizando diversos sellos, lo que lo convierte en el ejemplo más antiguo del mundo de escritura a máquina. Lo extraordinario es que nunca se ha descubierto otro documento similar, de modo que el desciframiento se tiene que basar en información muy limitada: hay 242 caracteres divididos en 61 grupos.

Sin embargo, un documento escrito a máquina supone una producción en serie, por lo que se confía en que los arqueólogos llegarán a descubrir muchísimos más discos similares, y aclarar algo sobre esta escritura tan difícil de solucionar.

Unos de los mayores desafíos fuera de Europa es el desciframiento de la escritura de la civilización índica, que se remonta a la Edad de Bronce, y que se puede encontrar en miles de sellos que datan del tercer milenio a. C. Cada sello muestra un animal acompañado de una breve inscripción, pero hasta ahora el significado de estas inscripciones ha escapado a todos los expertos.

En un ejemplo excepcional, la escritura se ha encontrado en un gran tablero de madera con letras gigantes de 37 cm de altura. Podría tratarse de la valla publicitaria más antigua del mundo. Esto da a entender que la alfabetización no

estaba limitada a la elite y plantea la cuestión de qué es lo que se anunciaba. La respuesta más probable es que formaba parte de una campaña de promoción de un rey, y si se logra establecer la identidad del rey, el anuncio podría abrir un camino por el que entrar en el resto de la escritura.

Apéndice G
Los cálculos matemáticos de RSA

Lo que sigue es una descripción matemática sencilla de la mecánica de la codificación y descodificación RSA.

(1) Alicia elige dos números primos gigantes, p y q Estos números primos deberían ser enormes, pero para simplificar vamos a suponer que Alicia escoge p = 17, q= 11. Alicia debe mantener estos números en secreto.

(2) Alicia multiplica estos números el uno por el otro y obtiene así otro número, N. En este caso, N= 187. Ahora elige otro número, e, y en este caso escoge e = 7, e y(p - 1) x (q - 1) deben ser relativamente primos, pero esto es un detalle técnico.

(3) Alicia puede ahora hacer público los números e y N en algo similar a una guía telefónica. Como estos dos números son necesarios para la codificación, deben estar disponibles para cualquiera que pudiera querer enviar un mensaje codificado a Alicia. Estos dos números juntos constituyen la clave pública. (Además de formar parte de la clave pública de Alicia, e podría también formar parte de la clave pública de cualquier otra persona. Sin embargo, el valor de N debe ser diferente para cada persona, lo que depende de su elección de p y q)

(4) Para codificar un mensaje, primero hay que convertir el mensaje en un número, M. Por ejemplo, una palabra se cambia en dígitos binarios ASCII, y los dígitos binarios pueden ser considerados como un número decimal. Luego, M se codifica para producir el texto cifrado, C, según esta fórmula: $C= M^e \pmod N$

(5) Imagine que Benito quiere enviar a Alicia un simple beso: tan sólo la letra X[27]. En ASCII, esa letra se representa con 1011000, lo que equivale a 88 en decimal. Así que M= 88.

[27] En inglés, se utiliza la X con el significado de «un beso». Se pueden poner muchas seguidas, expresando «muchos besos», siendo normal finalizar una carta con XXX. (N. del T.)

(6) Para codificar este mensaje, Benito comienza buscando la clave pública de Alicia, y descubre que N = 187, y e = 7. Esto le proporciona la fórmula de codificación requerida para codificar mensajes para Alicia. Con M = 88, la fórmula da:

$$C = 88^7 \pmod{187}$$

(7) Calcular esto directamente con una calculadora no es sencillo, porque su pequeña pantalla no tiene capacidad para números tan enormes. Sin embargo, existe un truco ingenioso para calcular exponenciales en aritmética modular. Sabemos que, como

$$7 = 4 + 2 + 1$$

$$88^7 \pmod{187} = [88^4 \pmod{187} \times 88^2 \pmod{187} \times 881 \pmod{187}] \pmod{187}$$

$$88^1 = 88 \pmod{187}$$

$$88^2 = 7.744 = 77 \pmod{187}$$

$$88^4 = 59.969.536 = 132 \pmod{187}$$

$$88^7 = 88^1 \times 88^2 \times 88^4 = 88 \times 77 \times 132 = 894.432 = 11 \pmod{187}$$

Ahora Benito envía el texto cifrado, C = 11, a Alicia.

(8) Sabemos que las exponenciales en aritmética modular son funciones de una sola vía, por lo que es muy difícil invertir los cálculos partiendo de C = 11 y recuperar el mensaje original, M. Por consiguiente, Eva no puede descifrar el mensaje.

(9) Sin embargo, Alicia puede descifrar el mensaje porque tiene una información especial: conoce los valores de p y q. Calcula un número especial, d, la clave de descodificación, conocida también como su clave privada. El número d se calcula según la siguiente fórmula:

$$7 \times d = 1 \pmod{16 \times 10}$$

$$7 \times d = 1 \pmod{160}$$

$$d = 23$$

(Deducir el valor de d no es sencillo, pero una técnica conocida como el algoritmo de Euclides permite a Alicia encontrar d rápida y fácilmente).

(10) Para descodificar el mensaje, Alicia usa simplemente la siguiente

fórmula:

$M=C^d \pmod{187}$

$M= 11^{23} \pmod{187}$

$M= [11^1 \pmod{187} \times 11^2 \pmod{187} \times 11^4 \pmod{187} \times 11^{16} \pmod{187}] \pmod{187}$

$M= 11 \times 121 \times 55 \times 154 \pmod{187}$

M= 88 = X en ASCII.

Rivest, Shamir y Adleman habían creado una función especial de una sola vía, que sólo podía ser invertida por alguien que tuviera acceso a una información privilegiada: los valores de p y q. Se puede personalizar cada función eligiendo p y q, que al multiplicarse entre sí dan N. La función permite a todo el mundo codificar mensajes para una persona concreta utilizando la elección de N de esa persona, pero sólo el receptor a quien va dirigido puede descodificar el mensaje, porque él es la única persona que conoce p y q, y, por tanto, es la única persona que conoce la clave de descodificación, d.

Agradecimientos

Mientras escribía este libro, he tenido el privilegio de conocer a algunos de los mejores codificadores y descifradores vivos del mundo, desde los que trabajaron en Bletchley Park a los que están creando cifras que enriquecerán la Era de la Información. Me gustaría dar las gracias a Whitfield Diffie y a Martin Hellman, que se tomaron la molestia de describirme su trabajo cuando fui a la soleada California. De manera similar, Clifford Cocks, Malcolm Williamson y Richard Walton me ofrecieron una ayuda valiosísima durante mi visita a la nublada Cheltenham. Estoy agradecido, en particular, al Grupo de Seguridad de la Información del Royal Holloway College de Londres, que me permitió asistir al curso de máster de Ciencias dedicado a la seguridad de la información. El profesor Fred Piper, Simon Blackbum, Jonathan Tuliani y Fauzan Mirza me enseñaron valiosas lecciones sobre los códigos y las cifras.

Durante mi estancia en Virginia tuve la suerte de que Peter Viemeister, un experto en ese misterio, me acompañara en una visita guiada al camino del tesoro Beale. Además, el Museo del Condado de Bedford y Stephen Cowart, de la Asociación de la Cifra y el Tesoro Beale, me ayudaron a investigar el tema. También quiero dar las gracias a David Deutsch y Michele Mosca, del Centro para la Informática Cuántica de Oxford, a Charles Bennett y a su grupo de investigación en los Laboratorios Thomas J. Watson de la IBM, a Stephen Wiesner, Leonard Adleman, Ronald Rivest, Paul Rothemund, Jim Gillogly, Paul Leyland y Neil Barrett.

Derek Taunt, Alan Stripp y Donald Davies me explicaron amablemente la manera en que Bletchley Park descifró la Enigma, y también recibí ayuda del Bletchley Park Trust, cuyos miembros pronuncian regularmente conferencias informativas sobre temas diversos. Los doctores Mohammed Mrayati e Ibrahim Kadi se han venido ocupando de revelar algunos de los primeros avances del criptoanálisis árabe y tuvieron la amabilidad de enviarme documentación relevante. La revista *Cryptologia* también publica artículos sobre el criptoanálisis árabe, además de sobre muchos otros temas criptográficos, y me gustaría agradecer a Brian Winkel que me enviase números atrasados de la publicación.

Quisiera animar a los lectores a que visiten el Museo Criptográfico Nacional de Washington, y las Salas del Gabinete de Guerra de Londres, y confío en que se sientan tan fascinados como lo estuve yo durante mis visitas. Muchas gracias a los conservadores y bibliotecarios de dichos museos por asistirme en mi investigación Cuando estuve apurado de tiempo, James Howard, Bindu Mathur, Pretty Sagoo, Anna Singh y Nick Shearing me ayudaron a descubrir artículos, libros y documentos importantes e interesantes, y les agradezco mucho sus esfuerzos. Gracias también a Antony Buonomo, de www.vertigo.co.uk, que me ayudó a establecer mi página web.

Además de contar con entrevistadores expertos, me he servido también de libros y artículos. La lista de lecturas adicionales contiene algunas de mis fuentes, pero no constituye una bibliografía completa ni una lista definitiva de referencias. Simplemente incluye material que puede resultar de interés para el lector general. Entre todos los libros que he encontrado durante mi investigación, me gustaría destacar uno en particular: *The Codebreakers,* de David Kahn. Este libro documenta casi todos los episodios criptográficos de la Historia, y constituye una fuente de datos inestimable.

Diversas bibliotecas, instituciones e individuos me han proporcionado fotografías. Todas las fuentes aparecen en la lista de créditos de las fotografías, pero quiero dar las gracias particularmente a Sally McClain por enviarme fotografías de los mensajeros de código navajo, a la profesora Eva Brann por descubrir la única foto conocida de Alice Kober, a Joan Chadwick por enviarme una foto de John Chadwick, y a Brenda Ellis, por permitirme tomar prestadas algunas fotos de James Ellis. Gracias también a Hugh Whitemore, que me permitió utilizar una cita de su obra de teatro *Breaking the Code,* basada en el libro de Andrew Hodges *Alan Turing —The Enigma.*

De manera más personal, me gustaría expresar mi agradecimiento a mis amigos y familiares que me han aguantado durante los dos años que he estado escribiendo este libro. Neil Boynton, Dawn Dzedzy, Sonya Holbraad, Tim Johnson, Richard Singh y Andrew Thompson me ayudaron a mantener la cordura mientras me enfrentaba a enrevesados conceptos criptográficos. En particular, Bernadette Alves me ofreció una rica combinación de apoyo moral y crítica perspicaz. Volviendo la vista atrás,

muchas gracias a todas las personas e instituciones que han formado mi carrera, incluyendo a la Wellington School, el Imperial College y el High Energy Physics Group de la Universidad de Cambridge; Dana Purvis, de la BBC, que me brindó mi primera oportunidad en la televisión; y Roger Highfield, del *Daily Telegraph*, que me animó a escribir mi primer artículo.

Finalmente, he tenido la inmensa suerte de trabajar con algunas de las mejores personas del mundo editorial. Patrick Walsh es un agente que ama la ciencia, se preocupa por sus autores y tiene un entusiasmo ilimitado. Él me ha puesto en contacto con los editores más amables y competentes, en particular Fourth Estate, cuyo personal soporta con brío admirable mi constante oleada de preguntas. Y en último lugar, pero ciertamente no por ello menos importante, mis editores, Christopher Potter, Leo Hollis y Petemelle van Arsdale, me han ayudado a mantener una trayectoria clara a través de un tema que se esparce con infinidad de giros y recovecos a lo largo de tres mil años. Por ello les estoy enormemente agradecido.

Lecturas adicionales

La siguiente lista contiene libros que pueden ser de interés para el público en general. No he incorporado referencias técnicas más detalladas, pero muchos de los textos incluidos contienen una bibliografía detallada. Por ejemplo, si desea saber más acerca del desciframiento del Lineal B (Capítulo 5), le recomendaría *El desciframiento del Lineal B,* de John Chadwick. Sin embargo, si este libro no es lo suficientemente detallado, consulte las referencias que contiene.

Hay gran cantidad de material interesante referente a los códigos y las cifras en Internet. Debido a ello, además de los libros, he incluido algunas de las páginas web que merece la pena visitar.

General

Kahn, David, *The Codebreakers* (Nueva York, Scribner, 1996).

Una historia de las cifras de 1.200 páginas. La historia definitiva de la criptografía hasta la década de 1950.

Newton, David E., *Encyclopedia of Cryptology* (Santa Bárbara, CA, ABC-Clio, 1997).

Una útil referencia, con explicaciones claras y concisas de la mayoría de los aspectos de la criptología antigua y moderna.

Smith, Lawrence Dwight, *Cryptography* (Nueva York, Dover, 1943).

Una excelente introducción elemental a la criptografía, con más de 150 problemas. Dover publica muchos libros sobre el tema de los códigos y las cifras.

Beutelspacher, Albrecht, *Cryptology* (Washington, D C, Mathematical Association of America, 1994).

Una excelente visión general del tema, desde la cifra del César a la criptografía de clave pública, más centrada en los aspectos matemáticos que en la historia. Es también el libro criptográfico con el mejor subtítulo: *An Introduction to the Art and Science of Enciphering, Encrypting, Concealing,* Hiding, and Safeguarding, Described Without any Arcane Skullduggery but not Without Cunning Waggery for the Delectation and Instruction of the General Public.

Capítulo 1

Gaines, Helen Fouché, *Cryptanalysis* (Nueva York, Dover, 1956).
Un estudio de las cifras y su solución. Una excelente introducción al criptoanálisis, con muchas útiles tablas de frecuencia en el apéndice.
Al Kadi, Ibraham A., «*The origins of cryptology: The Arab contributions*», Cryptologia, vol. 16, núm. 2 (abril de 1992), págs. 97-126.
Los manuscritos árabes recientemente descubiertos y la obra de Al Kindi.
Fraser, lady Antonia, *Mary Queen of Scots* (Londres, Random House, 1989).
Un ameno relato de la vida de María Estuardo.
Smith, Alan Gordon, *The Babington Plot* (Londres, Macmillan, 1936).
Escrito en dos partes, este libro examina la conspiración desde ambos puntos de vista: el de Babington y el de Walsingham.
Steuart, A. Francis (ed.), *Trial of Mary Queen of Scots* (Londres, William Hodge, 1951).
Parte de la serie «Juicios británicos famosos».

Capítulo 2

Standage, Tom, The Victorian Internet (Londres, Weidenfield &Nicolson, 1998).
La extraordinaria historia del desarrollo del telégrafo eléctrico.
Franksen, Ole Immanuel, *Mr Babbage* S *Secret* (Londres, Prentice-Hall, 1985).
Contiene una discusión sobre el trabajo de Babbage para descifrar la cifra Vegenère.
Franksen, Ole Immanuel, «Babbage and cryptography. Or, the mystery of Admiral Beaufort's cipher», en *Mathematíes and Computer Simulations*, vol. 35, 1993, págs. 327-367.
Un artículo detallado sobre el trabajo criptológico de Babbage y su relación con el contralmirante sir Francis Beaufort.
Rosenheim, Shawn, *The Cryptographic Imagination* (Baltimore, MD, Johns Hopkins University Press, 1997).
Una evaluación académica de los escritos criptográficos de Edgar Alian Poe y su influencia en la literatura y la criptografía.
Poe, Edgar Allan, *Cuentos*, Alianza, 1988.
Incluye «El escarabajo de oro».

Viemeister, Peter, *The Beale Treasure: History of a Mystery* (Bedford, VA, Hamilton's, 1997).
Un informe detallado de las cifras Beale escrito por un respetado historiador local. Incluye el texto completo del folleto de Beale y la forma más fácil de conseguirlo es pedirlo directamente a la editorial: Hamilton's; P.O. Box 932; Bedford, VA, 24523; EE UU.

Capítulo 3

Tuchman, Barbara W., *The Zimmermann Telegram* (Nueva York, Ballantine, 1994).
Una amena exposición del desciframiento más importante de la primera guerra mundial.
Yardley, Herbert O., *The American Black Chamber* (Laguna Hills, CA, Aegean Park Press, 1931).
Una picante historia de la criptografía, que fue un controvertido éxito de ventas cuando se publicó por primera
vez.

Capítulo 4

Hinsley, F. H., British Intelligence in The Second World War: Its Influence on Strategy and Operations *(Londres, HMSO, 1975).*
La descripción fidedigna de la inteligencia en la segunda guerra mu incluido el papel de la inteligencia Ultra.
Hodges, Andrew, *Alan Turing: The Enigma* (Londres, Vintage, 1992).
La vida y el trabajo de Alan Turing. Una de las mejores biografías científicas jamás escritas.
Kahn, David, *Seizing the Enigma* (Londres, Arrow, 1996).
La versión de Kahn de la historia de la batalla del Atlántico y la importancia de la criptografía. En particular, Kahn describe dramáticamente Los robos de los submarinos, que ayudaron a los descifradores de Bletchley Park.
Hinsley, F. H., y Stripp, Alan (eds.), *The Codebreakers: The Inside Story of Bletchley Park* (Oxford, Oxford University Press, 1992).

Una colección de reveladores ensayos escritos por hombres y mujeres que formaron parte de uno de los mayores logros criptoanalíticos de la Historia.

Smith, Michael, *Station X* (Londres, Channel 4 Books, 1999).

El libro basado en la serie televisiva del mismo nombre del Canal 4 británico. Contiene anécdotas de los que trabajaron en Bletchley Park, conocido también como Estación X.

Harris, Robert, *Enigma* (Londres,

Arrow, 1996).

Una novela que gira en torno a los descifradores de Bletchley Park.

Capítulo 5

Paul, Doris A., *The Navajo Code Talkers* (Pittsburgh, PA, Dorrance, 1973).

Un libro dedicado a garantizar que la contribución de los mensajeros del código navajo no caiga en el olvido.

McClain, S., *The Navajo Weapon* (Boulder, CO, Books Beyond Borders, 1994).

Un apasionante relato que cubre toda la historia de los mensajeros navajos, escrito por una mujer que ha dedicado mucho tiempo a hablar con los hombres que crearon y utilizaron el código navajo.

Pope, Maurice, *The Story oj Decipherment* (Londres, Thames &Hudson, 1975).

Una descripción de varios desciframientos, de los jeroglíficos hititas al alfabeto ugarítico, dirigida a los profanos en la materia.

Davies, W. V, *Reading the Past: Egyptian Hieroglyphs* (Londres, British Museum Press, 1997).

Parte de una excelente serie de textos introductorios publicados por el Museo Británico. Otros autores de la serie han escrito libros sobre el cuneiforme, el etrusco, las inscripciones griegas, el Lineal B, los glifos mayas y las runas.

Chadwick, John, *The Decipherment of Linear B* (Cambridge, Cambridge University Press, 1987). Una brillante descripción de este desciframiento.

Capítulo 6

Data Encryption Standard, FIPS Pub. 46-1 (Washington, D C, National Bureau of Standards, 1987).

El documento oficial de DES.

Diffie, Whitfield, y Hellman, Martin, «New directions in cryptography», en *IEEE Transactions on Information Theory*, vol. IT-22 (noviembre de 1976), págs. 644-654.

El artículo clásico que reveló el descubrimiento de Diffie y Hellman sobre el intercambio de claves, que abrió las puertas a la criptografía de clave pública.

Gardner, Martin, «A new kind of cipher that would take millions of years to break», en *Scientijic American,* vol. 237 (agosto de 1997), págs. 120-124.

El artículo que presentó el RSA al mundo.

Hellman, M. E., «The mathematics of public-key cryptography», en *Scientific American*, vol. 241 (agosto de 1979), págs. 130-139.

Una excelente visión de conjunto de las diversas formas de criptografía de clave pública.

Diffie, Whitfíeld, «The fírst ten years of public-key cryptography», en *Proceedings of the IEEE*, vol. 76, núm 5 (mayo de 1988), págs. 560-577.

Otra excelente visión de conjunto de la criptografía de clave pública.

Capítulo 7

Zimmermann, Philip R., *The Official PGP User's Guide* (Cambridge, MA, MIT Press, 1996). PGP, escrita por el hombre que lo creó.

Garfinkel, Simson, PGP: *Pretty Good Privacy* (Sebastopol, CA, O'Reilly & Associates, 1995).

Una excelente introducción al PGP y los temas en torno a la criptografía moderna.

Bamford, James, *The Puzzle Palace* (Londres, Penguin, 1983).

Nos introduce en la NSA (Agencia de Seguridad Nacional), la organización de inteligencia más secreta de Estados Unidos.

Koops, Bert-Jaap, *The Crypto Controversy* (Boston, MA, Kluwer, 1998).

Un excelente estudio del impacto de la criptografía en la privacidad, las libertades civiles, la imposición de la ley y el comercio.

Diffie, Whitfield, y Landau, Susan, *Privacy on the Line* (Cambridge, MA, MIT Press, 1998).

La política de intervención de líneas y la codificación.

Capítulo 8

Deutsch, David, *The Fabric of Reality* (Londres, Alien Lañe, 1997).

Deutsch dedica un capítulo a los ordenadores cuánticos, en una tentativa de combinar la física cuántica con las teorías del conocimiento, la informática y la evolución.

Bennett, C. H., Brassard, C., y Ekert, A., "Quantum computadorf, en *Physics World,* vol. 11, núm 3 (marzo de 1998), págs. 33-56.

Uno de los cuatro artículos de un número especial de *Physics World.* Los otros tres artículos tratan de la información cuántica y la criptografía cuántica, y están escritos por los expertos más importantes en el tema. Los artículos van dirigidos a licenciados en física y ofrecen una excelente visión de conjunto del estado actual de la investigación.

Páginas de Internet

El misterio del tesoro Beale http ://www.roanokeva.com/ttd/storie

Una colección de páginas relacionadas con las cifras Beale. La *Beale Cypher and Treasure Association* se encuentra actualmente en transición, pero confía en estar nuevamente activa en este año.

Bletchley Park

http://www.cranfield.ac.uk- La página oficial, que incluye los horarios de apertura e instrucciones.

La página de Alan Turing

http: // www.turing. org. uk/ turing

Emuladores de la Enigma

http ://www.attlabs.att.co.uk/ andyc/en http: / / www. izzy. net/~ian/ enigma/ app

Dos excelentes emuladores que muestran el funcionamiento de la máquina Enigma. El primero permite alterar las posiciones de la máquina, pero no es posible seguir la pista de los circuitos eléctricos a través de los modificadores. El segundo tiene sólo una posición, pero posee una segunda ventana que muestra el movimiento de los modificadores y el efecto que produce en el circuito eléctrico.

Phil Zimmermann y PGP http: / / www. nai. com/ producís/securit

Electronic Frontier Foundation http://www.eff.org/

Una organización dedicada a proteger los derechos y a fomentar la libertad en Internet.

Centre for Quantum Computation http ://www. qubit. org/

Information Security Group, Royal Holloway College http://isg.rhbnc.ac.uk/

National Cryptologic Museum

http://www.nsa.gov: 8080/museum/

American Cryptogram Association (ACA)

http: / / www. und. nodak. edu/ org/ cryptc

Una asociación

especializada en plantear y resolver «jeroglíficos»

criptográficos.

Cryptologia

http://www.dean.usma.edu/math/reso

Una publicación trimestral dedicada a todos los aspectos de la criptología.

Preguntas frecuentes (FAQ) sobre criptología

http://www.cis.ohio- state.edu/hypertext/ faq/ usenet/ cryptograp

Sección de preguntas frecuentes (FAQ) sobre criptología actual de los Laboratorios RSA

http://www.rsa.com/rsalabs/faq/html,

La página sobre seguridad y codificación de Yahoo!

http: / / www.yahoo.co.uk/ Computersj

Cripto Enlaces

http: / / www. ftech. net/~monark/ crypto

IBM.