Agenda

- Definiciones Básicas
- Breve recuento histórico
- Alicia y Betito se vuelven públicos
- Criptografía post-cuántica
- A manera de conclusiones

Introducción y Definiciones Básicas

Francisco Rodríguez Henríquez

Criptografía y sus Aplicaciones

CINVESTAV

•Durante milenios, la criptografía se utilizó esencialmente en contextos militares y diplomáticos.

•En la actualidad, con la era tecnológica y nuestra creciente dependencia en sistemas electrónicos se necesitan, cada vez más, técnicas de cifrado y de seguridad altamente sofisticadas.

•Lo anterior obliga a contar con comunicaciones digitales privadas y seguras disponibles para todos.

Terminología

Criptología: Término genérico utilizado para designar la disciplina que estudia cómo lograr comunicaciones seguras sobre canales que no lo son, junto con otros problemas relacionados.

Criptografía: Diseño de sistemas y esquemas para realizar comunicaciones confiables sobre canales inseguros.

Criptoanálisis: Disciplina que estudia cómo romper esquemas criptográficos.

Texto en claro: mensaje que desea transmitirse de manera segura.

cifra: documento que resulta después de haber cifrado el texto en claro.

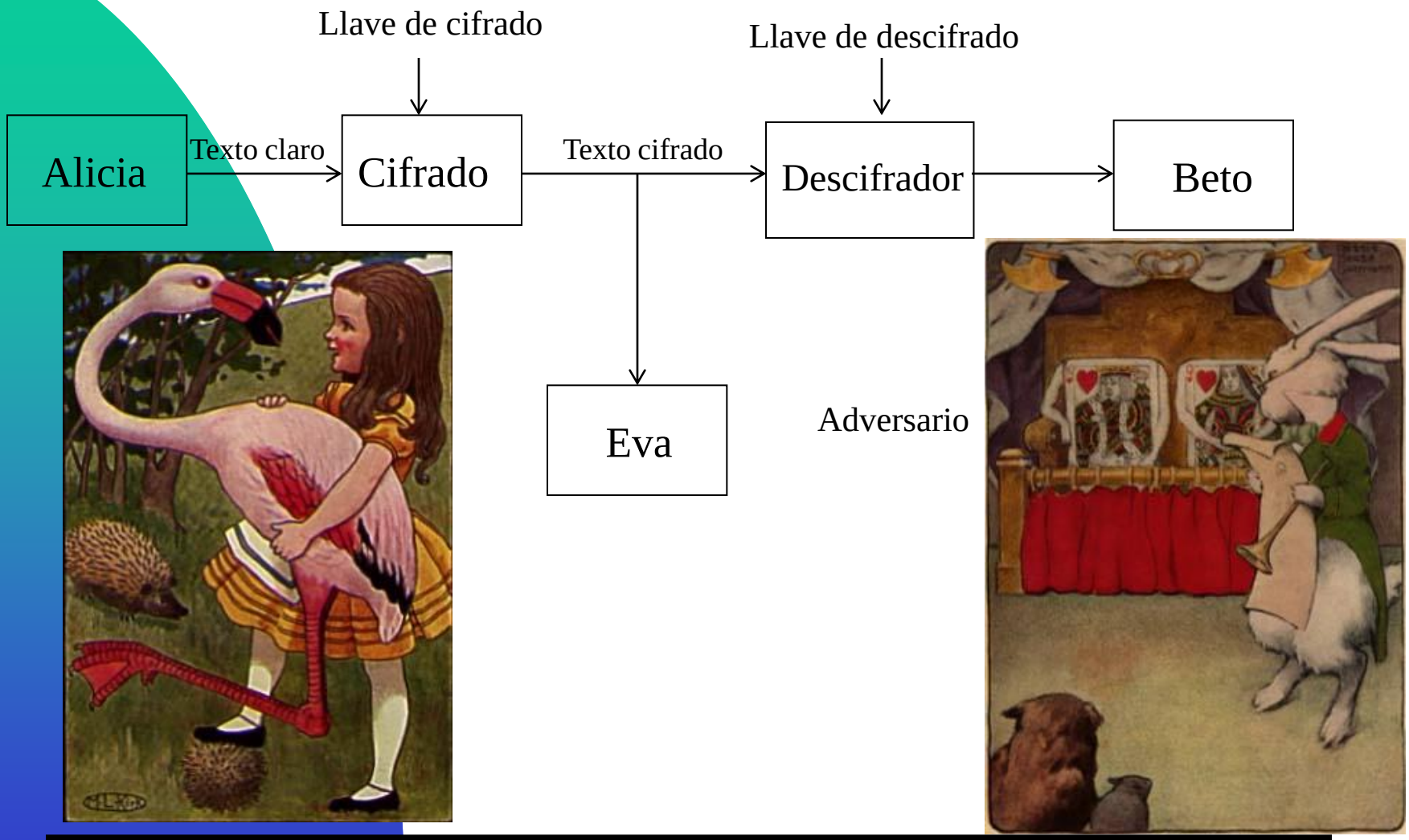
Llave o clave: información secreta que permite cifrar/descifrar documentos.

Aspectos de la criptografía moderna

CINVESTAV

- La criptografía moderna depende de manera directa de las matemáticas y del uso de sistemas digitales.
- Más específicamente se puede decir que está en la intersección de tres disciplinas: matemáticas, ciencias computacionales e ingeniería electrónica.
- Si no se tiene una comprensión profunda de las técnicas de criptoanálisis es imposible diseñar sistemas criptográficos confiables y seguros.

Comunicación Segura



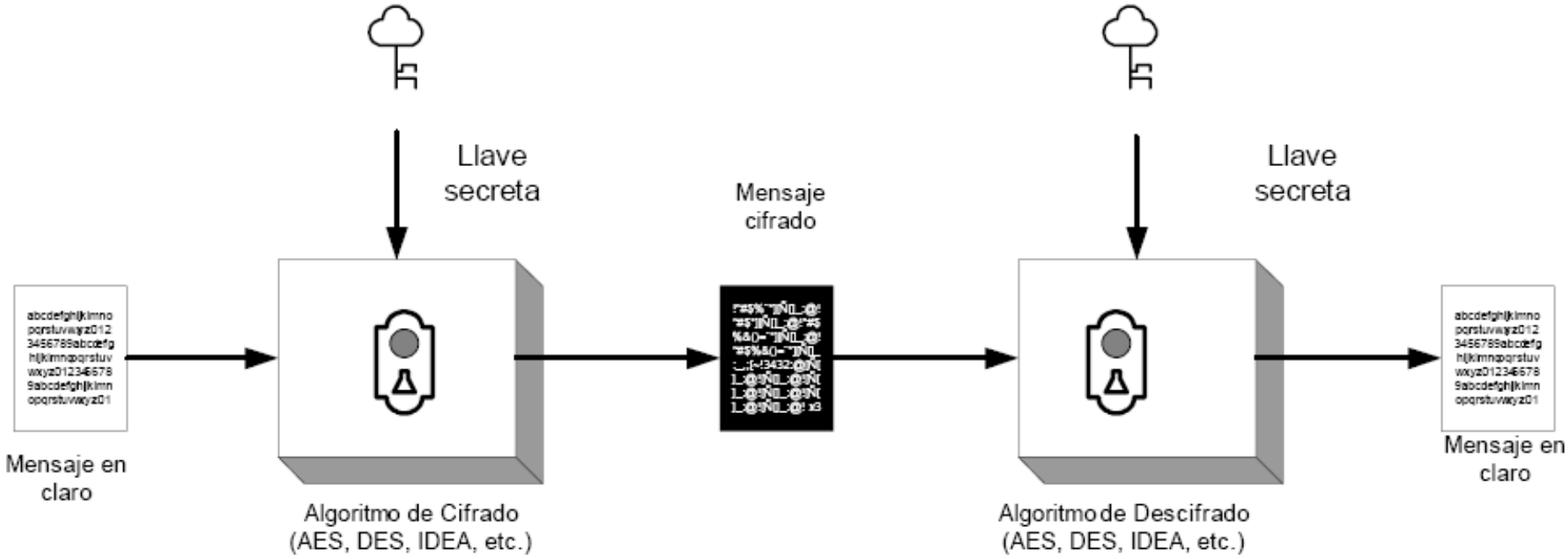
Objetivos del Adversario

1. Leer el mensaje original
2. Obtener la llave secreta de Alicia.
3. Modificar el contenido del mensaje original.
4. Usurpar la identidad de Alicia

Principio de Kerckhkoff

- se parte de la premisa que el oponente conoce el algoritmo criptográfico utilizado. Por lo tanto, la seguridad del sistema debe estar basada en:
  - La calidad (fortaleza) del algoritmo
  - El tamaño del espacio de la llave (tamaño en bits de la llave)

Criptografía de llave secreta



Criptografía de llave simétrica

Formalmente un *criptosistema* puede ser definido como una quíntupla $\{P,C,K,E,D\}$, donde:

P es el conjunto finito de los posibles textos en claro.

C es el conjunto finito de los posibles textos cifrados.

K el espacio de llaves, es un conjunto finito de todas las llaves posibles.

$$\forall k \in K \exists E_k \in E \text{ (regla de cifrado)} \exists D_k \in D \text{ (regla de descifrado)}$$

$$\text{Cada } E_k : P \to C \text{ y } D_k : C \to P \text{ son funciones tales que } \forall x \in P, D_k\left(E_k\left(x\right)\right) = x$$

Criptografía de llave simétrica

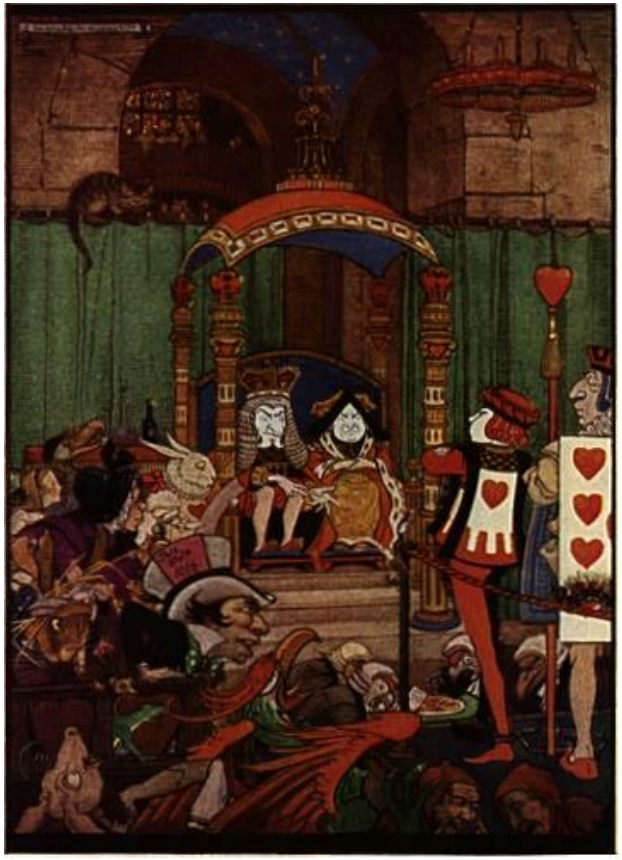
- Las llaves de cifrado y de descifrado son conocidas por las dos entidades (Alicia y Betito).
- Las llaves están relacionadas y es fácil derivar la llave de descifrado a partir de la llave de cifrado (en la mayoría de los casos las llaves son idénticas).
- Todos los criptosistemas clásicos (pre 1976) son simétricos. Ejemplos: DES, AES, etc.
- El modelo está pues basado en que las partes han convenido previamente un secreto compartido.

Tamaño de las llaves en criptosistemas

CINVESTAV

- De acuerdo al principio de Kerckhkoffs's la seguridad de los criptosistemas debe estar basada únicamente en dos propiedades importantes: calidad del algoritmo y longitud de la llave.
- Aunque la seguridad de un esquema es difícil de determinar sí es obvio que el tamaño de la llave debe ser lo suficientemente grande.
- Por ejemplo el cifrador DES utiliza llaves de 56 bits, por lo que existen 2^{56} posibles llaves [¡muy pocas!]
- La tecnología actual obliga a tener una seguridad de más de 80 bits.

Breve recuento histórico



Teoría Elemental de Números (1/2)

- Euclides: Máximo común divisor [circa 300AC]
- Eratóstenes: Criba para hallar números primos [circa 220 AC]
- Fibonacci: algoritmo de factorización de números enteros [circa 1200 DC]

Teoría Elemental de Números (2/2)

- Fermat: teoremas de números primos y factorización [circa 1630 DC]
- Euler: generalización del teorema petit de Fermat [circa 1750 DC]
- Gauss: nuevos algoritmos de factorización [circa 1820 DC]

Algunos cifradores clásicos

- Escítala : Método de cifrado por transposición [Esparta, circa 650 AC]
- Códigos César: Método de cifrado por sustitución mono-alfabético [Imperio romano, circa 50AC]
- Cifrador mono-alfabético Babington: Utilizado por María I, reina de los escoceses [1542 DC]

Cifrador por Substitución mono-alfabética

- El alfabeto de cifrado consiste en un reordenamiento del alfabeto del texto original. Así cada letra del alfabeto original es siempre reemplazada por una misma letra del alfabeto de cifrado.
- En el alfabeto castellano hay un total de 27! llaves distintas.

Ejemplo famoso: The gold-bug

53++!305))6*;4826)4+.)4+);806*;48!8`60))85;]8*:+*8!83(88)5*!;
46(;88*96*?;8)*+(;485);5*!2:*+(;4956*2(5*-4)8`8*; 4069285);)6
!8)4++;1(+9;48081;8:8+1;48!85;4)485!528806*81(+9;48;(88;4(+?3
4;48)4+;161;:188;+?;

cifra

'A good glass in the bishop's hostel in the devil's seat twenty-one degrees and thirteen minutes northeast and by north main branch seventh limb east side shoot from the left eye of the death's-head a bee line from the tree through the shot fifty feet out.'

Texto en claro

Edgar Allan Poe (1809-1849)

Nacimiento del criptoanálisis

- Al-kindi [Bagdad, Siglo IX]: inventó el *análisis por frecuencia* . Se aplica con éxito contra cifradores por substitución aprovechando la estructura del idioma en el que el texto original fue escrito.
- El análisis de frecuencia es capaz de *romper* cualquier cifrador por substitución mono-alfabética.
- En los siguientes 600 años, no se logró hallar ningún nuevo esquema de cifrado capaz de resistir este ataque.

Le chiffre indéchiffrable

- Basado en ideas propuestas por Alberti a mediados del siglo XV, Blaise de Vigenère propuso en 1562 un cifrador que juzgó indescifrable.
- El cifrador de Vigènere fue el primer cifrador por substitución poli-alfabética de que se tenga registro. Permanecería invencible por los siguiente tres siglos.

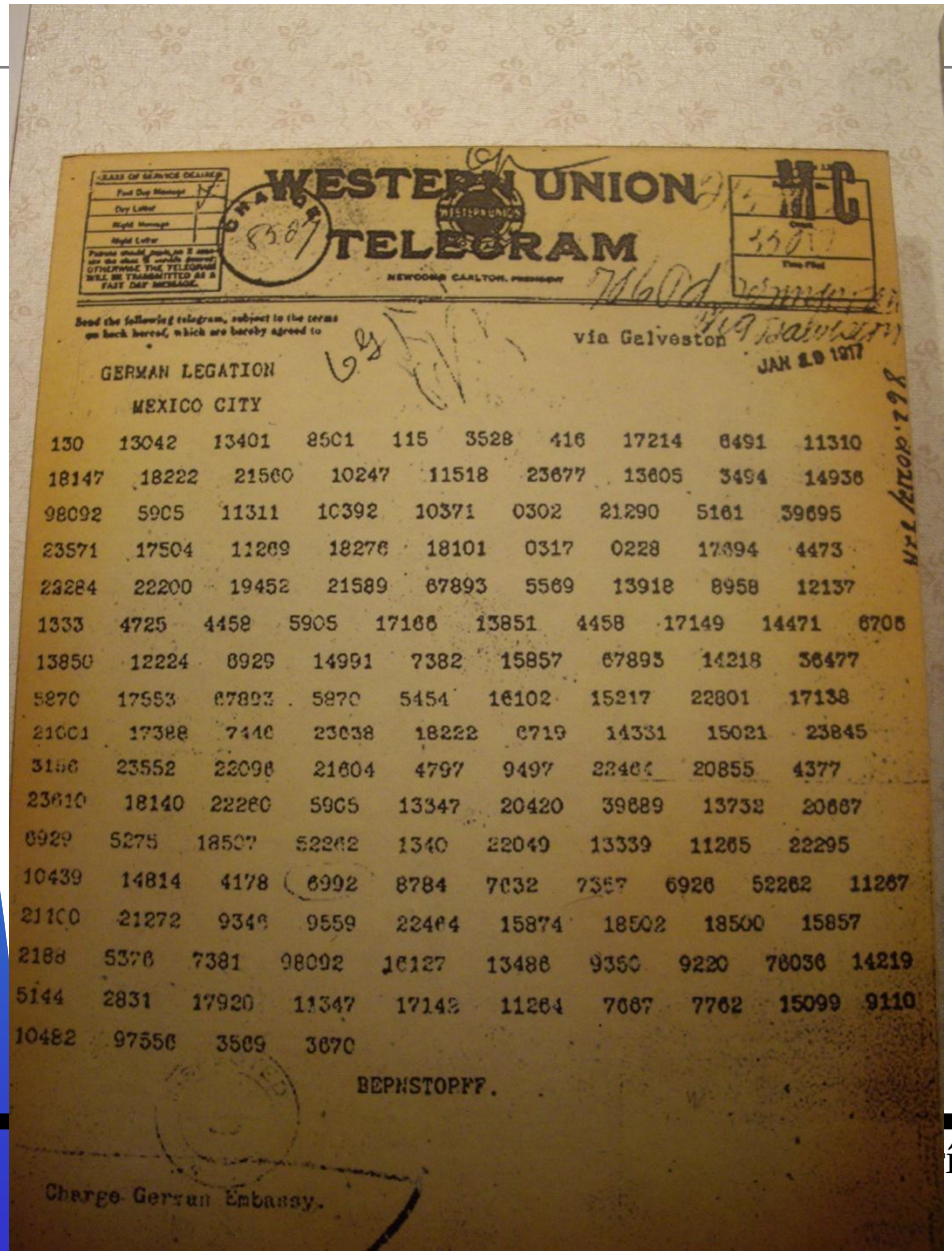
El rompimiento del cifrador de Vigènere

- Charles Babbage logró romper en 1854 el cifrador de Vigènere.
- Su descubrimiento nunca fue publicado por motivos de seguridad nacional de su país [Inglaterra]
- Es al científico prusiano Kasiski a quien se le acredita históricamente el haber logrado romper el cifrador de Vigènere.

¿El criptosistema Perfecto?

•En la práctica casi todos los criptosistemas pueden teóricamente ser rotos si se cuenta con tiempo y recursos computacionales suficientes.
•Sin embargo, hay un criptosistema que es considerado teóricamente invulnerable: One-time-pad (OTP) [Vernam 1917].
•Claude Shannon demostró en 1948 que su seguridad es teóricamente perfecta.
•Su seguridad es perfecta siempre y cuando la llave fue generada de una manera puramente aleatoria.
•OTP requiere un intercambio de llave con una longitud igual a la del texto en claro (¡Esto lo vuelve impráctico!)

El telegrama de Zimmermann



WESTERN UNION
TELEGRAM

via Galveston
JAN 19 1917

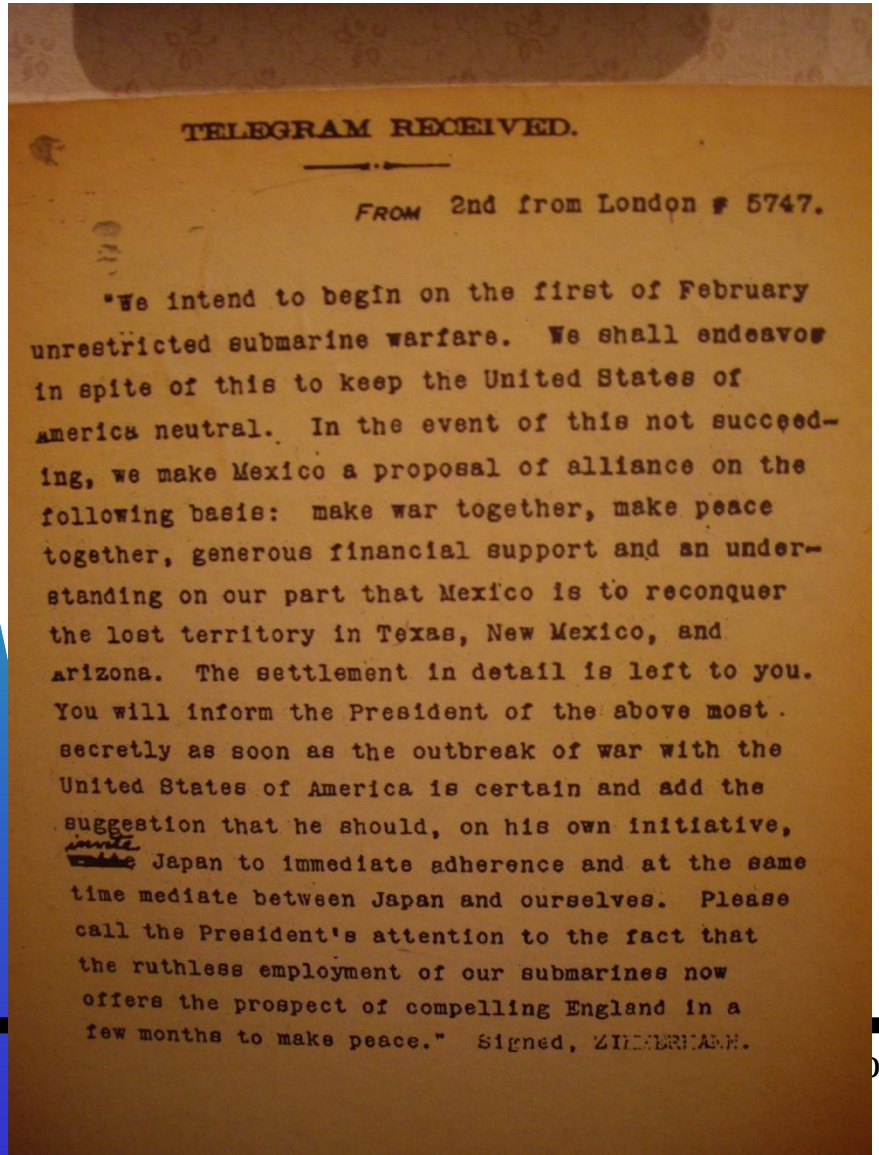
GERMAN LEGATION
MEXICO CITY

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 22098 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.

El Telegrama de Zimmermann



TELEGRAM RECEIVED.

FROM 2nd from London # 5747.

"We intend to begin on the first of February unrestricted submarine warfare. We shall endeavor in spite of this to keep the United States of America neutral. In the event of this not succeeding, we make Mexico a proposal of alliance on the following basis: make war together, make peace together, generous financial support and an understanding on our part that Mexico is to reconquer the lost territory in Texas, New Mexico, and Arizona. The settlement in detail is left to you. You will inform the President of the above most secretly as soon as the outbreak of war with the United States of America is certain and add the suggestion that he should, on his own initiative, invite Japan to immediate adherence and at the same time mediate between Japan and ourselves. Please call the President's attention to the fact that the ruthless employment of our submarines now offers the prospect of compelling England in a few months to make peace." Signed, ZIMMERMANN.

Telegram de Zimmermann

New York Tribune

Germany Asked Mexico To Unite with Japa War on United S

Message from Foreign Secretary Zimmermann t Reveals Astounding Plot to Attack from Borde Nation Should Go to War Over Submarine Crisi New Mexico and Arizona Promised as Rew

No Chance Of War Call By Wilson

with U.S. a Moral aster for Germany

San Francisco Chronicle

LEADING NEWSPAPER of the PACIFIC COAST

GERMANY PLANNED ALLIANCE WITH JAPAN AND MEXICO TO WAGE WAR ON UNITED STATES

THREE STATES TO BE LOOT MEXICO WOULD ANNEX

Here Is President Wilson's Proof of Pact Zimmermann's Letter Held by the U. S.

CALIFORNIAN LOST WHEN LACONIA IS DESTROYED

STATES MAY BE SHORN OF RAILWAY TAX AND CONTROL

LA FOLLETTE IN FIGHT TO BLOCK

America Must Act, Declares Stanford Head

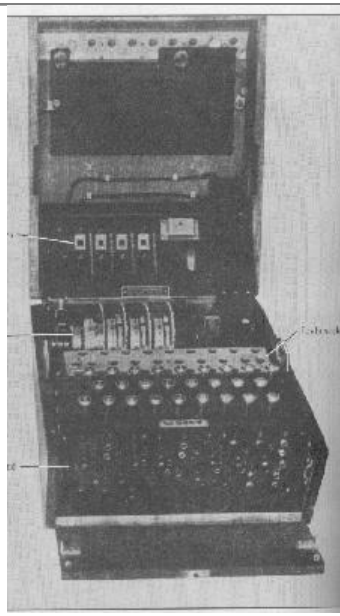
SPECIAL POLICE STAR IS TAKEN, APOLOGY REFUSED

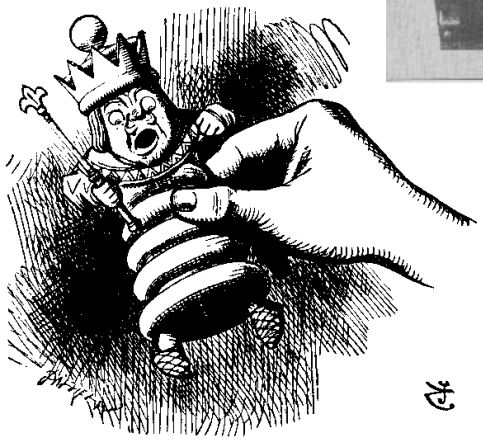
ROMINGER WOULD ABOLISH SALOONS BY AMENDED BILL

Telegrama de Zimmermann

Enigma y Alan Turing

- Enigma fue el cifrador usado por el ejército nazi para enviar comunicados secretos durante la segunda guerra mundial.
- Enigma fue roto por un grupo de inteligencia británico quienes habían recibido ayuda de criptoanalistas polacos.
- Enigma fue roto en una mansión llamada Bletchley Park, donde Alan Turing destaco con ideas brillantes que fueron decisivas para poder romper a Enigma.

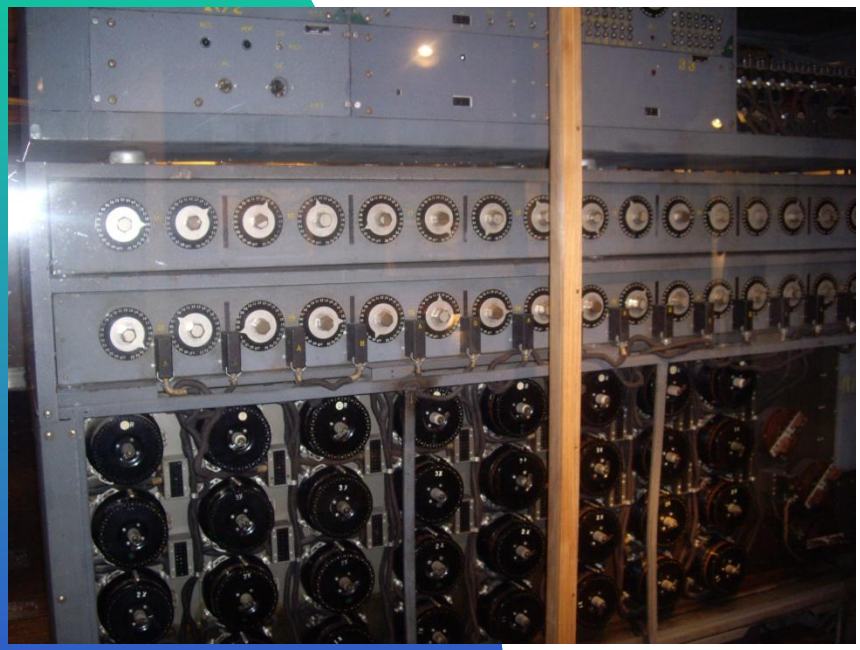


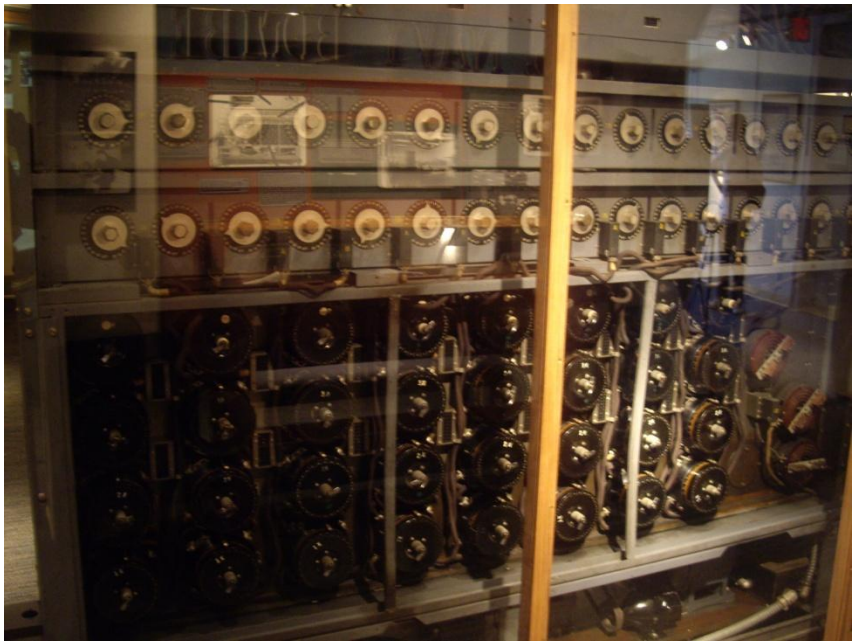


Enigma

Enigma: Fue un dispositivo utilizado durante la segunda guerra mundial por la Alemania nazi. Se tenía tal confianza en la fortaleza de Enigma que el alto comandoAlemán decidió utilizarlo en todos los mensajes codificados antes y durante la guerra.

Enigma





Purple

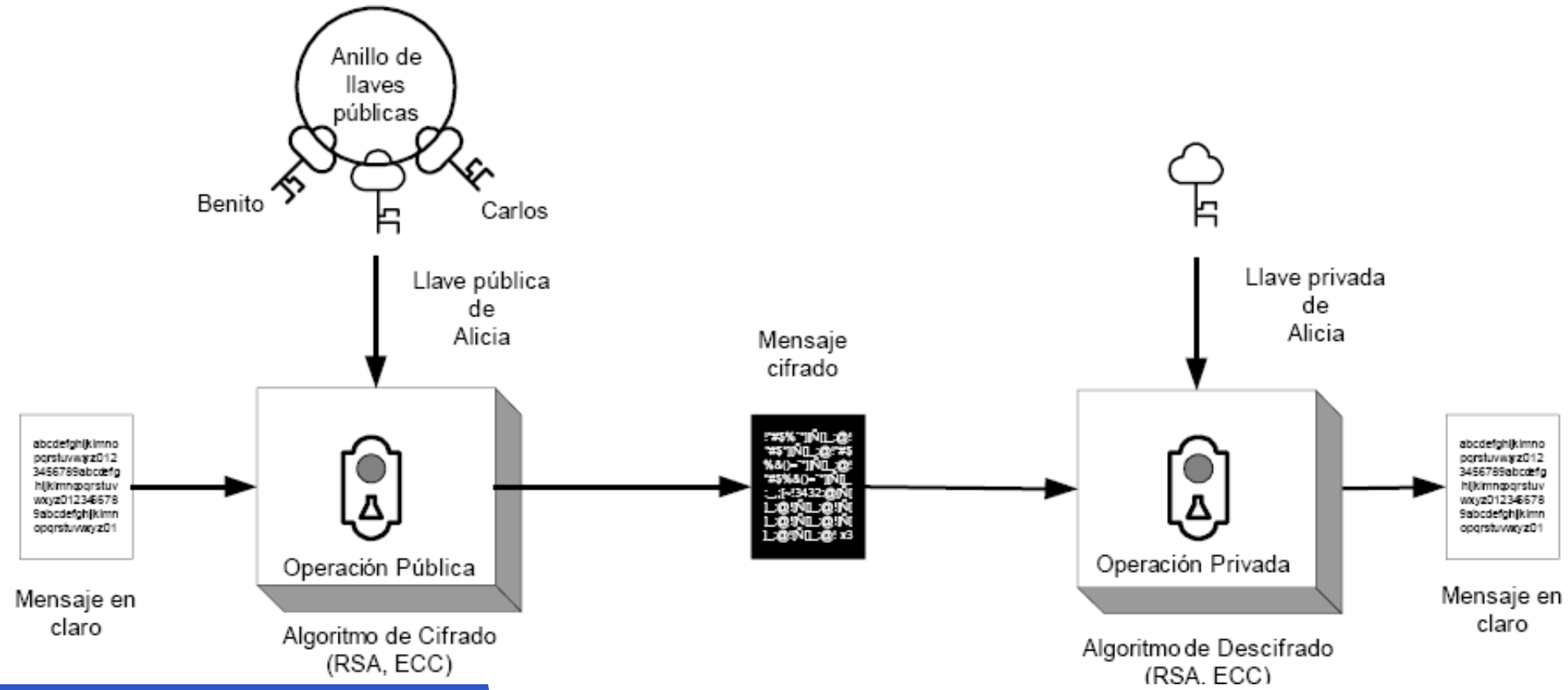
Claude Shannon alquimista

- En 1948 Shannon publicó el artículo: “A Mathematical Theory of Communication”, donde introdujo el concepto de la entropía de la información y con ello inventó el campo de teoría de la información.
- Al año siguiente publicó el artículo: “Communication Theory of Secrecy Systems”, con lo cual la criptografía pasó de ser un oficio a ser una disciplina científica. En ese artículo, Shannon demostró la seguridad perfecta del cripto-esquema “One-time pad” de Vernam usado en la primera guerra mundial.

Alicia y Betito se vuelven públicos

Francisco Rodríguez Henríquez

Criptografía de llave pública



Criptosistemas asimétricos o de llave pública

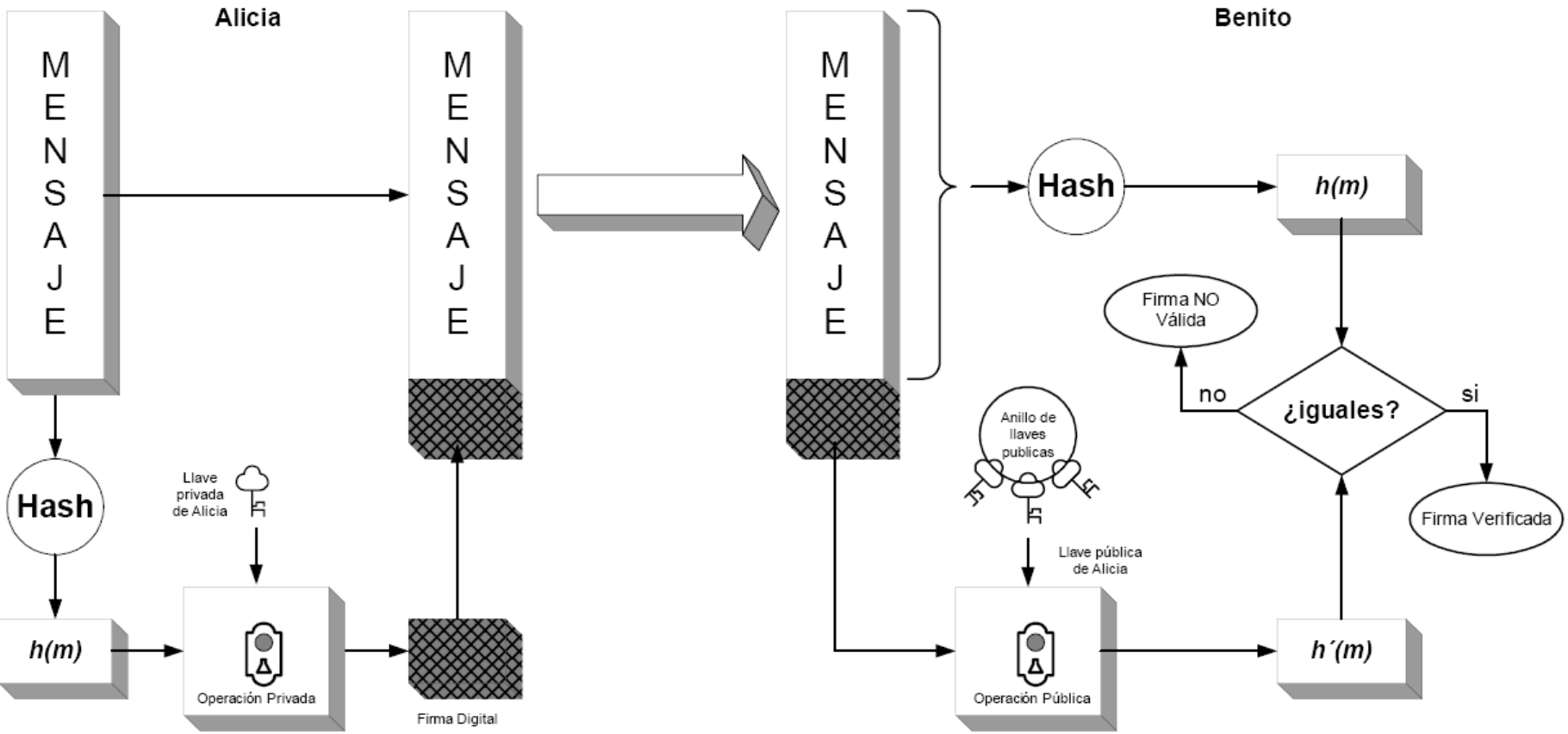
¿Para qué?

El problema de distribución y administración de llaves es difícil e ineficiente en criptosistemas simétricos cuando actúan en redes con muchos nodos.

Los criptosistemas asimétricos permiten implementar otras Primitivas digitales entre las que destacan:

- firma/verificación digital.
- No repudio
- Autenticación

Firma/verificación digital



Merkle, Hellman, Diffie

Rivest, Shamir, Addleman (RSA)

CINVESTAV

Criptografía de llave pública

CINVESTAV

•Excelentes herramientas pero con ciertos problemas intrínsecos.
•presentan un alto costo computacional.
•Representan un reto de implementación.
•hasta 2 órdenes de magnitud más lentos que los criptosistemas simétricos, por lo que no se utilizan para cifrar documentos grandes.

Ejemplos de Criptosistemas asimétricos

•RSA
•(EC)DSA
•NTRU
•Emparejamientos

Criptografía de llave pública

Un criptosistema de llave pública está fundamentado en una función $f(x)$ tal que:

Dado x, calcular $y=f(x)$ es fácil

Dado $y=f(x)$, calcular s es difícil

Se dice que $f(x)$ es una función de sólo-ida, donde para decidir qué es difícil utilizamos la teoría de la complejidad. Muchas veces, es la prueba dle tiempo la que decide qué es en verdad difícil.

Ejemplos de funciones de sólo-ida

- Logaritmo Discreto
  - Dados x, a y p, calcular $y=x^a \ mod \ p$ es fácil. Sin embargo, dados y, x y p, calcular a es difícil.
- Factorización
  - Dados x e y, calcular $n=xy$ es fácil. Sin embargo, dado n, encontrar los factores x e y es difícil.
- Raíz cuadrada discreta
  - Dados x y n, calcular $a=x^2 \ mod \ n$ es fácil. Sin embargo, dados a y n, encontrar x es difícil.

Pasadizos Secretos

- Para poder diseñar un cripto-sistema de llave pública, es necesario añadir una característica extra a la función $y=f(x)$, a saber:

  Dados y y alguna información especial de $f(x)$, calcular x es fácil.

  Dado y sin la información confidencial, computar x es difícil.

En tal caso, decimos que $f(x)$ es una función de sólo ida con pasadizo secreto, donde la información especial es el pasadizo secreto.

Colección de problemas difíciles

- Suma de subconjunto (knapsack)

  $x_i \in \{0,1\},\ 1 \le i \le n,$ tal que $s = \sum_{i=1}^{n} a_i x_i$

- Problema de factorización entera
  - Encuentre divisores primos de un entero n
- Residuo cuadrático
  - $a = x^2 \ (mod\ n)$
- Logaritmo discreto
  - $x = log_{\alpha} \beta$ en el grupo G (e.g. Z_p^*)

Colección de problemas difíciles

- Problema de RSA
  - $c = m^e \pmod n$, $n=pq$, $gcd(e,(p-1)(q-1))=1$
  - $x^{\phi(n)} = 1 \pmod n$ with $gcd(x,n)=1$
- Curvas elípticas
  - P,Q in $E(F_q)$, con $ord(P)=n$, $Q=mP$
  - Encuentre el entero m con $0 \leq m \leq n$

Logaritmo discreto y problemas de Diffie-Hellman

- Sea $G_1 = \langle P \rangle$ un grupo aditivo de orden n. Entonces:

El problema del logaritmo discreto (PLD) en G_1 es:

Dados n, P, $Q \in \langle P \rangle$, encuentre un entero $x \in [0, n-1]$, tal que

$Q = xP$.

El problema de Diffie-Hellman (PDH) en G_1 es:

Dados n, P, aP y bP, encuentre abP.

Emparejamiento Bilineal

Sea n un número primo $G_1 = \langle P \rangle$ un grupo aditivo de orden n con elemento identidad ∞. Sea G_2 un grupo multiplicativo de orden n con elemento identidad 1.

Un emparejamiento bilineal en (G_1, G_2) es una función $\hat{e} = G_1 \times G_1 \rightarrow G_2$, tal que:

1. Para todo $R,S,T \in G_1$: $\hat{e}(S+R,T) = \hat{e}(S,T)\,\hat{e}(R,T)$;

$$\hat{e}(S,R+T) = \hat{e}(S,R)\,\hat{e}(S,T)$$

Además el emparejamiento debe ser no degenerado y fácil de computar.

Emparejamiento Bilineal

Es fácil ver que el PLD en G_1, tiene la misma dificultad que el PLD en G_2. Además se define el problema de Diffie-Hellman Bilineal (PDHB) de la siguiente manera:

Dados P, aP, bP y cP, encuentre $\hat{e}(P,P)^{abc}$.

Se sabe que si el PDH en G_1 es fácil, entonces PDHB también lo es y si acaso el PDH en G_2 es fácil, entonces PDHB también lo es.

No se sabe *más nada* acerca de la dificultad del BDHP.

Criptografía cuántica:

- Como se afirmó en las láminas anteriores la criptografía moderna *presupone* que los problemas matemáticos en que descansan sus esquemas son difíciles.
- Sin embargo, el problema del logaritmo discreto, el problema de RSA, el de Diffie-Hellman y el de curvas elípticas pueden ser todos reducidos al llamado problema del subgrupo escondido HSP.

Criptografía Cuántica

- El algoritmo cuántico de Shor para factorización y logaritmo discreto, puede resolver en tiempo polinomial el problema de HSP.
- Lo anterior implica que las computadoras cuánticas tienen el potencial de romper la gran mayoría de los esquemas criptográficos tradicionales.

Criptografía post-cuántica

Francisco Rodríguez Henríquez

Complejidad Computacional

- Desarrollada a finales de los años sesentas por varios autores ilustres, entre los que destacan:
  - "*On the computational complexity of algorithms*" [Hartmanis & Stearns]
  - "*A Machine Independent Theory of the Complexity of Recursive functions*" [Blum]
  - "Reducibility among Combinatorial Problems" [Karp]

La teoría de la complejidad creó una herramienta para medir la complejidad computacional de los algoritmos. Para efectos prácticos, se le considera el debut de las ciencias Computacionales como ciencia.

Teoría de la Complejidad (1/2)

- ***P***: algoritmos resolubles en tiempo polinomial determinístico.
- ***NP***: algoritmos resolubles en tiempo polinomial no-determinístico.
- ***PSPACE***: algoritmos resolubles en espacio polinomial (tiempo ilimitado, cantidad polinomial de memoria)
- ***BQP***: algoritmos resolubles por una computadora cuántica con una cantidad polinomial de compuertas cuánticas.

Teoría de la Complejidad (2/2)

Se sabe que:

$$P \subseteq NP \subseteq PSPACE$$

$$P \subseteq BQP \subseteq PSPACE$$

Pero no mucho más. En particular una de las preguntas más importantes de la teoría de la complejidad computacional es saber si las clases ***P*** y ***NP*** son equivalentes o no.

Criptografía post-cuántica: ¿Para qué?

- Se puede afirmar que nadie sabe a ciencia cierta qué es la criptografía post-cuántica, pues, por principio de cuentas, nadie conoce bien a bien lo que las computadoras cuánticas podrán hacer [suponiendo que alguna vez puedan hacer algo a gran escala].
- Sin embargo, también es justo decir que hay suficientes dudas existenciales del lado de las computadoras clásicas [por ejemplo: ¿$\boldsymbol{P} \equiv \boldsymbol{NP}$?]
- Y en el caso de la criptografía todos los cripto-esquemas están basados en problemas de los que no se sabe si son intratables o no.

Tres principios de la Criptografía post-cuántica

- Desarrollar criptosistemas basados en problemas matemáticos que sean demostrablemente intratables para computadoras cuánticas. Esto es, si acaso, $\boldsymbol{BQP} \subseteq \boldsymbol{NP}$, buscar problemas que no estén en $\boldsymbol{BQP}$.
- Determinar qué tan práctico es el sistema en una implementación real
- Estimar la complejidad computacional cuántica de los problemas matemáticos intratables

Propuestas de cripto-sistemas post-cuánticos

- Grupos no Abelianos: Problemas de conjugados equivalentes al problema del logaritmo discreto, problema de la palabra [grupos de trenzas]
- Reducción de rejilla: [NTRU]
- Decodificación de síndromes en códigos de corrección de error [sistema McEliece]
- Sistemas cuadráticos multivariables [HFE]

A manera de conclusiones

"He's dreaming now", said Tweedledee: and what do you think he's dreaming about?"
Alice said "Nobody can guess that".
Why, about you!" Tweedledee exclaimed, clapping his hands triumphantly. And if he left to dreaming about you, where do you suppose you'd be?"
Where I am now, of course," said Alice.
Not you!" Tweedledee retorted contemptuously. "You'd be nowhere. Why, you're only a sort of thing in his dream!".

Through the Looking Glass, Lewis Carroll

A manera de Conclusiones

- Desde que Al-Kindi inventara el criptoanálisis por frecuencia en Bagdad en el siglo IX inició, parafraseando al famoso libro, una eterna trenza dorada entre esa disciplina y la criptografía.
- Después de Al-Kindi durante cerca de 600 años los criptoanalistas prevalecieron sobre los criptógrafos. Después con el código de Vigènere, la situación dio la vuelta a favor de estos últimos por cerca de 300 años.
- Tras una larga batalla que duró todo el siglo XX, los criptógrafos

A manera de Conclusiones

- Tras una larga batalla que duró todo el siglo XX, los criptógrafos lograron retomar el control con la invención de la criptografía de llave pública y el desarrollo de modernos cifradores simétricos.
- Sin embargo la nueva arma de los criptoanalistas, el cómputo cuántico luce poderoso y amenaza con volver a cambiar el orden de las cosas.
- Pero ya los criptógrafos se aprestan a contra atacar estudiando métodos post cuánticos.

Y la última palabra es…

¡Gracias!