Que es la CRIPTOLOGIA

2008

Hugo Araya Carrasco

Definición de criptología

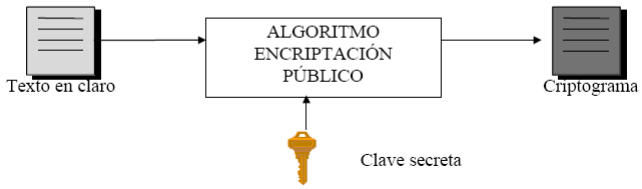
La ***criptología*** está formada por dos técnicas complementarias: ***criptoanálisis y criptografía***.

La criptografía es la técnica de convertir un texto inteligible, texto en claro (plaintext), en otro, llamado criptograma (ciphertext), cuyo contenido de información es igual al anterior, pero sólo lo pueden entender las personas autorizadas.

El criptoanálisis es la técnica de descifrar un criptograma sin tener la autorización.

Hugo Araya Carrasco

Figura 2.2.1



Hugo Araya Carrasco

La palabra criptografía proviene del griego *kryptos*, que significa esconder y *gráphein*, escribir, es decir, escritura escondida. La criptografía ha sido usada a través de los años para mandar mensajes confidenciales cuyo propósito es que sólo las personas autorizadas lo puedan entender el mensaje.

Alguien que quiere mandar información confidencial aplica técnicas criptográficas para poder "esconder" el mensaje (lo llamaremos cifrar o encriptar), manda el mensaje por una línea de comunicación que se supone insegura y después solo el receptor autorizado pueda leer el mensaje "escondido" (lo llamamos descifrar o desencriptar)

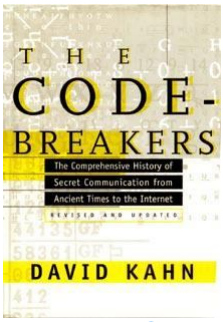
Hugo Araya Carrasco

Desde sus inicios, la criptografía llegó a ser una herramienta muy usada en el ambiente militar, en la segunda gran guerra tuvo un papel determinante, una de las máquinas de cifrado y que tuvo gran popularidad se llamó **ENIGMA**.

Al terminar la guerra las agencias de seguridad de las grandes potencias invirtieron muchos recursos para su investigación.

La criptografía como la conocemos hoy surgió con la invención del computador.

Una buena referencia sobre la historia de la criptografía desde sus inicios hasta la 2° gran guerra se puede encontrar en **D. Kahn**, The Codebreakers, the Story of Secret Writing, Macmillan Publishing Co. NY 1967



Hugo Araya Carrasco

La criptografía actual se inicia en la segunda mitad de la década de los años 70. No es hasta la invención del sistema conocido como **DES** (**D**ata **E**ncryption **S**tandard) en 1976 que se da a conocer más ampliamente, principalmente en el mundo industrial y comercial.

Posteriormente con el sistema **RSA** (**R**ivest, **S**hamir, **A**dleman) en 1978, se abre el comienzo de la criptografía en un gran rango de aplicaciones: en transmisiones militares, en transacciones financieras, en comunicación de satélite, en redes de computadoras, en líneas telefónicas, en transmisiones de televisión etcétera.

La criptografía se divide en dos grandes ramas, la criptografía de clave ***privada o simétrica*** y la criptografía de ***clave pública o asimétrica***, **DES** pertenece al primer grupo y **RSA** al segundo.

Hugo Araya Carrasco

Los principales problemas de seguridad que resuelve la criptografía son: la privacidad, la integridad, la autenticación y el no rechazo.

La privacidad, se refiere a que la información sólo pueda ser leída por personas autorizadas.

La integridad, se refiere a que la información no pueda ser alterada en el transcurso de ser enviada.

La autenticidad, se refiere a que se pueda confirmar que el mensaje recibido haya sido mandado por quien dice lo mando o que el mensaje recibido es el que se esperaba.

El no rechazo, se refiere a que no se pueda negar la autoría de un mensaje enviado.

Hugo Araya Carrasco

Criptografía Simétrica

La criptografía simétrica se refiere al conjunto de métodos que permiten tener comunicación segura entre las partes siempre y cuando anteriormente se hayan intercambiado la clave correspondiente que llamaremos clave simétrica. La simetría se refiere a que las partes tienen la misma llave tanto para cifrar como para descifrar.

Este tipo de criptografía es conocida también como criptografía de clave privada o criptografía de llave privada.

La criptografía simétrica ha sido la más usada en toda la historia, ésta a podido ser implementada en diferente dispositivos, manuales, mecánicos, eléctricos, hasta los algoritmos actuales que son programables en cualquier computador. La idea general es aplicar diferentes funciones al mensaje que se quiere cifrar de tal modo que solo conociendo una clave pueda aplicarse de forma inversa para poder así descifrar.

Hugo Araya Carrasco

El criptoanálisis abarca muchas técnicas diversas, muchas veces no dependen del conocimiento del algoritmo sino que mediante sistemas de aproximación matemática se puede descubrir el texto o la clave. La dificultad del análisis depende de la información disponible, así el criptoanalista puede tener acceso a:

- Un criptograma
- Un criptograma y su texto en claro.
- Un texto claro elegido y su criptograma.
- Un criptograma elegido y su texto en claro.
- Un texto en claro y su criptograma que están los dos elegidos.

Aumenta la dificultad cuanto menos información se tiene. En todos se busca la clave que proporciona la solución para todo el sistema de seguridad.

Hugo Araya Carrasco

En el criptoanálisis científico se utilizan las siguientes definiciones:

Distancia unívoca. Cantidad mínima del mensaje para poder descifrar la clave. Un sistema ideal tiene una distancia unívoca infinita.

Sistema incondicionalmente seguro. El criptograma generado es menor que la distancia unívoca.

Romper un sistema. Conseguir un método práctico para descifrar la clave de un sistema criptográfico.

Sistema probablemente seguro. No se ha probado como romperlo.

Sistema condicionalmente seguro. Los analistas potenciales no disponen de medios para romperlo.

Hugo Araya Carrasco

No existen los sistemas completamente seguros, siempre se pueden violar probando todas las claves posibles. Por lo tanto, en criptografía se buscan sistemas que cumplan una de siguientes condiciones:

✓El **precio** para romperlo es más caro que el **valor** de la información.

✓El **tiempo** necesario para romperlo es más largo que el **tiempo de vida** de la información.

Hugo Araya Carrasco

Ejemplos de criptoanálisis:

Sistema de prueba y ensayo.

Se prueban todas las claves posibles. Es el más utilizado pero el menos científico. Se puede hacer siguiendo una lógica (nombres propios, geográficos, etc…) o aleatoriamente.

En el caso de no utilizar una lógica se calcula una probabilidad de acierto del 50% de los intentos.

En el sistema DES se utiliza una clave de 56 bits:

Nº de claves 2^{56} = 7,2 x10^{16} claves.

Si una prueba cada 1 micro seg. ==>2^{55} = 1.142 años para encontrar la clave.

Si 10^{6} pruebas cada 1 micro seg. ==> 10,01 horas para encontrar la clave.

Hugo Araya Carrasco

Métodos estadísticos.

Son los métodos tradicionales, es mejor que prueba y ensayo pero sólo sirve para algoritmos actualmente en desuso. Aprovechan la estadística de la fuente.

En un texto de lengua castellana, la estadística de las letras más comunes es:

16,8% → E
12% → A.
8,7% → 0.
8% → L y S.

Si el sistema substituye las letras por otros símbolos, utilizando la frecuencia de aparición es muy fácil detectar la correspondencia entre símbolo y letra.

Hugo Araya Carrasco

Algo de Historia de la criptología

Método Julio Cesar

Es el más antiguo conocido. La época de Julio Cesar es la primera que se tiene noticia de la popularización de la escritura de un idioma, el latín, ya que éste tuvo una gran difusión entre diferentes ejércitos y clases sociales. Así apareció la necesidad de ocultar información escrita y, por lo tanto, de la criptología.
El sistema reemplaza cada letra por la situada tres posiciones delante en el alfabeto. Por ejemplo:

B => E
Y => A

LLEGUE VI VENCI => OOHJXH YL YHQFL

Es fácil de romper:

- Prueba y ensayo con 26 intentos.
- Métodos estadísticos.

Hugo Araya Carrasco

Sistemas monoalfabéticos

Sustituyen cada letra por otra que ocupa la misma posición en un alfabeto desordenado, así se consiguen tantas claves como posibilidades de alfabetos hay:

Nº de claves 26! = $4x10^{26}$

Es mucho mejor que el de Julio Cesar y tiene más claves que el sistema más utilizado actualmente DES (**2^{56} = $7,2x10^{16}$** claves). No se puede utilizar prueba y ensayo para romperlo.

El problema está en **cómo recordar la clave**, es decir, el alfabeto desordenado. Para ello se utiliza una palabra de uso común que permite crear, con un algoritmo conocido, el alfabeto desordenado. Entonces, **en la práctica**, las claves posibles no son los alfabetos sino que las palabras fáciles de recordar, **muchas menos que 26!**.

Hugo Araya Carrasco

El sistema es el siguiente:

1. Se busca una palabra (clave) fácil de recordar y se le quitan las letras duplicadas. **SEGURIDAD => SEGURIDA**
2. Se añaden al final de la palabra las restantes letras del alfabeto. **SEGURIDABCFH.....XYZ**
3. Se ordenan en una matriz cuya primera fila es la palabra clave

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

4. El nuevo alfabeto se lee por columnas

YNBSZOCEPFGQHUTJRVKIWLDXMA

Hugo Araya Carrasco

Con este método la clave es más fácil de transmitir y recordar pero el sistema de prueba y ensayo se reduce a todas las palabras conocidas. El sistema de criptoanálisis mejor para romper el algoritmo es el **estadístico**.

Diseñar un programa que implemente el algoritmo monoalfabetico.

Diseñar un programa que dado un mensaje encriptado con el método Monoalfabetico intente desencriptarlo.

Hugo Araya Carrasco

Metodo Playfair

Inventado por el británico Ser Charles Wheatstone en 1854. Es un sistema **monoalfabético de digramas** (grupos de dos letras). Utiliza una palabra clave y una matriz de 5x5.

Ejemplo

CLAVE: SEGURIDAD => SEGURIDA

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

I / J comparten celda

Hugo Araya Carrasco

Método de encriptación:

1. Las palabras se separan en digramas. Un digrama nunca puede tener dos letras repetidas, en ese caso se pone una de relleno (X).
Ejemplo: LLAVE => LXLAVE.

2. Si las dos letras están en la misma fila se reemplazan por la siguiente de la derecha, las filas tienen continuidad mediante un sistema circular. Ejemplo: ER => GS

3. Si las dos letras están en la misma columna se sustituyen por la inmediata inferior, siguiendo un sistema circular.
Ejemplo: BY => LU

4. En los casos restantes se sustituye cada letra por la correspondiente de misma fila y la columna de la otra letra del digrama.
Ejemplo: LE => HU

Hugo Araya Carrasco

Ventajas:

- Utiliza digramas, 26 x 26 = 676 símbolos.
- La identificación individual es muy difícil.
- Métodos estadísticos de criptoanálisis complicados.

Durante muchos años se consideró irrompible. Fue utilizado por la armada inglesa y de USA en las dos guerras mundiales. En realidad el sistema mejora la estadística pero sigue pareciéndose al texto en claro, sobre todo, para las letras poco frecuentes. Por lo tanto, con computadores se puede romper fácilmente.

Hugo Araya Carrasco

Criptografía Visual

Una idea ingeniosa de usar un método de comparición de secretos con un esquemas límite (n,k) es la criptografía visual, esto consiste en lo siguiente: una imagen es partida en n partes, y si se sobreponen al menos k de estas partes se puede reconstruir la imagen.

Veamos en ejemplo de un esquema (2,2), esto trabaja considerando que si la imagen es de banco y negro, entonces la imagen podrá ser un conjunto de cuadros completamente negros y completamente blancos, por ejemplo la siguiente imagen

Hugo Araya Carrasco

Ahora cada cuadro de la imagen podrá ser considerado como blanco o negro, equivalentemente con valores 0 y 1. Para partir esta imagen en dos partes $n=2$ y considerando el límite con $k=2$, se procede como sigue.

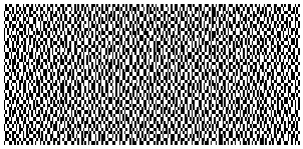
Cada cuadro que es completamente negro podrá ser partido en dos partes de la siguiente forma:

Y un cuadro completamente blando podrá ser partido en dos de la

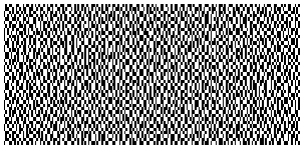
Hugo Araya Carrasco

Que significa suma módulo 2, es decir 1+0=1, 0+1=1, 0+0=0 pero también 1+1=0, de este modo se pueden tomar cualquiera de las dos particiones de los cuadros de color blanco.

Para formar las dos partes de la figura en un acetato se elige aleatoriamente una de las combinaciones anteriores según se parta un cuadro blanco o uno negro. En el caso de la figura, elegidas las partes, la figura partida en un esquema limite (2,2) queda así:



Parte 1

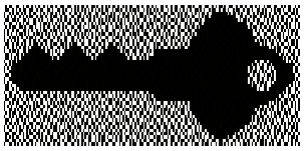


Parte 2

Hugo Araya Carrasco

De esta forma se tiene partida la figura en dos partes y se recuperará solo sobreponiendo una sobre la otra.

Al sobreponer las dos partes se recupera la figura, de la siguiente forma:



En el caso general se parte los cuadros blancos y negros en *n* pedazos y hasta no tener *k* pedazos negros el cuadro reconstruido será siendo blanco, a partir de k pedazos negros hasta *n* el cuadro reconstruido será negro. En nuestro caso, un cuadro con solo la mitad negra será considerado blanco, es necesario que tenga dos mitades negras para que el cuadro reconstruido se considere negro, que es el caso del esquema (2,2).

Hugo Araya Carrasco


Hugo Araya Carrasco