Seguridad Informática Chile

Hackeando la ignorancia, pirateando tu cultura.

Seguridad Informática
Chile

Ransomware Web desde Cero

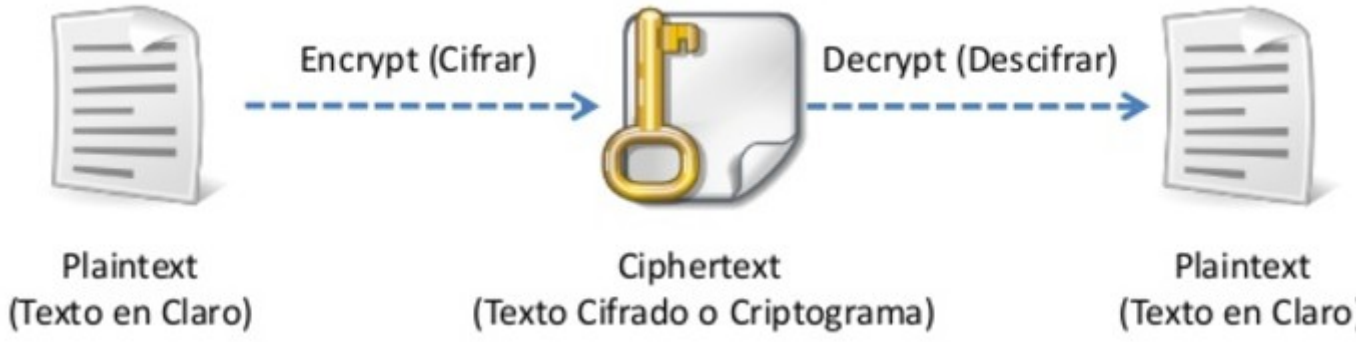
Instructor: Sebastian Veliz Donoso

Sitio: https://cybersecuritylaboratory.wordpress.com/
Contacto: cyslabs@gmail.com
https://www.linkedin.com/in/sebastianvelizdonoso

Contexto del Taller

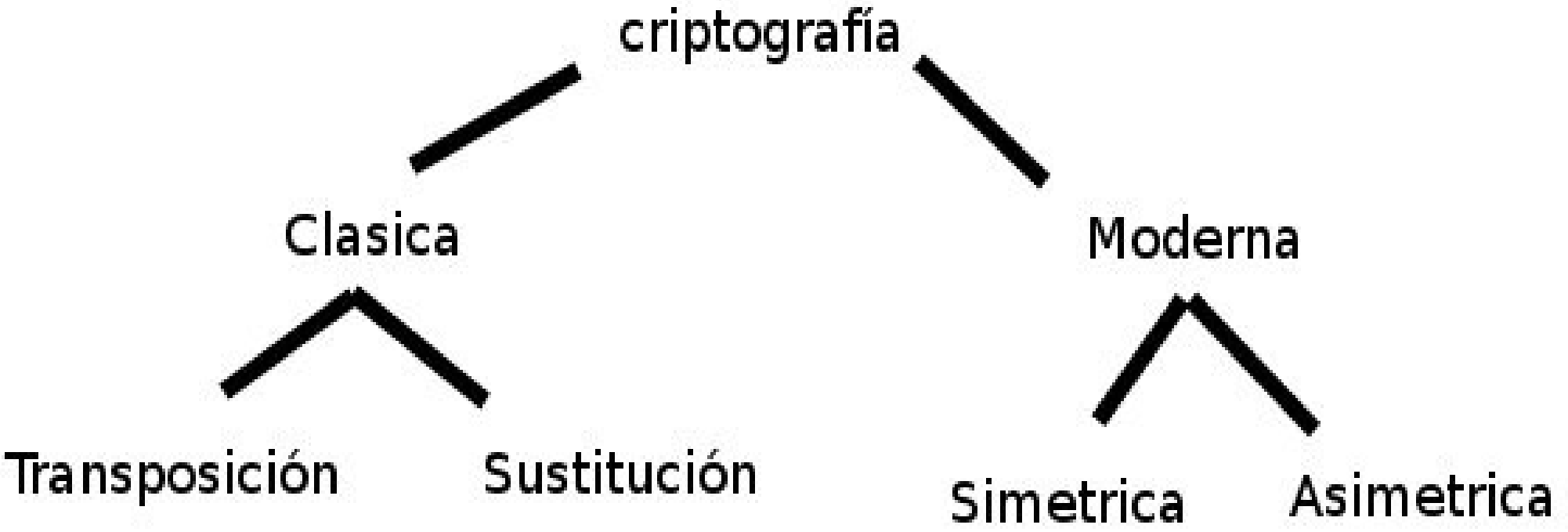
Introducción

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 puedan entender el mensaje.



Seguridad Informática
Chile

Tipos de Criptografía



Criptografía Clásica

los cifrados clásicos operan en un alfabeto de letras (como "A-Z"), a las cuales se les aplican métodos a mano o con aparatos mecánicos muy simples. Son tipos muy básicos de cifrado, lo que no los hace muy fiables

A	B	C	D	E	F	G	H	I	J	K	L	M	N
0	1	2	3	4	5	6	7	8	9	10	11	12	13
Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	
14	15	16	17	18	19	20	21	22	23	24	25	26	

Cifrado por transposición

En criptografía, un cifrado por transposición es un tipo de cifrado en el que unidades de texto plano se cambian de posición siguiendo un esquema bien definido; las 'unidades de texto' pueden ser de una sola letra (el caso más común), pares de letras, tríos de letras, mezclas de lo anterior.

Cifrado por sustitución

En un cifrado por transposición, las unidades del texto plano son cambiadas usando una ordenación diferente y normalmente bastante compleja, pero las unidades en sí mismas no son modificadas. Por el contrario, en un cifrado por sustitución, las unidades del texto plano mantienen el mismo orden, lo que hace es sustituir las propias unidades del texto plano.

Cifrado por sustitución

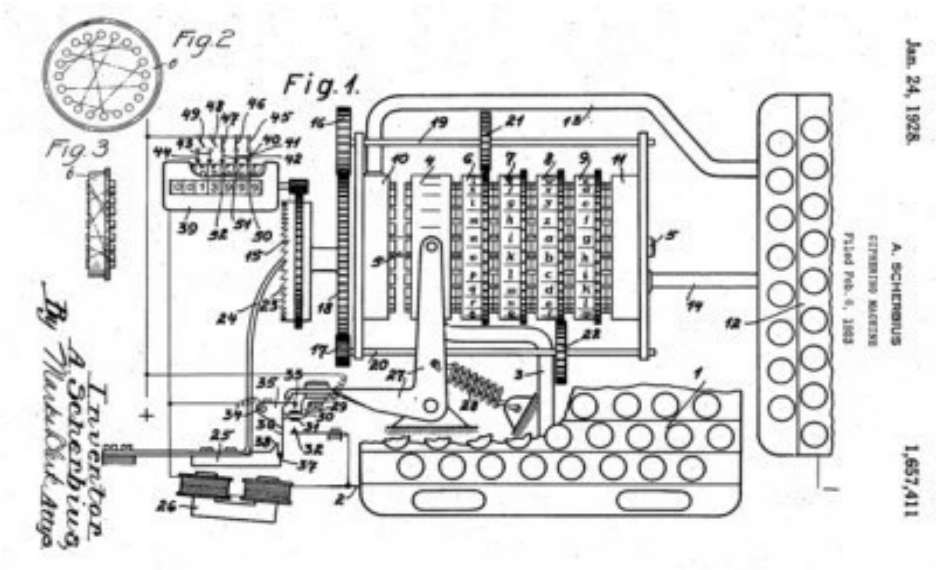
alberti

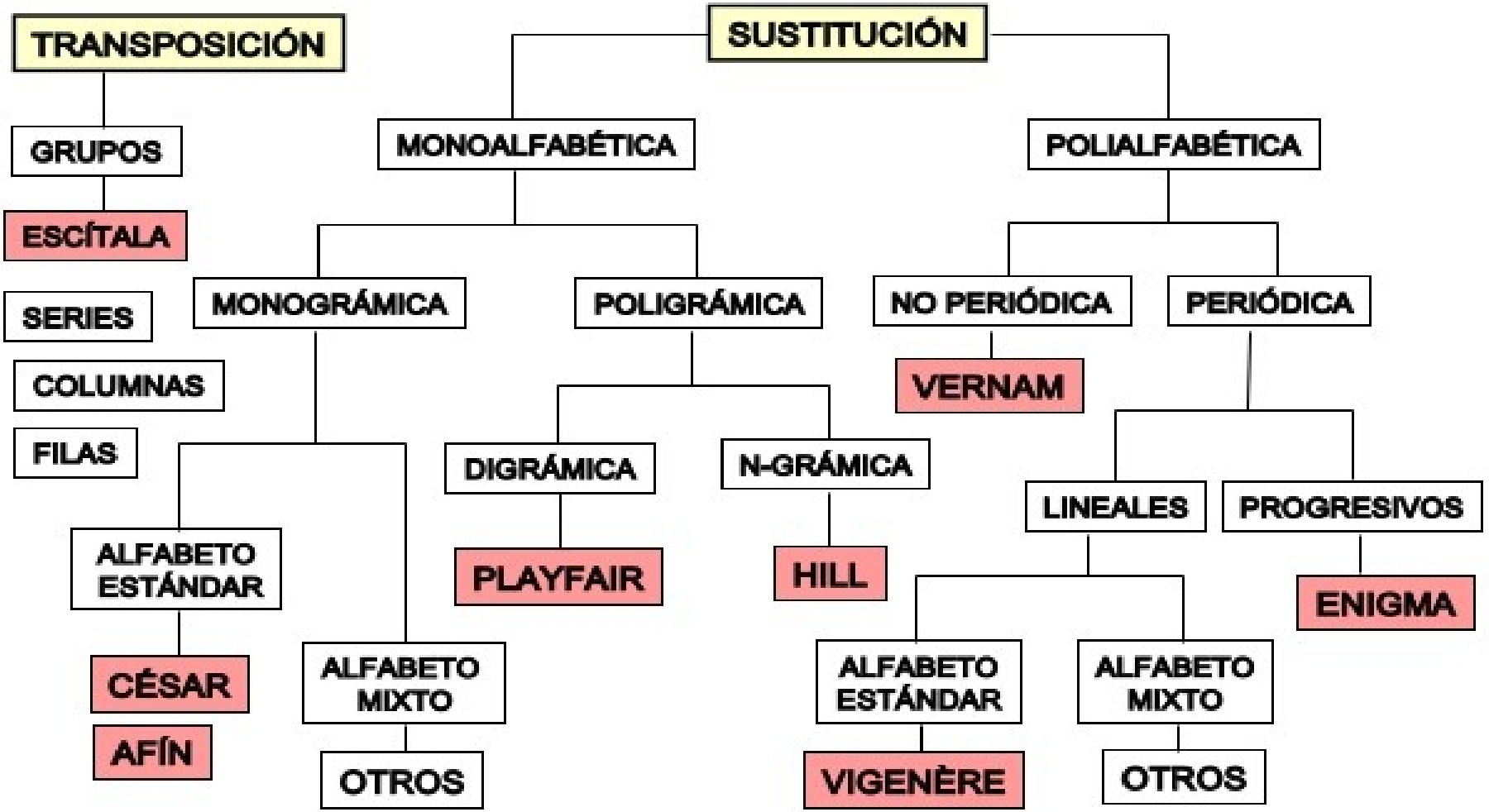
vigenere

	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
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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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

Criptografía de la Segunda Guerra Mundial

En la Segunda Guerra Mundial, las máquinas de cifrado mecánicas y electromecánicas se utilizaban extensamente. Se hicieron grandes avances en la rotura de cifrados, todos en secreto. La información acerca de esta época ha empezado a desclasificarse al llegar a su fin el periodo de secreto británico de 50 años, al abrirse lentamente los archivos estadounidenses y al irse publicando diversas memorias y artículos.




TRANSPOSICIÓN
GRUPOS
ESCÍTALA
SERIES
COLUMNAS
FILAS
SUSTITUCIÓN
MONOALFABÉTICA
POLIALFABÉTICA
MONOGRÁMICA
POLIGRÁMICA
NO PERIÓDICA
PERIÓDICA
VERNAM
DIGRÁMICA
N-GRÁMICA
LINEALES
PROGRESIVOS
ALFABETO ESTÁNDAR
ALFABETO MIXTO
PLAYFAIR
HILL
ENIGMA
CÉSAR
AFÍN
OTROS
ALFABETO ESTÁNDAR
ALFABETO MIXTO
VIGENÈRE
OTROS

Criptografía Moderna

La era de la criptografía moderna **comienza realmente con Claude Shannon**. En 1949 publicó el artículo **Communication Theory of Secrecy Systems** en la Bell System Technical Journal, y poco después el libro Mathematical Theory of Communication, con Warren Weaver.

La criptografía desapareció de la escena para quedarse dentro de las organizaciones gubernamentales dedicadas al espionaje y el contraespionaje. De ellas la más importante fue la NSA de Estados Unidos.

Criptografía Moderna

La NSA **acaparó y bloqueó casi totalmente la publicación de cualquier avance en el campo de la criptografía** desde principios de la década de 1950 hasta mediados de los 70. Por esta razón casi toda la información disponible sobre el tema era la básica y totalmente anticuada.

Criptografía Moderna

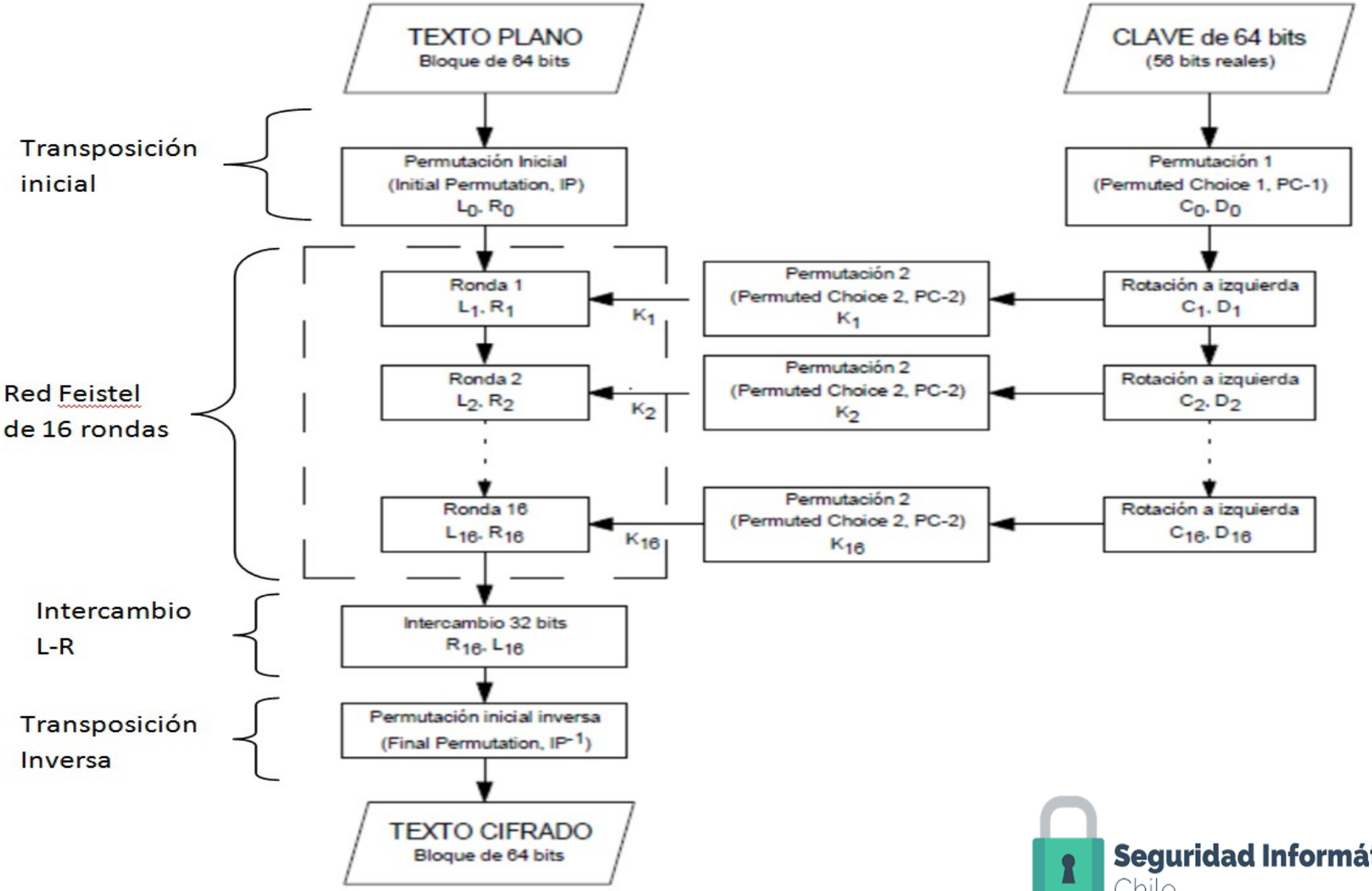
A mediados de los 70 se vivieron dos importantes avances públicos. El primero fue la publicación del borrador del **Data Encryption Standard** en el Registro Federal estadounidense el 17 de marzo de 1975. La propuesta fue enviada por IBM, por invitación de la Oficina Nacional de Estándares (ahora NIST), en un esfuerzo por desarrollar sistemas de comunicación electrónica segura para las empresas como los bancos y otras organizaciones financieras grandes.

Criptografía Moderna

A mediados de los 70 se vivieron dos importantes avances públicos. El primero fue la publicación del borrador del **Data Encryption Standard** en el Registro Federal estadounidense el 17 de marzo de 1975. La propuesta fue enviada por IBM, por invitación de la Oficina Nacional de Estándares (ahora NIST), en un esfuerzo por desarrollar sistemas de comunicación electrónica segura para las empresas como los bancos y otras organizaciones financieras grandes.

Criptografía simétrica

DES- Data Encryption Standard

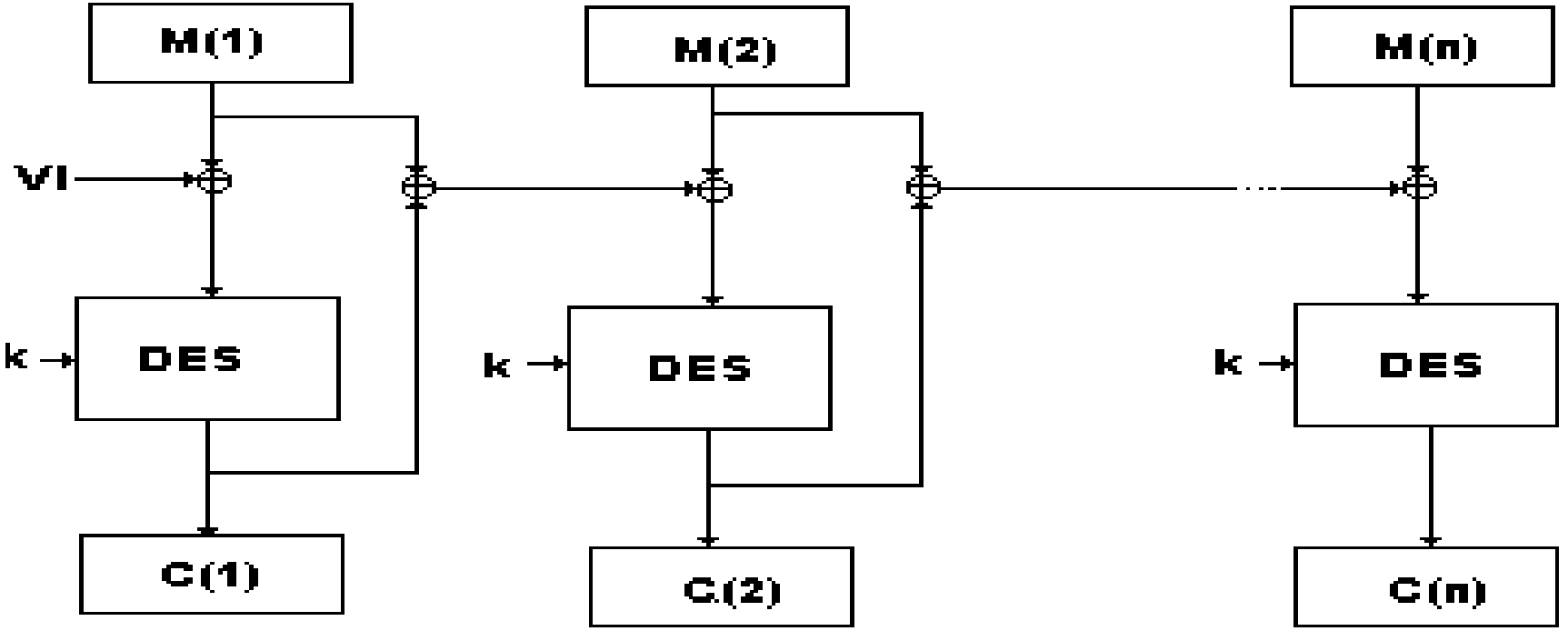


DES- Data Encryption Standard

Se ha demostrado que el tamaño de su clave, 56 bits, es insuficiente ante ataques de fuerza bruta (un ataque así, llevado a cabo por el grupo pro libertades civiles digitales Electronic Frontier Foundation en 1997, **tuvo éxito en 56 horas.**

Algunas fuentes dicen que fue por culpa de la NSA, que pidió reducir de los 128 bits iniciales a 64 y después hasta los 56

Triple DES



La variante más simple del Triple DES funciona de la siguiente manera:

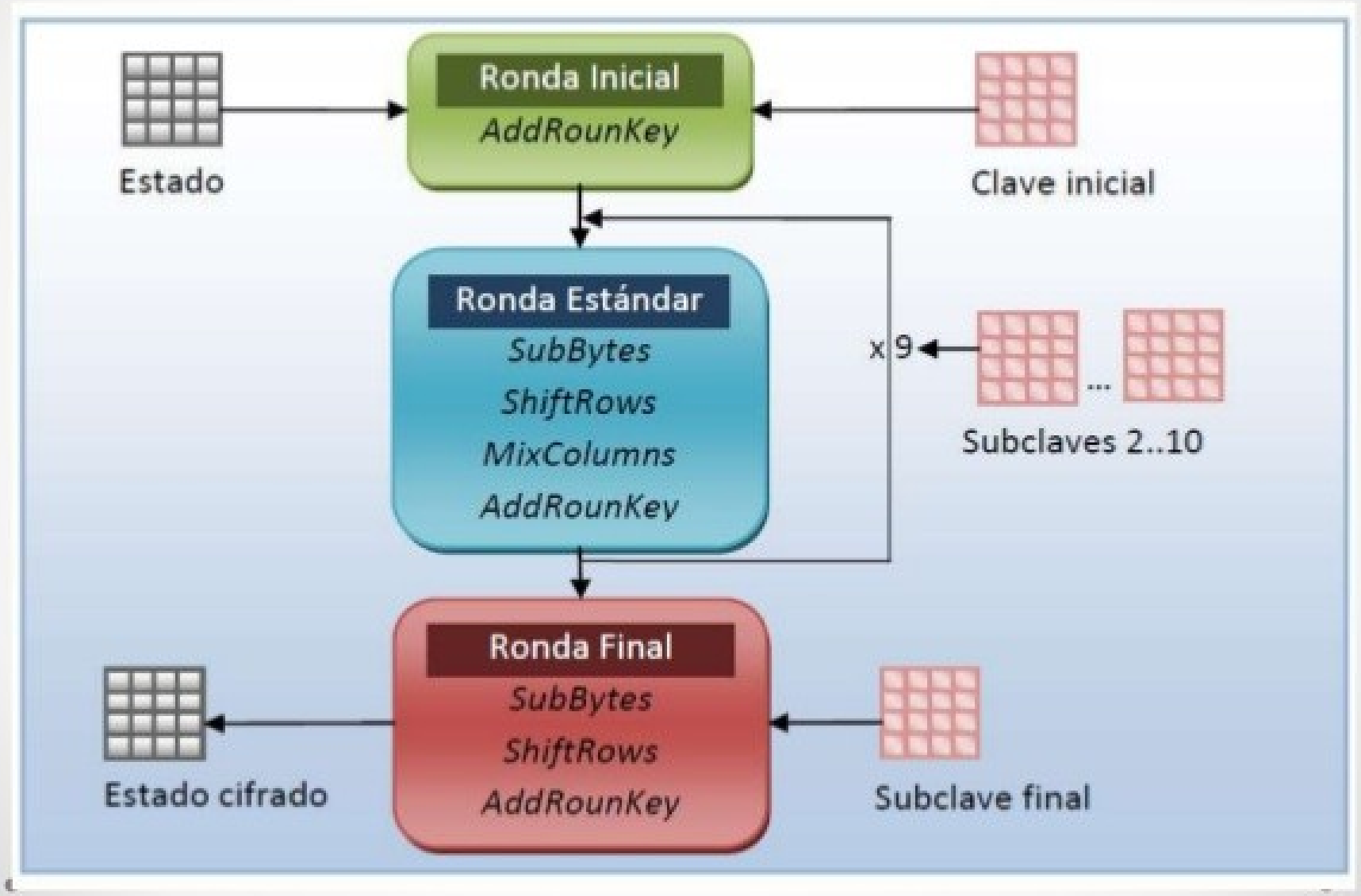
Ecuación 1 Cifrado del TDES

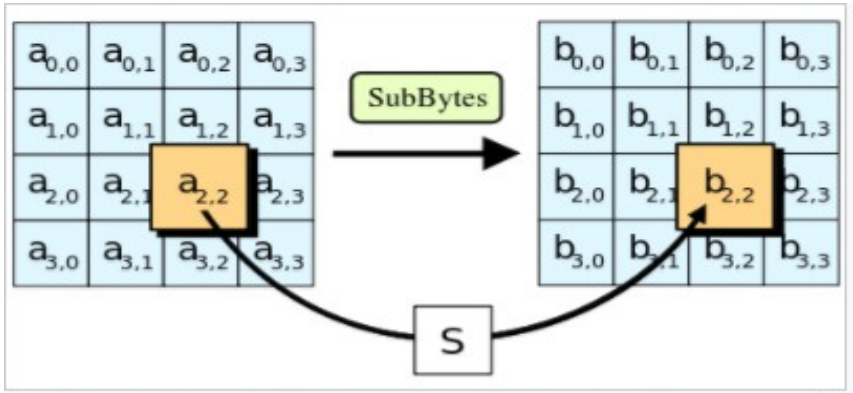
$$C = E_{DES}^{k3}\left(D_{DES}^{k2}\left(E_{DES}^{k1}(M)\right)\right)$$

AES - Advanced Encryption Standard

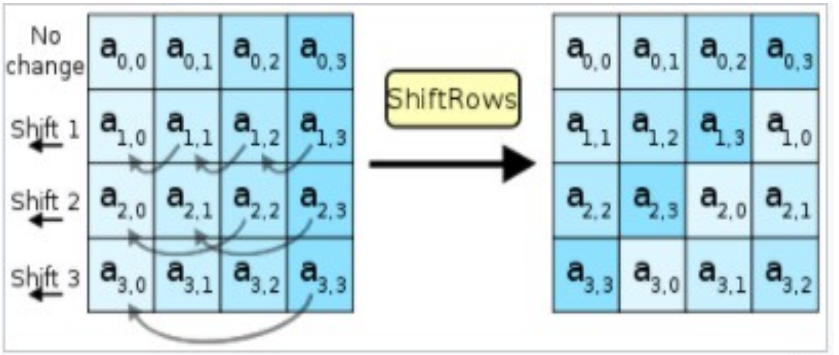
DES fue suplantado oficialmente por el Advanced Encryption Standard (AES) en 2001, cuando el NIST anunció el FIPS 197. Tras una competición abierta, el NIST seleccionó el algoritmo Rijndael, enviado por dos criptógrafos belgas, para convertirse en el AES.

Esquema general del AES

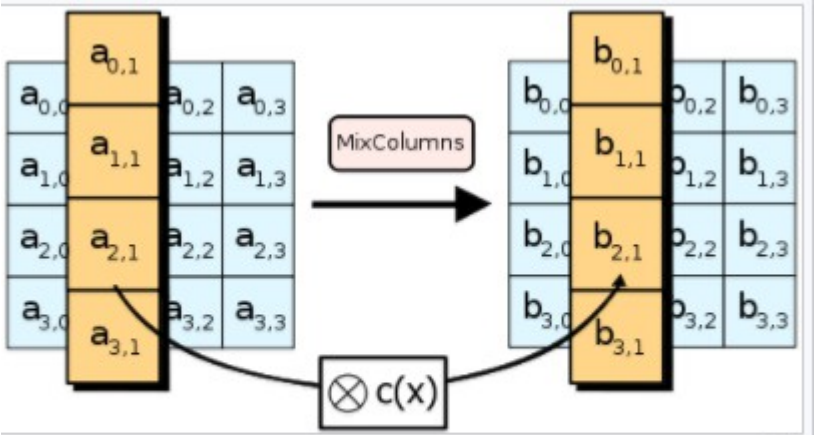




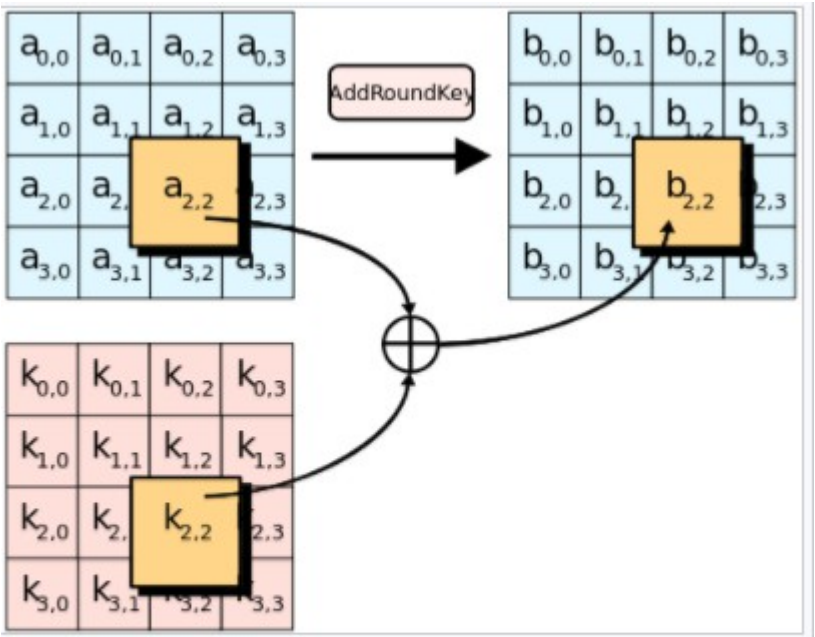
En la fase de `SubBytes`, cada byte en el state es reemplazado con su entrada en una tabla de búsqueda fija de 8 bits, *S*; $b_{ij} = S(a_{ij})$.



En el paso `ShiftRows`, los bytes en cada fila del state son rotados de manera cíclica hacia la izquierda. El número de lugares que cada byte es rotado difiere para cada fila.



En el paso `MixColumns`, cada columna del state es multiplicada por un polinomio constante *c(x)*.



En el paso `AddRoundKey`, cada byte del state se combina con un byte de la subclave usando la operación XOR (⊕).

Modos de operación de una unidad de cifrado por bloques

- **Modo ECB (Electronic codebook)**: El método más simple de modo de cifrado es el llamado ECB (electronic codebook), en el cual el mensaje es dividido en bloques, cada uno de los cuales es cifrado de manera separada. La desventaja de este método es que bloques idénticos de mensaje sin cifrar producirán idénticos textos cifrados. Por esto, no proporciona una auténtica confidencialidad y no es recomendado para protocolos criptográficos, como apunte no usa el vector de inicialización (IV).
- **Modo CBC (Cipher-block chaining)**: En el modo CBC (cipher-block chaining), antes de ser cifrado, a cada bloque de texto se le aplica una operación XOR con el previo bloque ya cifrado. De este modo, cada bloque cifrado depende de todos los bloques de texto claros usados hasta ese punto. Además, para hacer cada mensaje único se debe usar un vector de inicialización en el primer bloque.
- Modo PCBC (Propagating cipher-block chaining): El modo propagating cipher-block chaining fue diseñado para que pequeños cambios en el texto cifrado se propagasen más que en el modo CBC.
- **Modo OFB (Output feedback):** El modo OFB (output feedback) emplea una clave para crear un bloque pseudoaleatorio que es operado a través de XOR con el texto claro para generar el texto cifrado. Requiere de un vector de inicialización que debe ser único para cada ejecución realizada.

AES - Advanced Encryption Standard

El mayor problema que presenta el AES es el número de rondas, que se considera muy bajo para lo que debería ser un algoritmo “seguro”, con 10 rondas para claves de 128 bits, 12 rondas para claves de 192 bits y 14 rondas para claves de 256 bits).

La NSA, cuyos archivos SECRET se cifran con una clave de 128 bits, mientras que los TOP SECRET han de ser cifrados como mínimo con una de 192 bits.

Criptografía Asimétrica

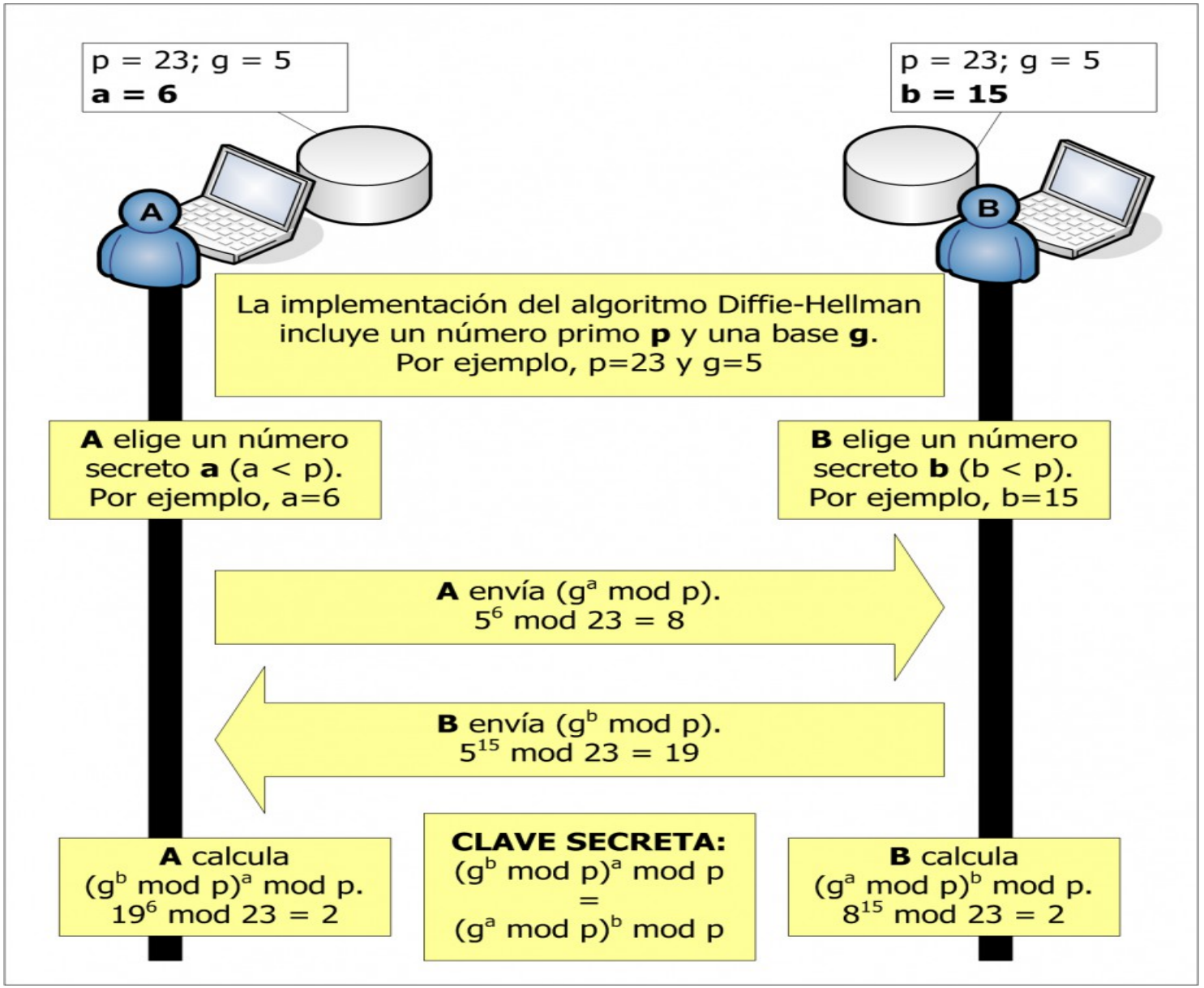
En 1976 se hizo público el artículo New Directions in Cryptography, de **Whitfield Diffie y Martin Hellman**. Este artículo cambió de manera fundamental la forma en la que los criptosistemas pueden funcionar. Introdujo un método radicalmente nuevo para distribuir las claves criptográficas, dando un gran paso adelante para resolver uno de los problemas fundamentales de la criptografía, la distribución de claves, y ha terminado llamándose intercambio de claves Diffie-Hellman.

Criptografía Asimétrica

Ejemplo de cifrado de mensaje: ***Ana envía un mensaje a David***

1. Ana redacta un mensaje
2. Ana cifra el mensaje con la **clave pública** de David
3. Ana envía el mensaje cifrado a David a través de internet, ya sea por correo electrónico, mensajería instantánea o cualquier otro medio
4. David recibe el mensaje cifrado y lo descifra con su **clave privada**
5. David ya puede leer el mensaje original que le mandó Ana

Diffie-Hellman



Diffie-Hellman

A partir de las ecuaciones anteriores, **intentar calcular los valores de “a” y “b” es lo que se conoce como el problema del algoritmo discreto**, un problema que se cree computacionalmente intratable y cuya notación es la siguiente:

a = log discg (ga mod p) = log disc 5 (8)
b = log discg (gb mod p) = log disc 5 (19)

Con los valores del ejemplo sí que es posible encontrar la solución, ya que se ha escogido un número primo “p” muy pequeño (p = 23), y se sabe que “a” y “b” son menores que “p”. Por lo tanto, para obtener los valores secretos en este ejemplo, un atacante tendría que probar sólo 22 posibles valores.

RSA-Rivest, Shamir y Adleman

En criptografía, RSA (Rivest, Shamir y Adleman) es un sistema criptográfico de clave pública desarrollado en 1977. Es el primer y más utilizado algoritmo de este tipo y es válido tanto para cifrar como para firmar digitalmente.
La seguridad de este algoritmo radica en el problema de la factorización de números enteros. Los mensajes enviados se representan mediante números, y **el funcionamiento se basa en el producto, conocido, de dos números primos grandes elegidos al azar** y mantenidos en secreto. Actualmente estos primos son del orden de **10^200**

RSA-Rivest, Shamir y Adleman

$p = 61$	1° nº primo privado
$q = 53$	2° nº primo privado
$n = pq = 3233$	producto $p \times q$
$e = 17$	exponente público
$d = 2753$	exponente privado

La clave pública es (e, n). La clave privada es (d, n). La función de cifrado es:

$$\mathrm{encrypt}(m) = m^e \pmod{n} = m^{17} \pmod{3233}$$

Donde m es el texto sin cifrar. La función de descifrado es:

$$\mathrm{decrypt}(\mathrm{c}) = c^d \pmod{n} = c^{2753} \pmod{3233}$$

Donde c es el texto cifrado. Para cifrar el valor del texto sin cifrar 123, nosotros calculamos:

$$\mathrm{encrypt}(123) = 123^{17} \pmod{3233} = 855$$

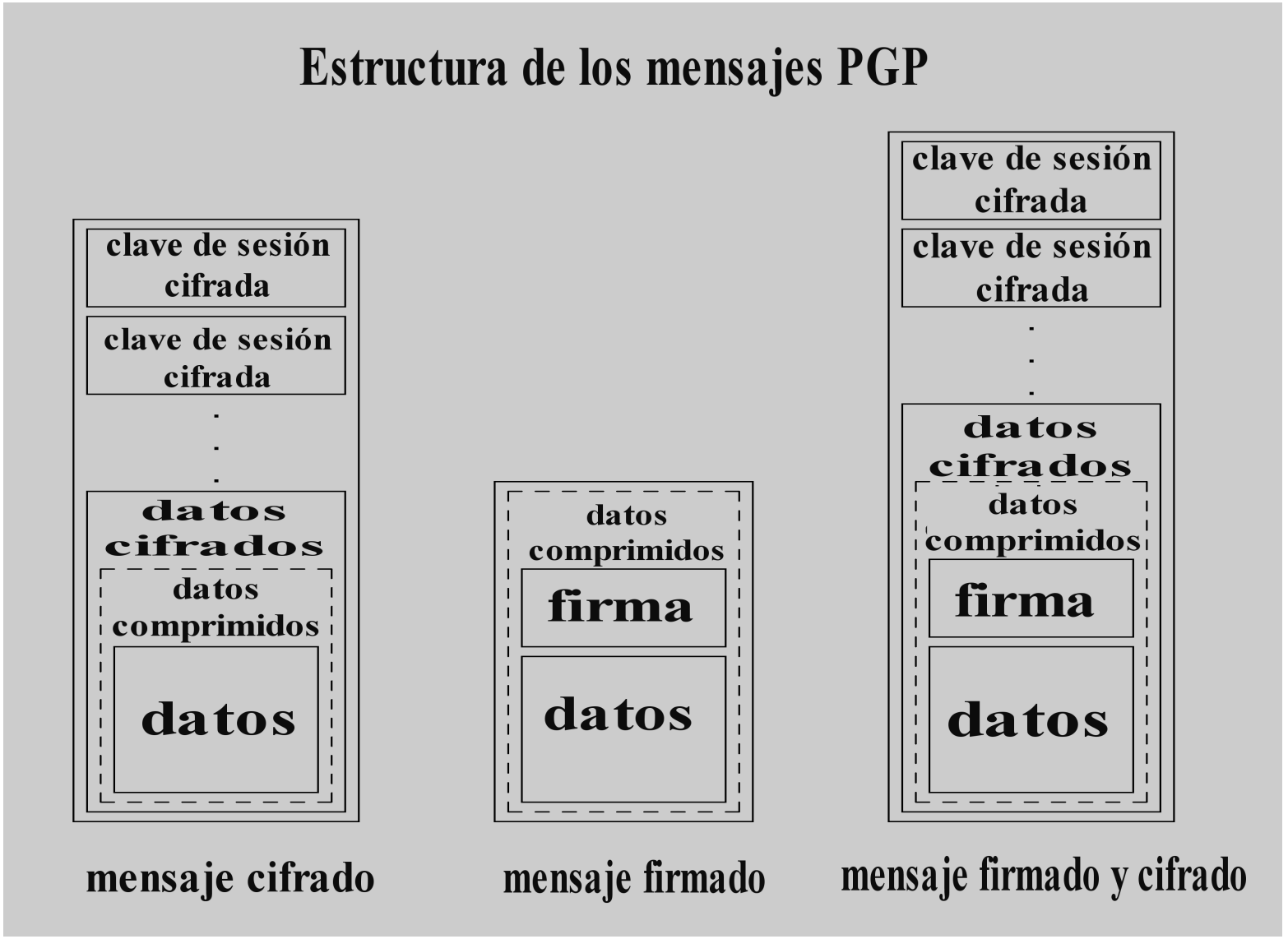
Para descifrar el valor del texto cifrado, nosotros calculamos:

$$\mathrm{decrypt}(855) = 855^{2753} \pmod{3233} = 123$$

PGP-Pretty Good Privacy

El actor más notable en la defensa del cifrado fuerte para uso público fue **Phil Zimmermann** con la **publicación de PGP** (Pretty Good Privacy) en **1991**. Distribuyó una versión freeware de PGP cuando previó la amenaza de una legislación, por aquel entonces en consideración por el gobierno estadounidense, que requeriría la creación de puertas traseras en todas las soluciones criptográficas desarrolladas dentro de EE. UU. Sus esfuerzos para publicar PGP en todo el mundo le granjearon una larga batalla con el Departamento de Justicia por la supuesta violación de las restricciones de exportación. Finalmente, el Departamento de Justicia abandonó el caso contra Zimmermann,4 y la distribución freeware de PGP se hizo mundial y terminó convirtiéndose en un estándar abierto (RFC2440 u OpenPGP).

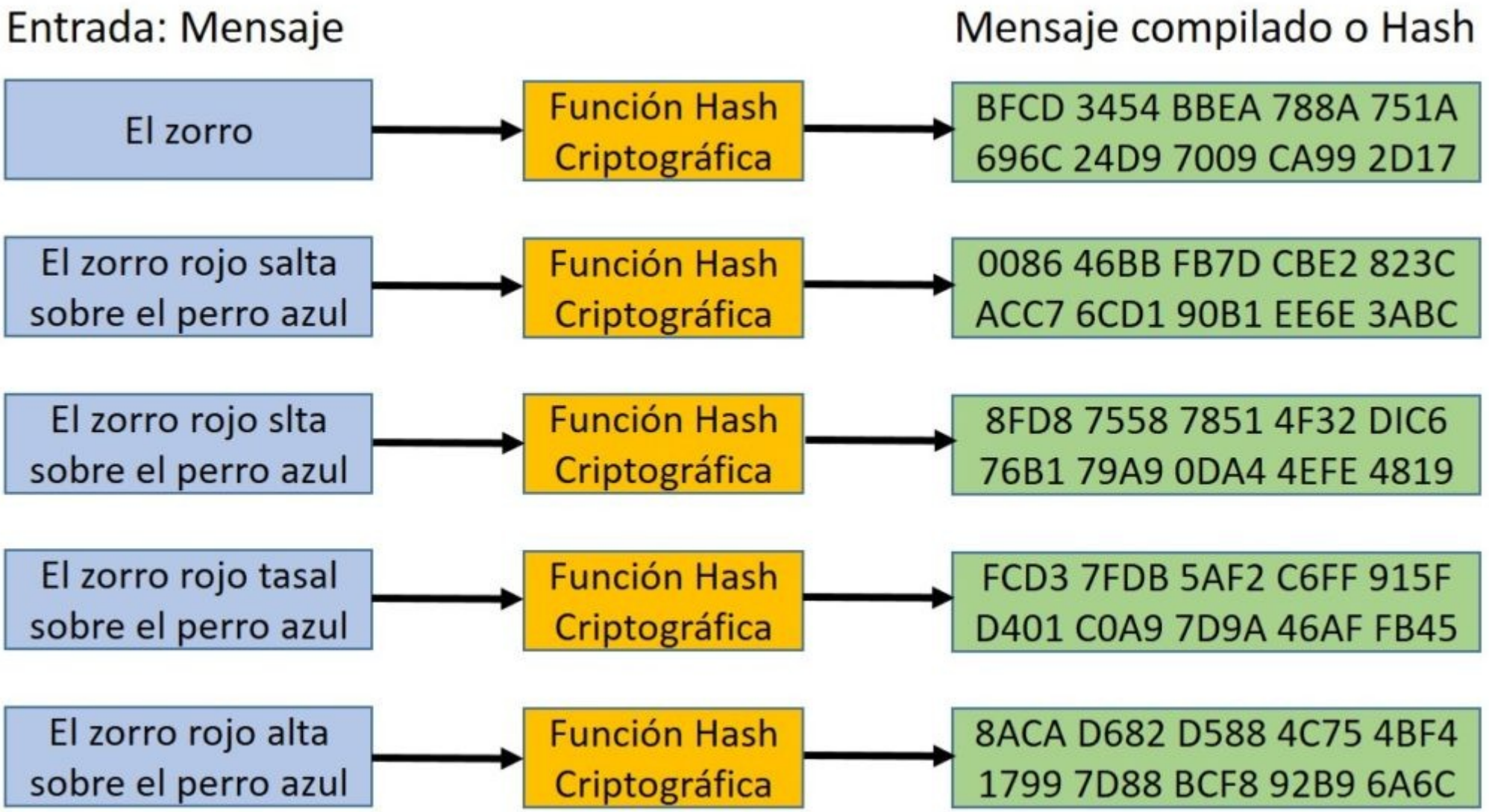
PGP-Pretty Good Privacy



Función hash

Los hash o funciones de resumen son algoritmos que consiguen crear a partir de una entrada (ya sea un texto, una contraseña o un archivo, por ejemplo) una salida alfanumérica de longitud normalmente fija que representa un resumen de toda la información que se le ha dado (es decir, a partir de los datos de la entrada crea una cadena que solo puede volverse a crear con esos mismos datos).

Función hash



Función hash

- Para una clave de 12 dígitos, escrita con un teclado con 97 caracteres (base 97), habría que realizar (esto no tiene nada que ver con los algoritmos de HASH):

$$97^{12} = 693.842.360.995.438.000.295.041 \text{ comprobaciones.}$$

- Para MD5, la salida es de 128 bits, sería necesario realizar:

$$2^{128}=3'402823669 * 10^{38} \text{ operaciones.}$$

Trabajemos ahora con los ataques basados en búsqueda de colisiones:

- Para MD5, la salida es de 128 bits, luego hay que operar sobre la mitad de bits, y sería necesario realizar:

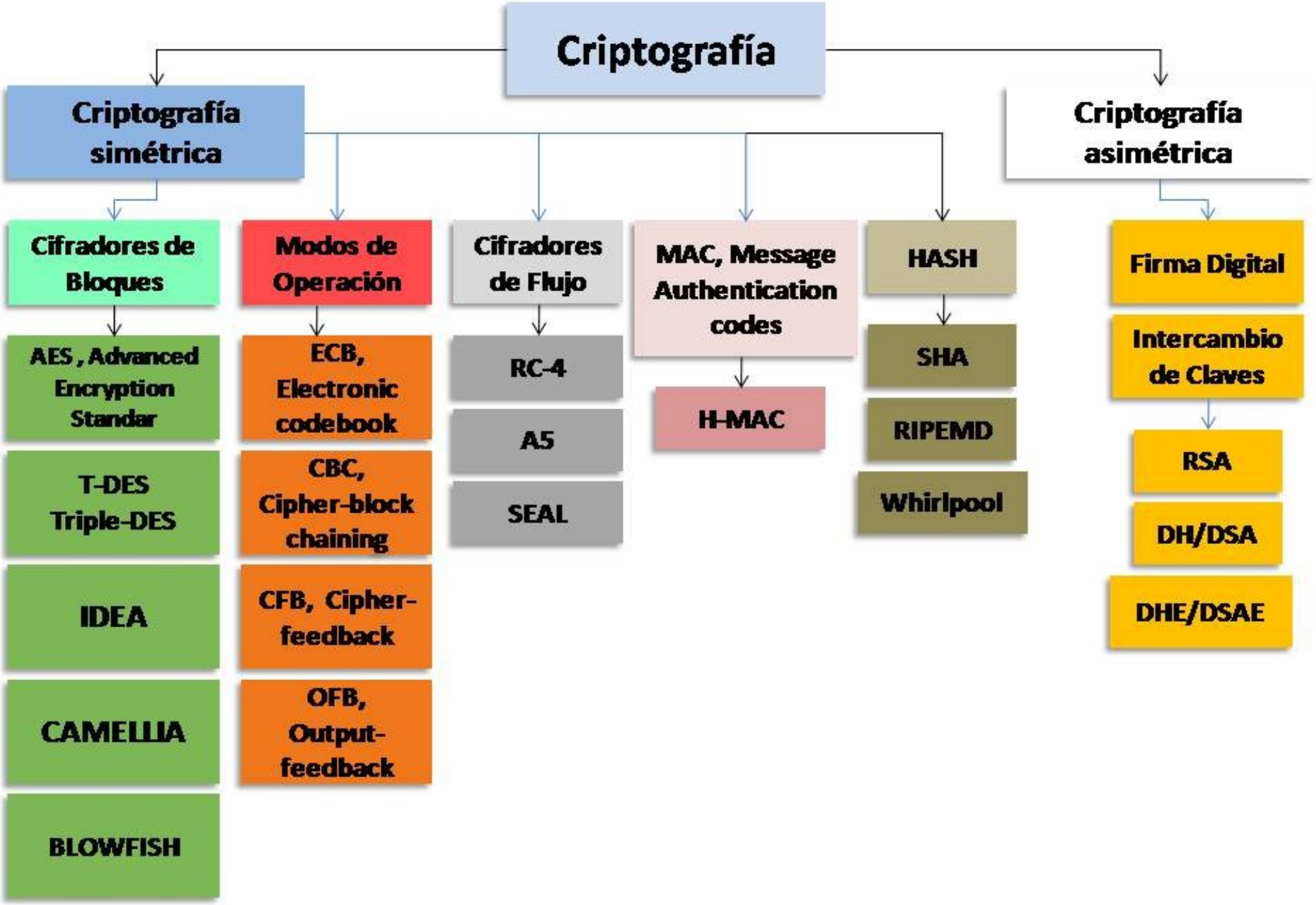
$$2^{64}=18.446.744.073.709.551.616 \text{ operaciones.}$$

- Para el algoritmo SHA 1, cuya salida es de 160 bits:

$$2^{80}=1.208.925.819.614.629.174.706.176 \text{ operaciones.}$$

  Curiosidad: 1.000.000 de ordenadores capaces de procesar en 1 µs cada operación tardarían más de 38.000 años en las 2^{80} operaciones.

Y para los más desconfiados e incluso paranoicos: ¿qué hay de las supercomputadoras y de la gente que sí dispone de los medios necesarios? Cuando saltaron las primeras alarmas sobre estos algoritmos, hace unos dos años, las cifras eran las siguientes:


Criptografía
Criptografía simétrica
Criptografía asimétrica
Cifradores de Bloques
Modos de Operación
Cifradores de Flujo
MAC, Message Authentication codes
HASH
Firma Digital
AES , Advanced Encryption Standar
T-DES Triple-DES
IDEA
CAMELLIA
BLOWFISH
ECB, Electronic codebook
CBC, Cipher-block chaining
CFB, Cipher-feedback
OFB, Output-feedback
RC-4
A5
SEAL
H-MAC
SHA
RIPEMD
Whirlpool
Intercambio de Claves
RSA
DH/DSA
DHE/DSAE

Taller Práctico

- Nivelacion Python
- Python y Criptografía
- Mi primer Ransomware con Python
- Mi primer Ransomware Web con PHP
- Infectando Maquinas automáticamente

Conclusiones


Fin del Taller
Gracias!