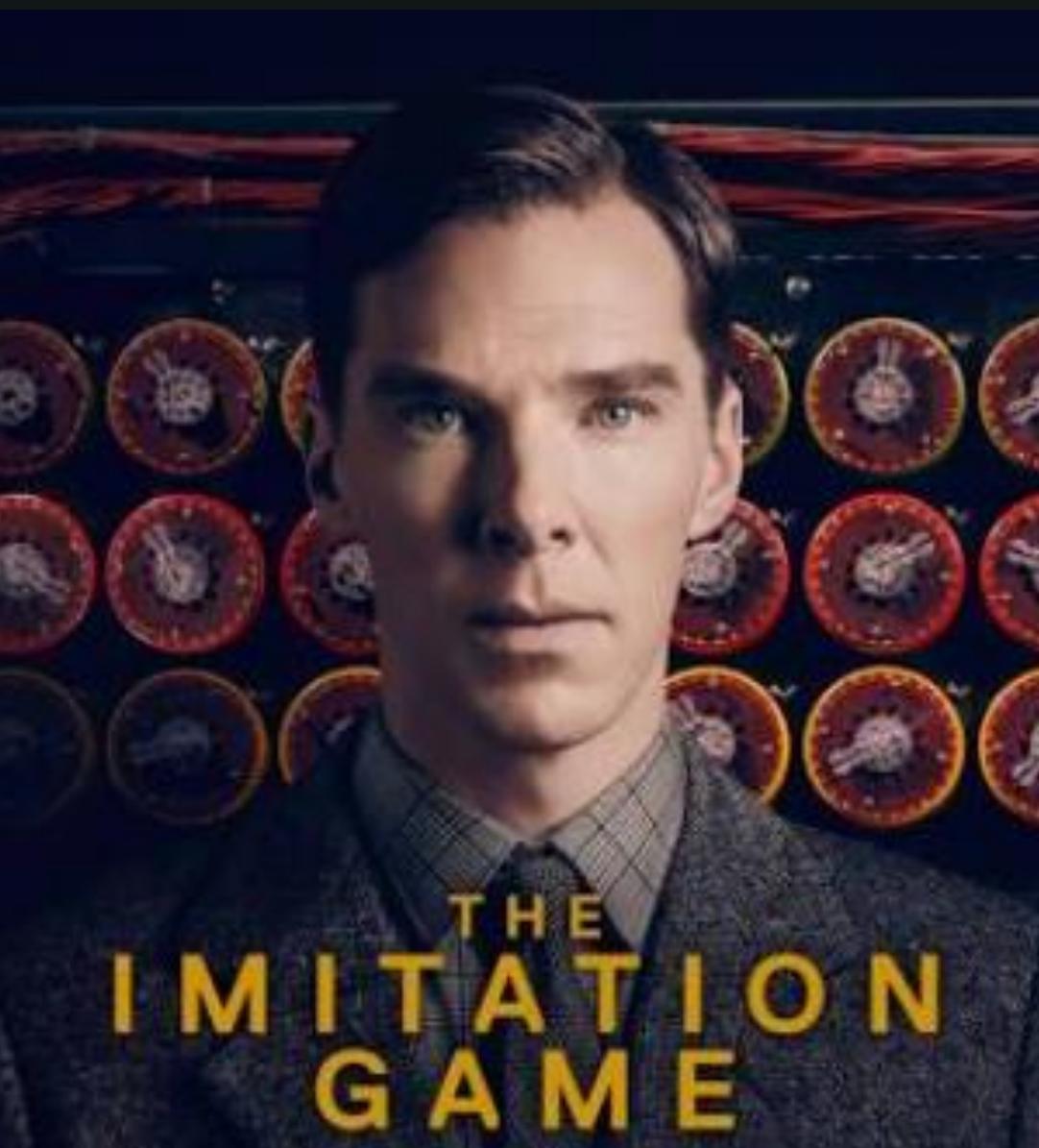




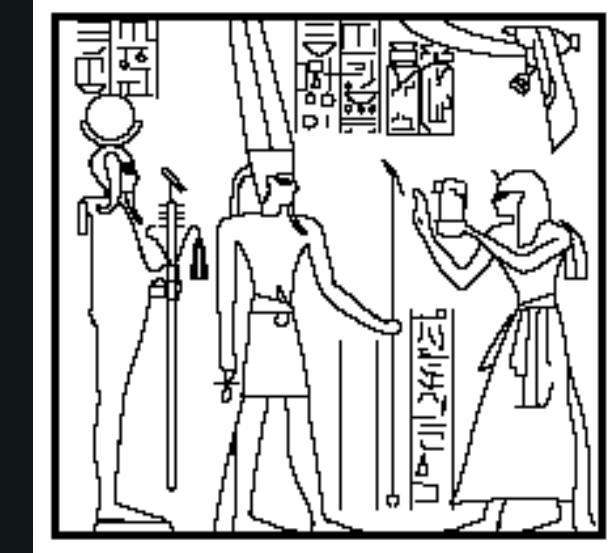
Bienvenidos a

Ciberseguridad

Criptografía



Criptología



- Del griego *krypto*: 'oculto' y *logos*: 'estudio'.
- Disciplina o ciencia que estudia la manera de cifrar y descifrar los mensajes con una o más llaves para que resulte imposible conocer su contenido a los que no dispongan de las claves utilizadas.
 - Su uso más antiguo se puede encontrar en algunos jeroglíficos de hace 4500 años en Egipto.
- La criptología se divide en:
 - **Criptografía** (escritura oculta): Arte de escribir en forma secreta o de modo enigmático.
 - **Criptoanálisis** (análisis de lo oculto): Arte de descifrar criptogramas.
 - **Esteganografía** (escritura cubierta, oculta o protegida): Arte de ocultar mensajes u objetos, dentro de otros.
 - **Estegoanálisis** (análisis de lo cubierto): Estudio de la detección de mensajes ocultos usando esteganografía.

Elementos

Cifrado

- Algoritmo.

Texto Plano/Claro

- Documento original (M).

Criptograma

- Documento/texto cifrado (C).

Claves

- Llaves (criptovariables) que permiten cifrar/descifrar un criptograma.

Espacio de llaves

- Conjunto de todas las llaves posibles.

Alfabeto

- Conjunto de todos los caracteres posibles.

Criptosistema

- Conjunto completo de elementos que conforman un sistema criptográfico.

Propósito

- Proteger información de forma tal que **solo quien está autorizado** pueda leerla y comprenderla.
- En la antigüedad se pretendía garantizar la confidencialidad, la integridad y la autenticidad. A finales del siglo XX se han añadido la disponibilidad y, últimamente el no repudio.



Clasificación



Criptografía Clásica

- La seguridad se basa en el **secreto del algoritmo**:
 - Cifrado por transposición.
 - Cifrado por sustitución.

Criptografía
Moderna

- La seguridad se basa en el **secreto de la clave**.

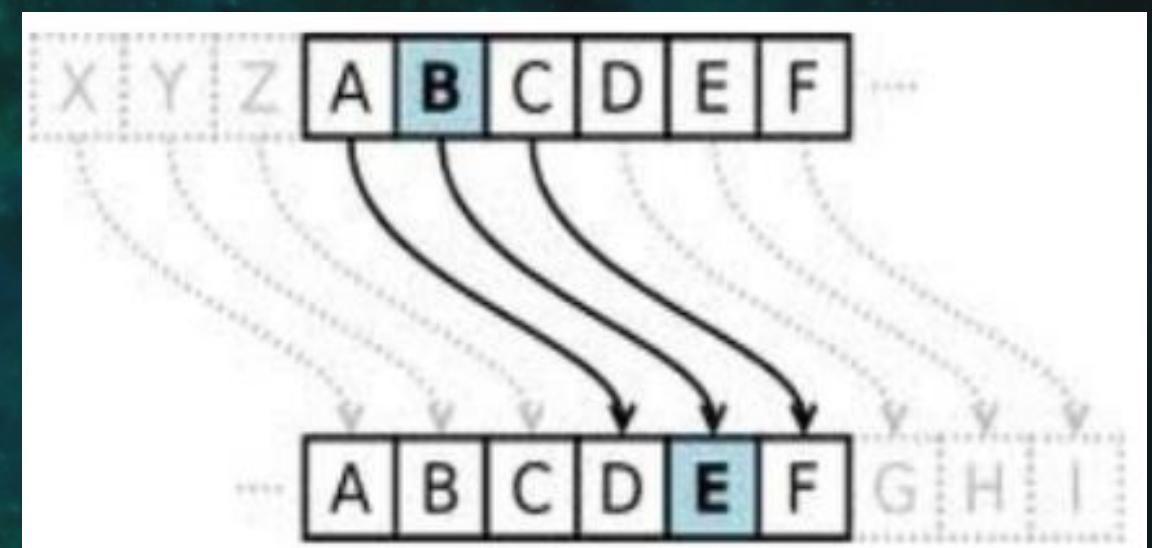
Criptografía Clásica - Transposición

- También conocido como permutación.
- Los caracteres se cambian de posición según ciertas reglas. El criptograma tendrá los mismos caracteres del mensaje, pero con una distribución diferente.
- Su criptoanálisis se realiza aplicando técnicas de Anagramación.
- Algunos ejemplos:
 - Escritura inversa (Hola = aloh).
 - Transposición de Columna/Fila.
 - Rejilla.
 - Grupos.
 - Escítala.



Criptografía Clásica - Sustitución

- También conocido como confusión.
- El criptograma tendrá caracteres distintos a los que tenía el mensaje.
- Se sustituyen caracteres por otros del mismo u otros alfabetos.
- Se puede esconder la distribución característica del lenguaje en el criptograma.



Criptografía Clásica - Sustitución

- Tipos:
 - **Sustitución Simple:** un carácter del mensaje se remplaza por un carácter del alfabeto del criptograma (alfabeto de sustitución).
 - **Monoalfabéticos:** Un carácter del mensaje se remplaza por un carácter del alfabeto de sustitución.
 - Ejemplos: Atbash, Cesar, ROT13, afín, francmasón.
 - **Polialfabéticos:** Un carácter no siempre se sustituye por el mismo carácter. Se utilizan varios alfabetos.
 - Ejemplos: Alberti, Vigenère, Vernam.
 - **Homófonos:** Los caracteres más comunes del mensaje se pueden representar con más de un carácter del alfabeto de sustitución.
 - Ejemplo: Código navajo.
 - **Poligráfico o por bloques:** Se sustituyen grupos de caracteres del mensaje por otros.
 - Ejemplos: Playfair, Hill.

Criptografía Clásica - Ejemplos

Escitala
400 A.C.

Polybios
Siglo II A.C.

Cesar
Siglo I A.C.

Alberti
1467

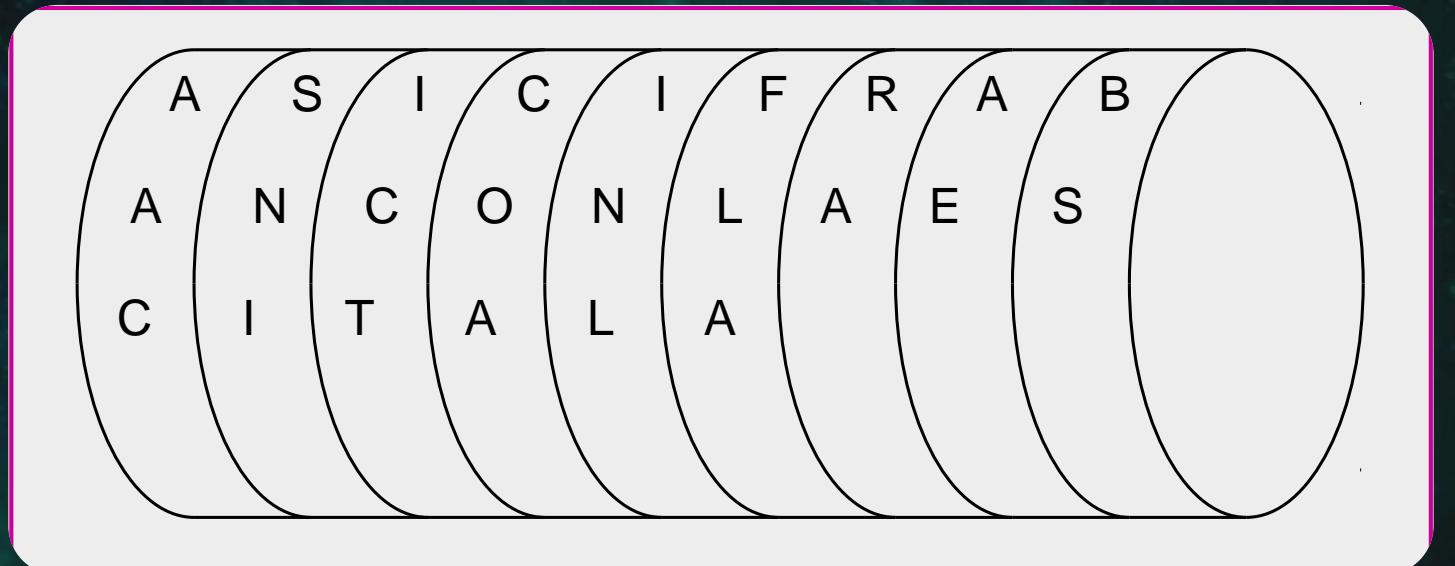
Vigenére
1586

Enigma
1923

Hill
1929

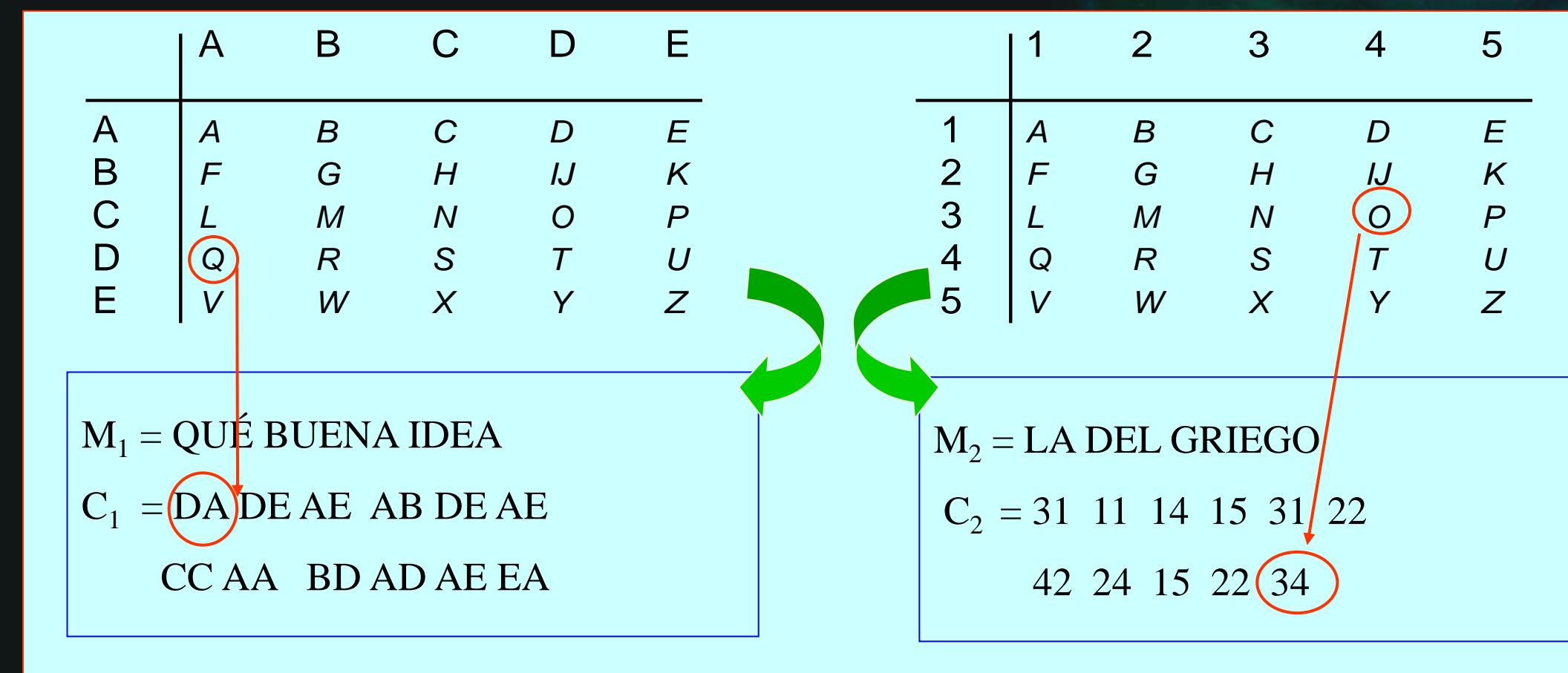
Criptografía Clásica - Escitala (400 A.C.)

- Fue el primer cifrador por transposición.
- Bastón en el que se enrollaba una cinta de cuero y luego se escribía en ella el mensaje de forma longitudinal.
 - Al desenrollar la cinta, las letras aparecerán desordenadas.
- Para descifrar el criptograma y recuperar el mensaje en claro hay que enrollar la cinta en un bastón con el mismo diámetro.
- Ejemplo
 - El texto en claro es:
 - M = ASI CIFRABAN CON LA ESCITALA
- El texto cifrado o criptograma será:
 - C = AAC SNI ICT COA INL FLA RA AE BS



Criptografía Clásica - Polybios (Siglo II A.C.)

- Cifrador por sustitución.
- Duplica el tamaño del texto plano, por lo que no es tan eficiente.



Criptografía Clásica - César (Siglo I A.C.)

- Usado por Julio César.
- El algoritmo consiste en el desplazamiento de tres espacios hacia la derecha de los caracteres del texto plano.
- Es un cifrador por sustitución monoalfabético en el que las operaciones se realizan módulo n, siendo n el número de elementos del alfabeto (en ese entonces el latín).
- Alfabeto de cifrado del César para castellano (mod 27):

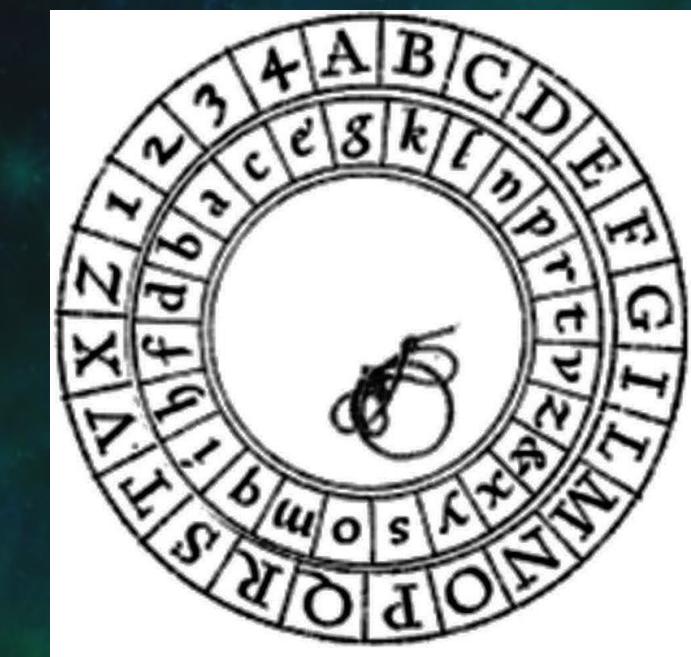
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	
M _i	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
C _i	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	

- Para aumentar la seguridad podemos incluir en el alfabeto de cifrado una clave:
 - La clave K es una palabra o frase que se escribe a partir de una posición p₀ del alfabeto en plano.
 - Los caracteres repetidos de la clave no se escriben.
 - Una vez escrita en la posición indicada se añaden las demás letras en orden

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

Criptografía Clásica - Alberti (1467)

- Alberti es polialfabético por sustitución y describe un disco cifrador con el que es posible cifrar textos sin que exista una correspondencia única entre el alfabeto del mensaje y el de cifrado.
- Con este sistema, cada letra del texto en claro podía ser cifrada con un carácter distinto dependiendo esto de una clave secreta.



Criptografía Clásica - Vigenère (1586)

- Cifrador polialfabético que soluciona la debilidad del cifrado del César, en el cual una letra se cifra siempre igual.
- Se usa una clave K de longitud L y se cifra carácter a carácter sumando “módulo n” al texto en claro con los elementos de esta clave: $C_i = M_i + K_i \text{ mod } 27$
- Sea la llave K = CLAVE y el mensaje M = “HOLA AMIGOS”

M = H O L A A M I G O S
K = C L A V E C L A V E
C = J Z L V E Ñ S G K W

- Para codificar y decodificar se utiliza la tabla Vigenère:

Criptografía Clásica - Vigenère - Tabla

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

M = HOLAAMIGOS
K = CLAVECLAVE
C = JZLVEÑSGKW

Criptografía Clásica - Vigenère - Criptoanálisis

- Método de Kasiski (1863)
- Consiste en buscar repeticiones de “cadenas de caracteres” en el criptograma. Si estas cadenas son mayores o iguales a tres caracteres y se repiten más de una vez, es probable que se deba a cadenas de texto plano que se han cifrado con una misma porción de la clave.
- Si se detectan estas cadenas, la distancia entre las mismas será múltiplo de la longitud de la clave.
- Luego, el máximo común divisor entre esas cadenas es un candidato a ser la longitud de la clave (L).

APRENDIMOS	A	UTILIZAR	LA	PRENSA
CLAVECLAVE	C	LAVECLAV	EC	LAVECL
CARZRFTMJW	C	FTDPKKAM	PC	ARZRUL

Criptografía Clásica - Vigenère - Criptoanálisis

- Índice de Coincidencia (IC) (1920)

ZZEDB	QPIRD	MCIYS	ÑKEKO	ÑWOXS	ICQKD	OMIVZ	VKSAG	DMQCS	YMOOD
GNSHV	VKMJD	XOIVI	VGGDO	OZSMW	VAUDS	IWGXU	DIYVE	ZHIVZ	KATAW
HMVXH	XCEAS	IBEMW	VALJP	DIXNB	DLSLD	IAMOD	VCQUJ	XOELV	KXIAD
YMWYJ	ZAHNQ	PIVNB	OIHQO	ÑAMVV	VJIAE	ZAGJR	KSSBE	VLVNH	YMOUJ
XOELV	KSIPO	WPEVR	DKLXF	PMITK	DMNIXS	ÑBEKO	YMJQB	DBMEO	TZIUE
OIHJA	ZUXNH	VSEXZ	KKYJZ	ZZETO	LMSAT	KZPJR	ZSEUO	GIWDS	NBIHE
KZSAR	ZUHNH	PATJR	NMWNZ	HCGPO	XOSPO	WPEBO	GPHXS	IWXAD	WWXNF
PMGXU	DWXAS	ÑJYNB	KATNQ	ZAOJE	NPPNG	VAIUE	IIIIVI	NPWCS	XPEJZ
HCGPO	XOSES	NIOEW	ZQSAS	BZIBO	NBSMD	ÑSSBR	DIWLD	IAYKD	OMZJQ
DWCBW	ZTTAS	WINJP	VIEHJ	YIVTS	VKEAU	VZOXH	NWOTD	ÑLIBS	YIOXS
GJMLV	ZZSHS	GIVYD	IGOJK	ZSEJG	NWOTO	YIETA	VAXQZ	GIZNZ	VMWCO
WIVNA	ZUHJR	VKS VH	VKSBR	ZOEAW	IICJG	NWOTO	YITJG	ZKMJJ	IIFJB
YMVJS	IXIAA	VUIVI	ZLIAG	KBE					

C1: ZQMÑNIOVDYGVXVOVIDZKHXIVDDIVXKYZPOÑVZKYYXWDPDÑ
YDŁOZVKZLKZGNKZPNHXWGIWPÐNKZNVINXHXNZBNNDIODZWVYV
VNNYGZGIZNYVGWVZVVZINYZIYIVZK

C2: ZPCKWCMKMMMNKOZAWIHAMCBAILACOXMAIIAJASLMOSPKMM
BMBZIUSKZMZSIBZUAMCOPPWWMJAAPAIIPPCOIQZBSIAMWTIIKZ
WLIJZIGSWIAIMIUKKOIWIKIMXULB

C3: EIIEOQISQOSMIGSUGYITVEELXSMQEIWVHVMIGSVOEIELINEJMIHX
EYESPEWISHTWGSEHXXGXYTOPIIWEGSOSISSWYZCTNEVEOOIOMSVOE
OEXZWVHSSECOTMFVIIIE

C4: DRYKXXVACOHJVMDXVVAXAMJNLOULAYNNQVAJBNULPVXTXKQ
EUJNXJTAJUDHANJNPPBXANXANNJNUVCJPEEABMLKJBAJHTAXBXL
HYJJTTQNCNJVB AJTJJJAVA

C5: BDSOSDZGSDVDIOWSUEZWHSWPBDDJVDJQBOVEREHJVORFKSOBO
OAHZZOTROSERHRZOOOSDFUSBQEGOISZOSWSODRDDQWSPJSUHDSS
VSDKGOAZZOARHRWGOGJBSAIG

Criptografía Clásica - Enigma (1923)

- Máquinas con rotores que permiten cifrado polialfabético.
- Inventada por el ingeniero alemán Arthur Scherbius.
- Tomaron un papel principal en la Segunda Guerra Mundial.
 - Esta máquina debe su fama a la amplia utilización durante la Segunda Guerra Mundial, por parte del ejército alemán.
- Enigma (roto por “el Bombe” de Alan Turing).



ENIGMA

Many thousands of these cipher machines were used by German forces. When a letter is pressed on the keyboard, a system of rotors and wires changes it to a different letter which then lights up on the lampboard above.

Criptografía Clásica - Enigma (1923)

- Fialka



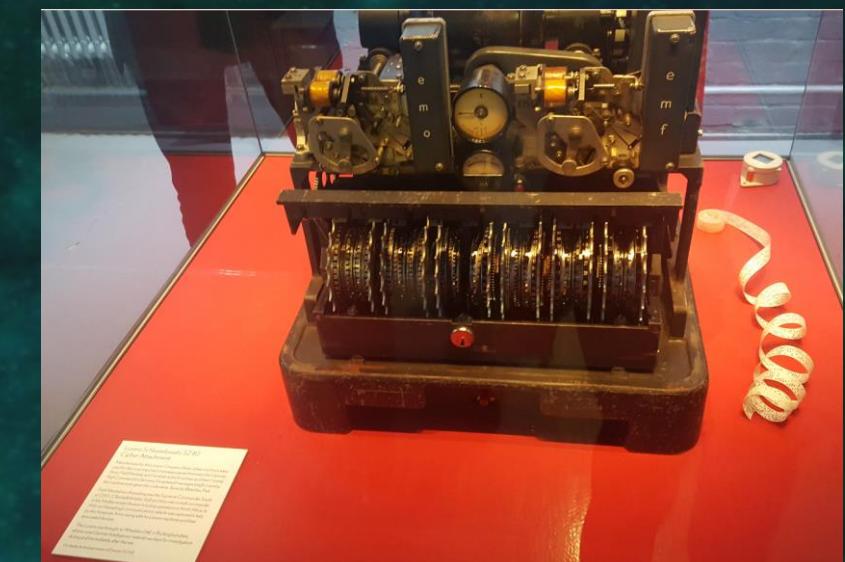
- Purple



- Hagelin



- Lorenz



Criptografía Clásica - Enigma (1923)

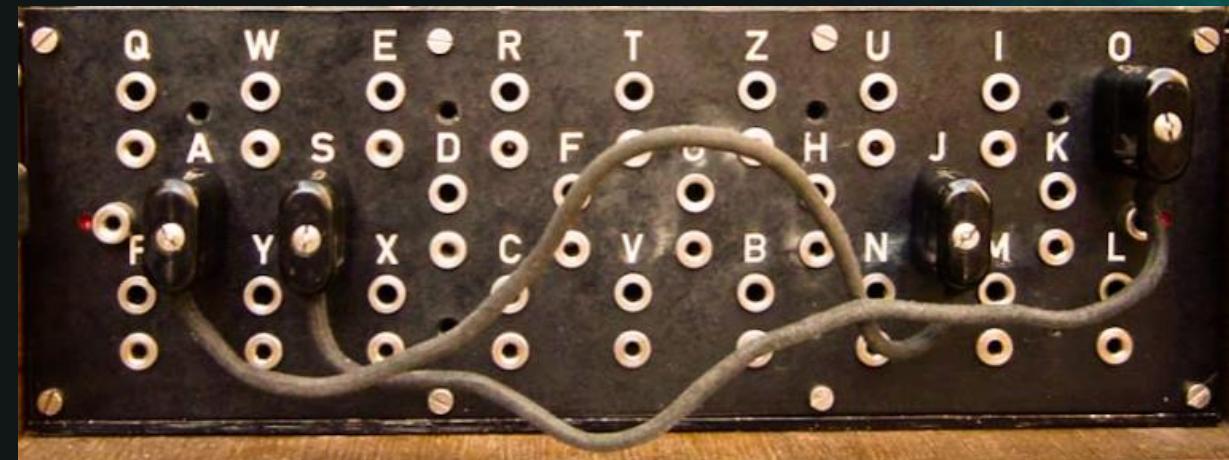
- Consiste en un banco de rotores montados sobre un eje, en cuyos perímetros había 26 contactos eléctricos, uno por cada letra del alfabeto inglés.
- Su cifrado fue roto durante la segunda guerra.
- En 1929, personas de origen polaco interceptaron una máquina Enigma enviada de Berlín a Varsovia y equivocadamente no protegida como equipaje diplomático.
- Un joven matemático polaco, Marian Rejewski, notó un patrón con el que podía suponer el cableado de un rotor, no por las letras, sino por la manera que éstas cambiaban.
- A mediados de 1939 los polacos compartieron su trabajo con franceses y británicos debido a la posible invasión de su país.
- Creditos a: Marian Rejewski, Jerzy Rozycki y Henryk Zygalski.

Criptografía Clásica - Enigma (1923)

Rotores

Plugboard

	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
initial position	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑
	G	E	T	N	D	H	Q	Z	U	P	B	R	C	O	X	M	K	Y	A	W	F	I	L	S	V	J
first turn	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑
	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑
	J	G	E	T	N	D	H	Q	Z	U	P	B	R	C	O	X	M	K	Y	A	W	F	I	L	S	V
second turn	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑
	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑
	V	J	G	E	T	N	D	H	Q	Z	U	P	B	R	C	O	X	M	K	Y	A	W	F	I	L	S
third turn	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑
	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑
	S	V	J	G	E	T	N	D	H	Q	Z	U	P	B	R	C	O	X	M	K	Y	A	W	F	I	L



$$26 \times 26 \times 26 = 17.576$$

$$5 \times 4 \times 3 = 60 \times 17576 = 1.054.560$$

Combinaciones posibles: 150.738.274.937.250

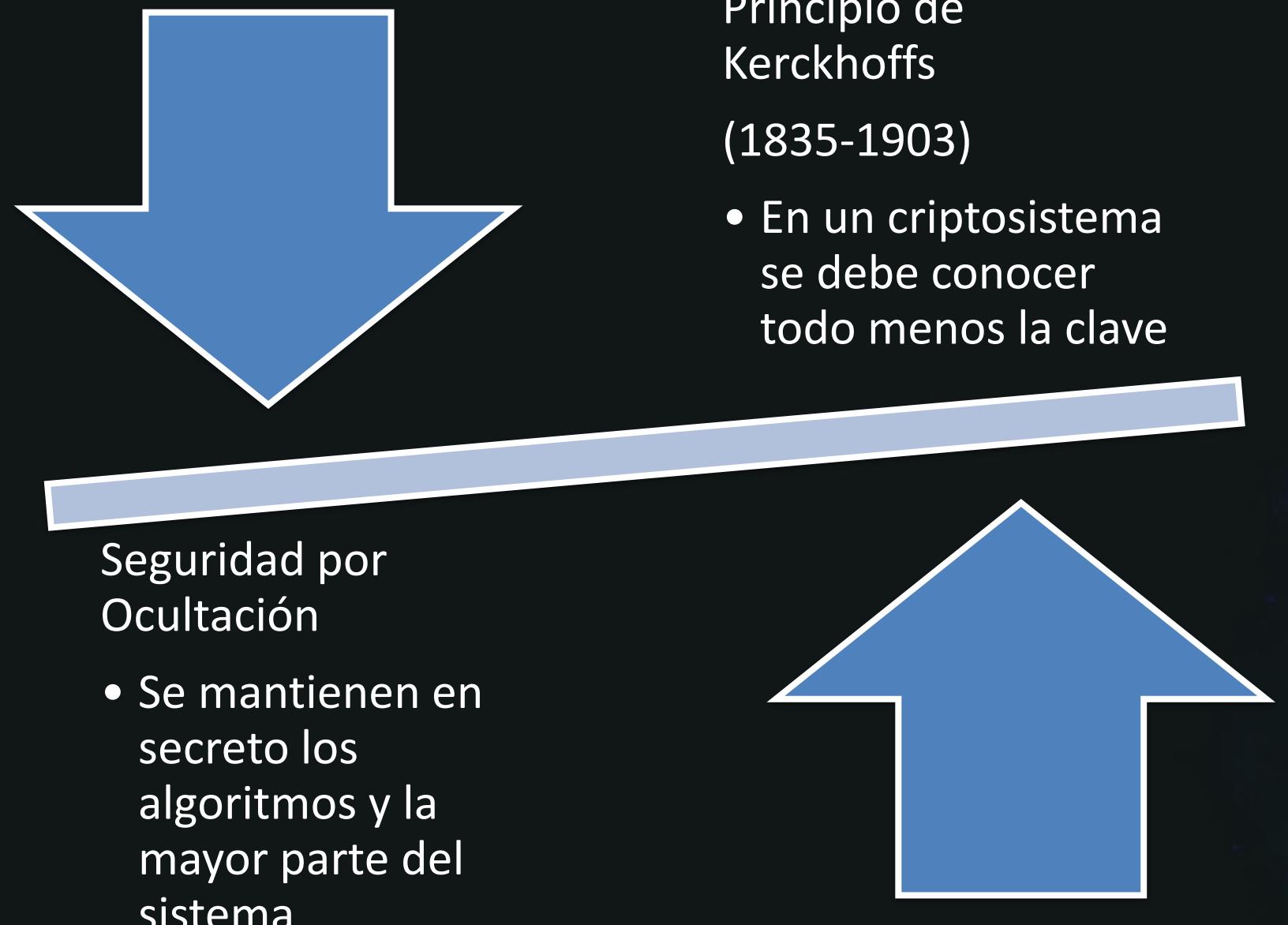
Criptografía Clásica - Hill (1929)

- Sistema de sustitución poligráfica basada en álgebra lineal.
- Usa matriz clave K , matriz columna de mensaje y de criptograma.
 - La matriz clave K debe tener inversa K^{-1} en el cuerpo de cifrado “ n ”
 - Luego: $K^{-1} = T \text{Adj}(K)/|K| \text{ mod } n$
 - $\text{Adj}(K)$ es la matriz adjunta.
 - T es la matriz traspuesta.
 - $|K|$ es el determinante, que no podrá ser cero ni tener factores en común con “ n ” puesto que está en el denominador.
- Es vulnerable a un ataque usando Gauss-Jordan.
- Ejemplo:
 - Mensaje: ACT (0 2 19)
 - Clave: GYBNQKURP (6 24 1 13 16 10 20 17 15)
 - Cifrado: POH (15 14 7)

$$\begin{pmatrix} C_1 \\ C_2 \\ C_3 \\ \vdots \\ C_N \end{pmatrix} = \begin{pmatrix} k_{11} & k_{12} & k_{13} & \dots & k_{1N} \\ k_{21} & k_{22} & k_{23} & \dots & k_{2N} \\ k_{31} & k_{32} & k_{33} & \dots & k_{3N} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ k_{N1} & k_{N2} & k_{N3} & \dots & k_{NN} \end{pmatrix} X \begin{pmatrix} M_1 \\ M_2 \\ M_3 \\ \vdots \\ M_N \end{pmatrix} \text{ mod } n$$

$$\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix} \begin{pmatrix} 0 \\ 2 \\ 19 \end{pmatrix} \equiv \begin{pmatrix} 67 \\ 222 \\ 319 \end{pmatrix}$$
$$\begin{pmatrix} (67)\text{mod}(26) \\ (222)\text{mod}(26) \\ (319)\text{mod}(26) \end{pmatrix} \equiv \begin{pmatrix} 15 \\ 14 \\ 7 \end{pmatrix}$$

Dicotomía Ideológica (clásica vs moderna)



- Requisitos:
 - El algoritmo de cifrado y descifrado deberá ser rápido y fiable.
 - Debe ser posible transmitir información por una línea de datos, almacenarlos o transferirlos.
 - La seguridad del sistema deberá residir solamente en el secreto de una clave y no en las funciones de cifrado.
 - La fortaleza del sistema se entenderá como la imposibilidad computacional de romper el cifrado o encontrar una clave secreta a partir de una pública.

Criptografía Moderna - Pilares

La Teoría de la Información

- Estudio de la cantidad de información contenida en los mensajes y claves, así como su entropía

La Teoría de los Números

- Estudio de las matemáticas discretas y cuerpos finitos que permiten las operaciones de cifrado y descifrado

La Teoría de la Complejidad Algorítmica

- Estudio de la clasificación de los problemas como computacionalmente tratables o intratables

Criptografía Moderna - Teoría de la Información

- Surgió en 1948, estudiado por Claude Shannon en años posteriores a la 2^a Guerra Mundial.
- La teoría de la información mide la cantidad de información que contiene un mensaje a través del número medio de bits necesario para codificar todos los posibles mensajes con un codificador óptimo.
 - Ante varios mensajes posibles, en principio todos equiprobables, aquel que tenga una menor probabilidad de aparición, contendrá mayor cantidad de información.
- La entropía de un mensaje X, que se representa por $H(X)$, es el valor medio ponderado de la cantidad de información de los diversos estados del mensaje. Es una medida de la incertidumbre media acerca de una variable aleatoria y el número de bits de información.
 - La entropía es no negativa y se anula si y sólo si un estado de la variable es igual a 1 y el resto 0.
 - La entropía será máxima (mayor incertidumbre del mensaje) cuando exista una equiprobabilidad en todos los valores de la variable X.

Criptografía Moderna - Teoría de Números

- Matemática Discreta: Rama de matemáticas puras que estudia las propiedades de los números enteros.

Pertenecen a la teoría las cuestiones de:

- Divisibilidad.
- Algoritmo de Euclides para calcular el máximo común divisor.
- Factorización de los enteros como producto de números primos.
- Búsqueda de los números perfectos.
- Congruencias.
- Conjunto completo de restos.

Se investigan propiedades de funciones multiplicativas y otras:

- Función de Moebius.
- Función ϕ de Euler.
- Sucesiones de números enteros.
- Factoriales.
- Números de Fibonacci.

Criptografía Moderna - Teoría de la C.A.

- C.A.= Complejidad Algorítmica.
- Permite conocer la fortaleza de un algoritmo y tener así una idea de su vulnerabilidad computacional.
- Complejidad Computacional
 - Los algoritmos pueden clasificarse según su tiempo de ejecución, en función del tamaño u orden de la entrada.
- Hablamos así de complejidad:
 - Polinomial → comportamiento similar al lineal.
 - Polinomial No Determinista → comportamiento exponencial.
- Esto dará lugar a “problemas fáciles” y “problemas difíciles” cuyo uso será muy interesante en la criptografía.

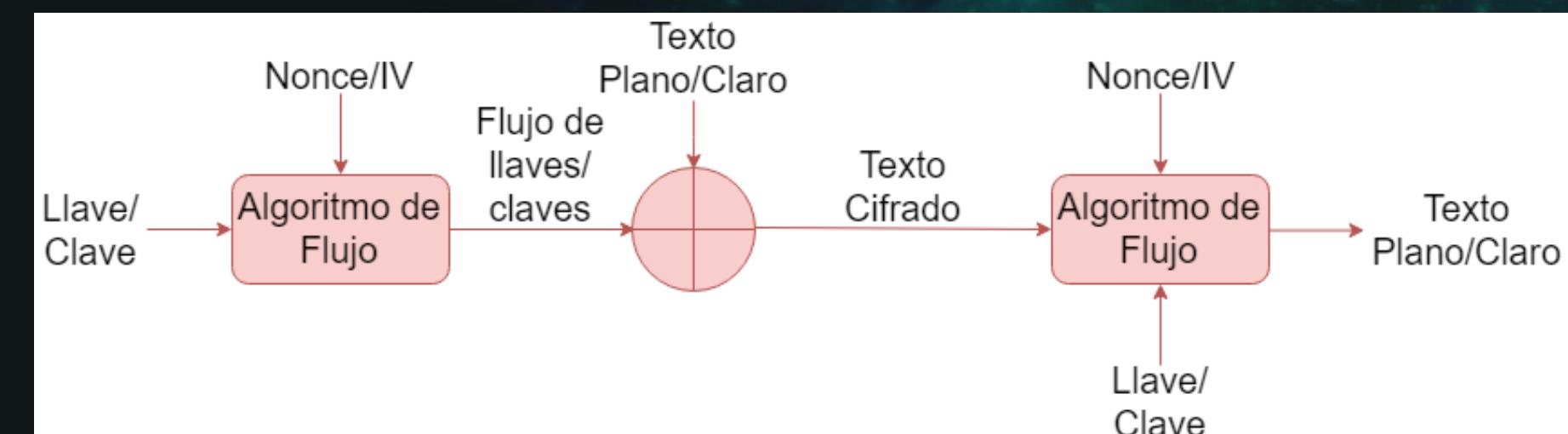
Criptografía Moderna - Clasificación



Criptografía Moderna - Cifrado de Flujo

- Usa el concepto de Vernam, que cumple con las ideas de Shannon sobre secreto perfecto:
 - El espacio de las claves/llaves es igual o mayor que el espacio de los mensajes.
 - Las claves/claves deben ser equiprobables.
 - El flujo de llaves se usa una sola vez y luego se destruye (one-time pad).
- El algoritmo de cifrado se aplica a un elemento de información mediante un generador de claves pseudoaleatorio y de mayor longitud que el mensaje.
- El cifrado se hace bit a bit.

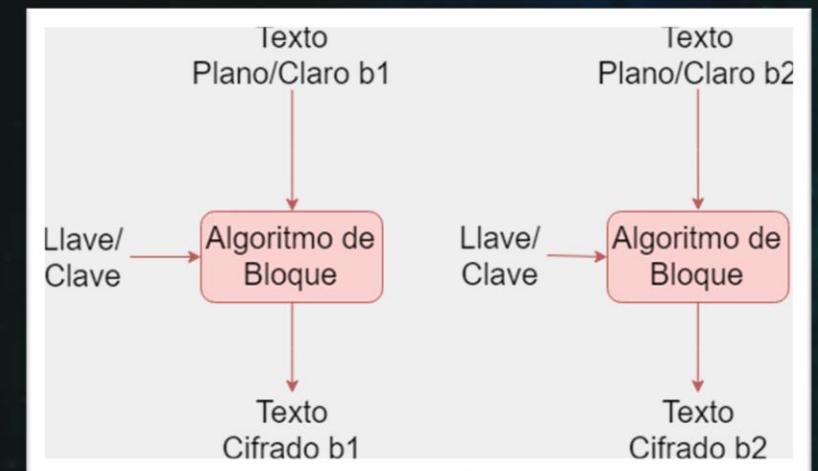
XOR	0	1
0	0	1
1	1	0



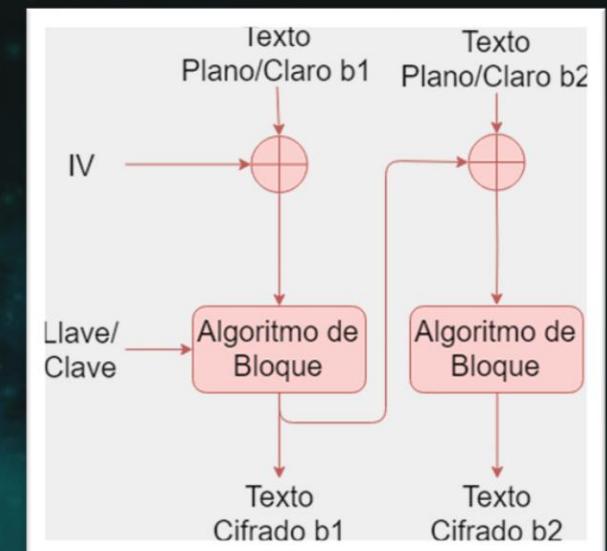
Criptografía Moderna - Cifrado en bloque

- El mensaje claro/plano se agrupa en bloques antes de aplicar un algoritmo a cada uno con la misma clave.
- El tamaño del boque no debe ser muy pequeño (facilita ataques de estadística del lenguaje) ni muy grande (lento, bajo rendimiento).
- Las operaciones sobre los bloques incluyen sustitución y permutación (AES) y redes feistel (DES).
- La forma en la que se cifran/descifran esos bloques, se lo llama “modo de cifrado” y son ECB,CBC,CTR,OFB,CFB.

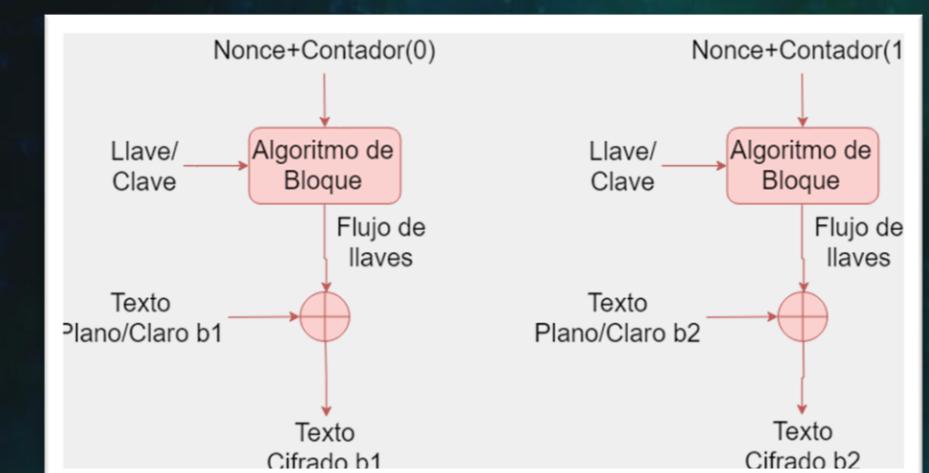
ECB



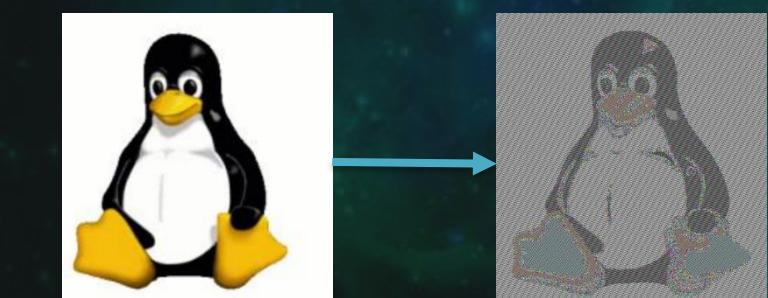
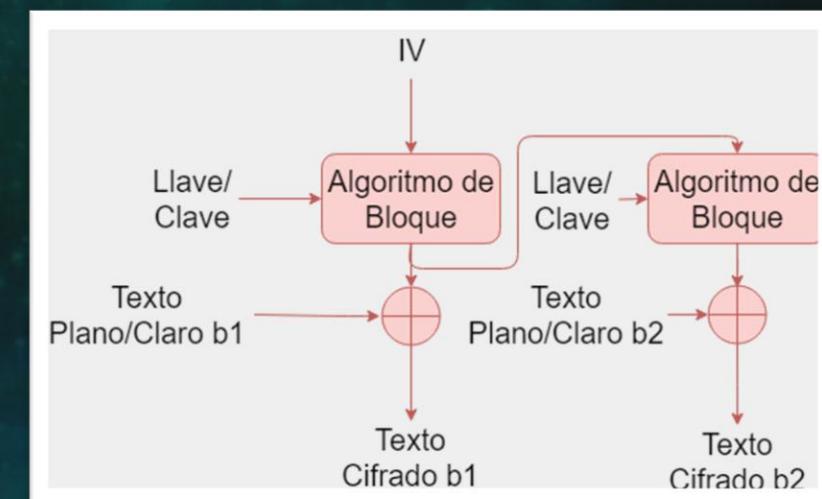
CBC



CTR



OFB



Criptografía Moderna - Sistemas de Llave secreta

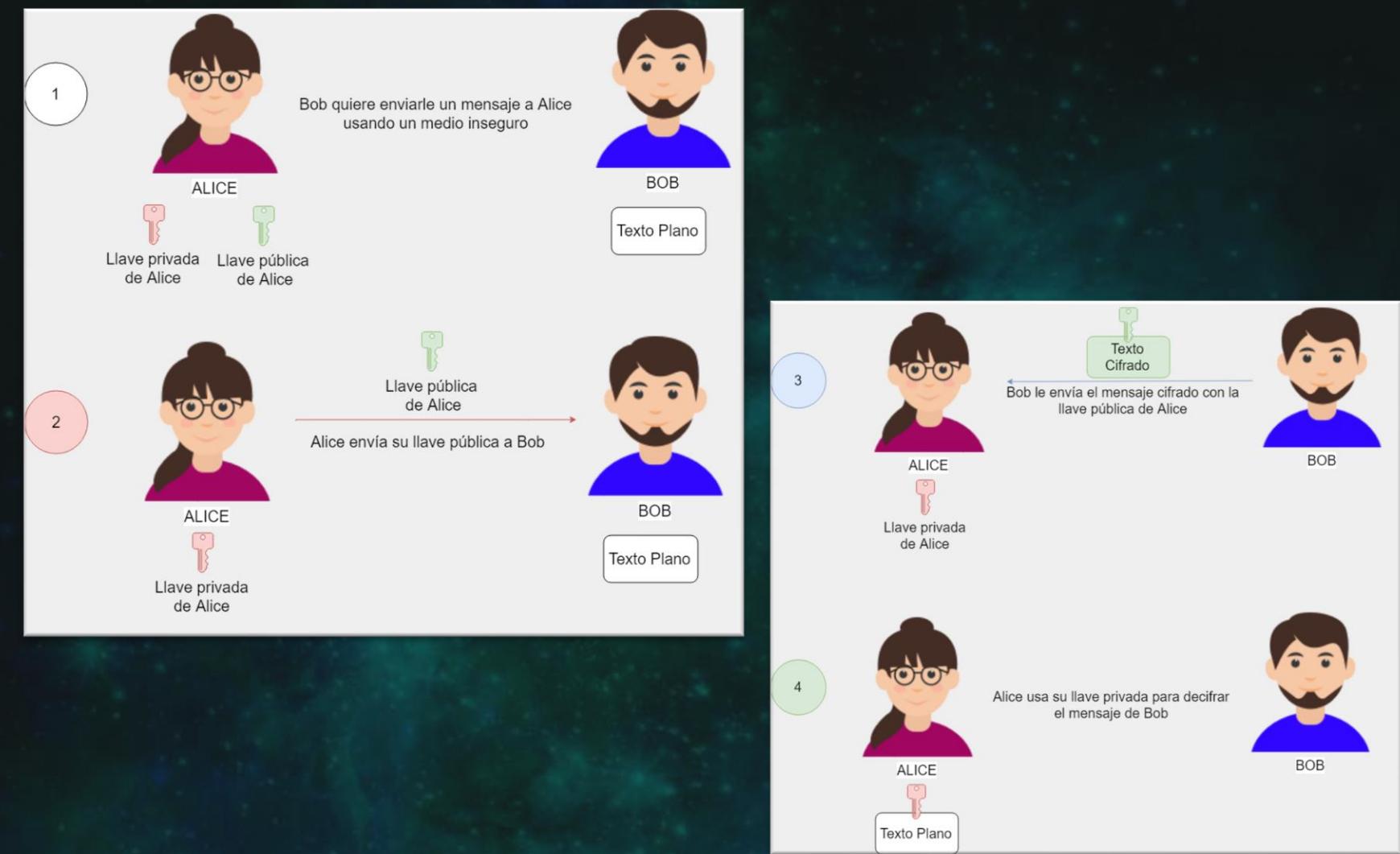
- Llamados criptosistemas simétricos.
- Con la misma clave se cifra y se descifra.
 - No es posible enviar la llave de forma segura a través de un medio inseguro.
- Es veloz.
- Con una llave pequeña, se obtiene alta seguridad.
- Ataque posible: Fuerza bruta.
- Ejemplos:
 - DES, AES/Rijndael, Salsa20, RC5, Blowfish.



Criptografía Moderna - Cifrado en bloque

- Sistemas de Llave pública

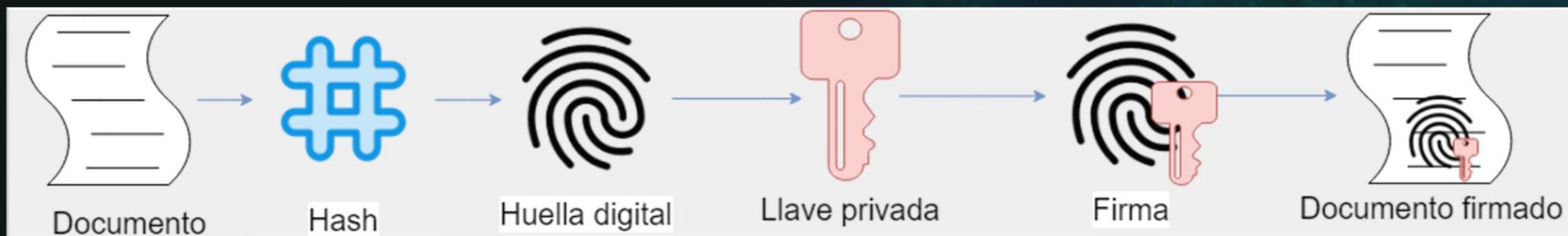
- Llamados criptosistemas asimétricos.
- Cada usuario posee un par de claves, una privada y otra pública. Lo que se cifra con una clave, se descifra con la clave otra.
- Se inventaron para evitar el problema de intercambio de llaves de los sistemas simétricos.
- La seguridad yace en la dificultad de saber la clave privada a partir de la pública.
- Usan las funciones unidireccionales con trampa.
- Usa llaves de tamaño mayor a las simétricas y son más lentos para procesar.
- Ejemplos:
 - Curvas elípticas, Diffie-Hellman, RSA, El Gamal.



Criptografía Moderna - Usos

Firma digital

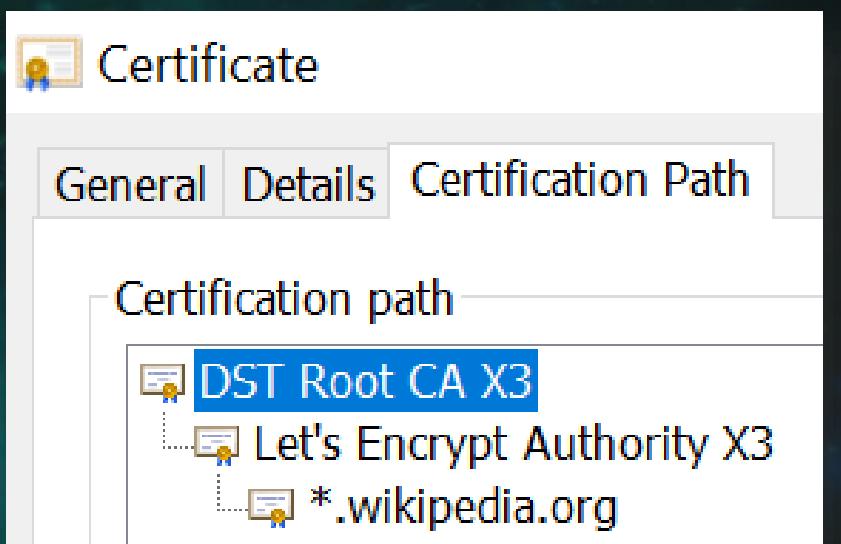
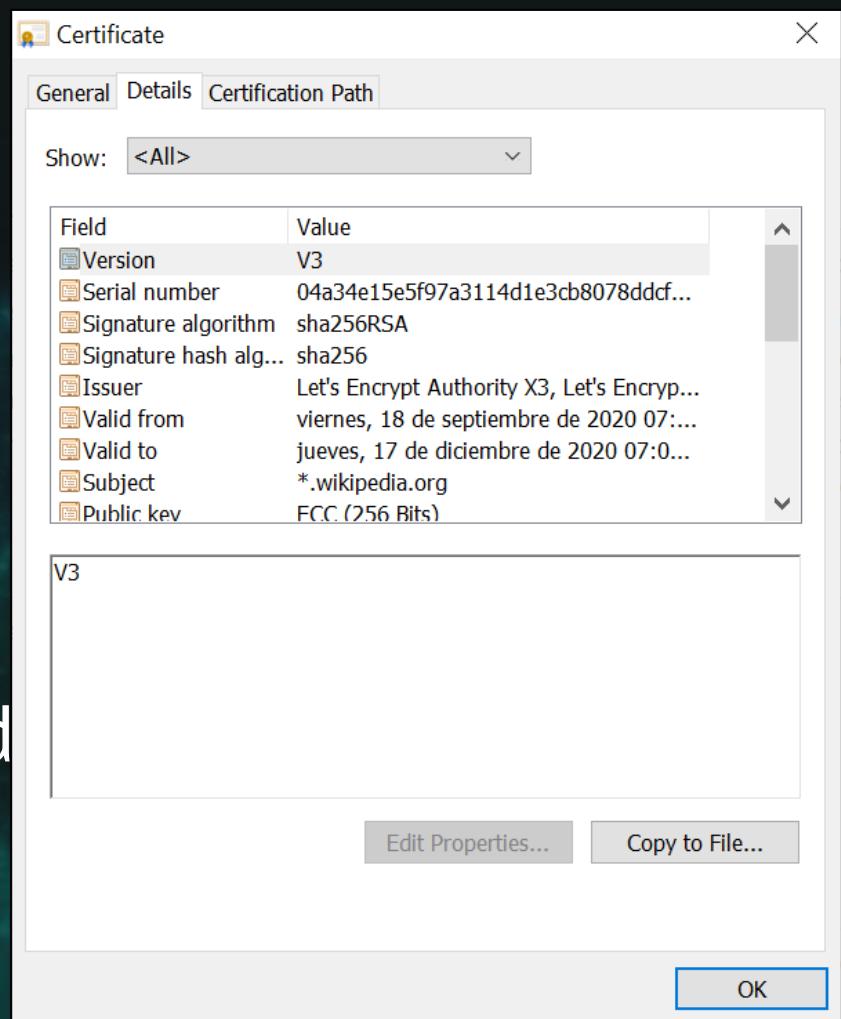
- El emisor envía un mensaje firmado y el receptor puede identificar que el emisor envió ese mensaje y que no fue alterado en el camino.
- Autenticación, Integridad y no repudio.
- Se obtiene un hash del documento y se aplica una clave privada al resultado, obteniendo la firma. Se transmite luego el documento y la firma juntos.
- El receptor recibe el documento, aplica el algoritmo de hash correspondiente y lo compara con el valor firmado. Tienen que coincidir.
- La firma electrónica es un concepto legal y no tiene que ver con esto.
- Algoritmos permitidos: RSA+MD5, DSA+SHA1 y ECDSA+SHA1.



Criptografía Moderna - Usos

Certificado digital

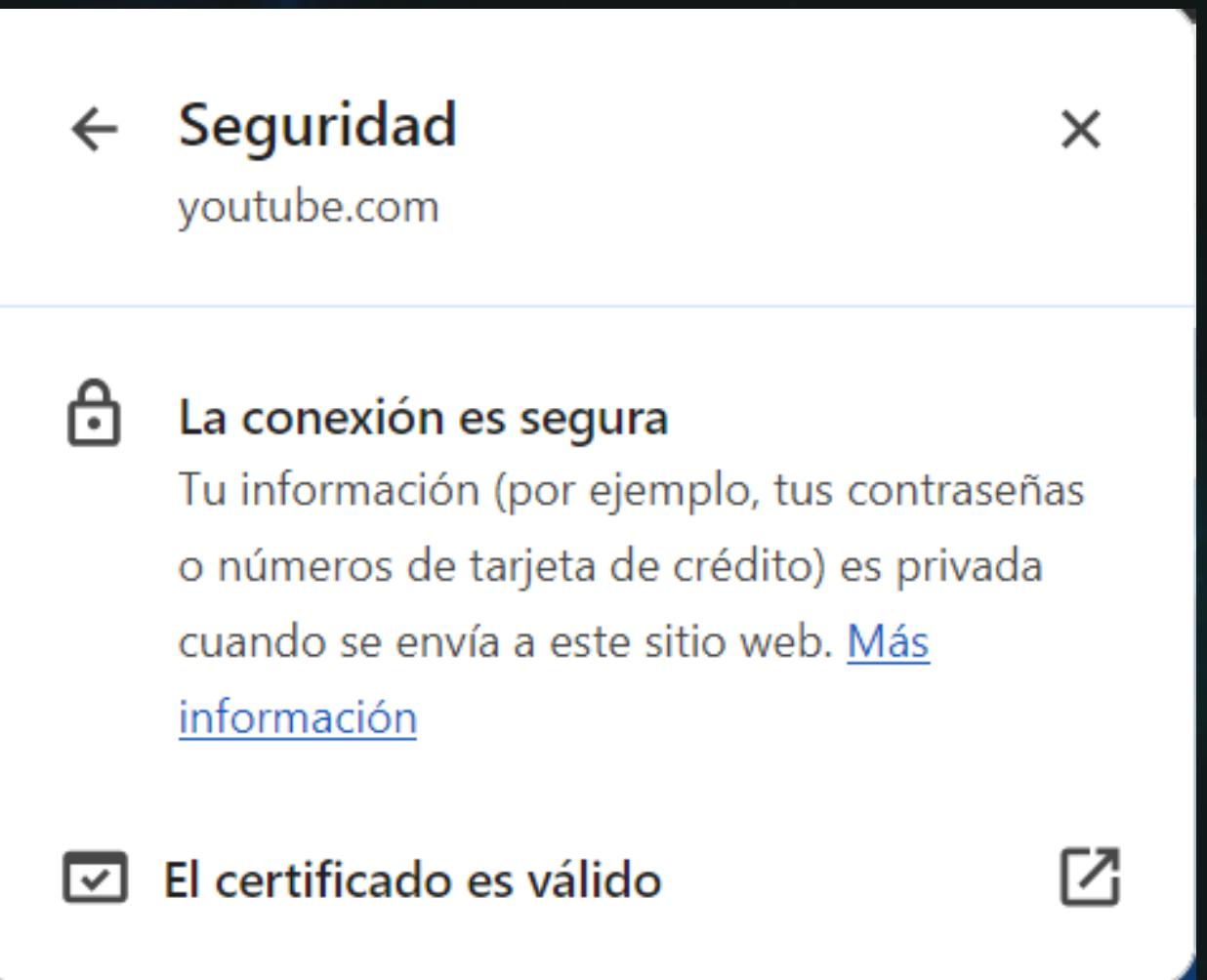
- Fichero electrónico emitido por una autoridad certificante pedido por alguna entidad.
- Los navegadores vienen con certificados raíz preinstalados.
 - Los certificados que dependan del certificado raíz, heredan su fiabilidad
- Contiene los datos del firmante (clave pública, identidad, etc), versión, validez, algoritmo de hash, etc.
- En 2016, los certificados firmados con SHA1, se indicaban en los navegadores como no seguros.
- Formatos: X.509, SPKI, PGP, SAML.
- Ejemplos: Let's Encrypt, Comodo, Verisign.



Criptografía Moderna - Usos

HTTPS

- HTTPS: Hyper Text Transfer Protocol Secure. Emplea cifrado para proteger la transferencia de datos.
- SSL/TLS: Secure Socket Layer/ Transport Layer Security: Protocolos de red que establecen una comunicación cifrada. Actualmente se usa TLS. Este protocolo permite que los browsers se identifiquen y se establezca una conexión cifrada a un sitio que cuente con el protocolo.
- La autoridad certificante brinda un certificado SSL para el sitio web.
- El desarrollador del sitio lo instala y configura en el servidor web para recibir peticiones por el puerto 443.



Criptografía Moderna - Cuántica

- Usa principios de la mecánica cuántica para garantizar **confidencialidad**.
 - Dinámica de partículas cuánticas: fotones, electrones, etc.
 - Si un atacante espía durante la creación de la llave secreta, el proceso se altera (teorema de no clonado).
- Intercambio de llaves cuánticas: QKD (método de comunicación)
- Se usa principalmente para el intercambio de llaves cuánticas.
 - En 2004 se hizo una transferencia bancaria a través de QKD.
- Podría romper la criptografía actual.
- Por supuesto, también existe el criptoanálisis cuántico.
 - Ataque de división del número de fotones.
 - Ataque de MITM (interceptando el mensaje enviado).

La informática cuántica puede romper la seguridad de Internet y hacerlo inservible

• Google podría haber logrado lo que se conoce como supremacía cuántica, un cálculo que sería imposible hacer con un ordenador

OpenSSH goes Post-Quantum, switches to qubit-busting crypto by default

11 APR 2022 25
Cryptography

Criptoanálisis - Tipos de Ataques

Fuerza bruta

- Intentan probar todas las llaves posibles (costo, tiempo).

Analíticos

- Usan algoritmos y manipulación algebraica para reducir la complejidad del ataque.

Estadísticos

- Utilizan debilidades estadísticas del diseño del sistema.

Implementación

- No ataca el algoritmo sino como fue implantado.

Solo texto cifrado

- El atacante intenta desencriptar el texto cifrado directamente.

Texto plano conocido

- El atacante intenta desencriptar el texto cifrado conociendo parte del texto plano.

Texto plano elegido

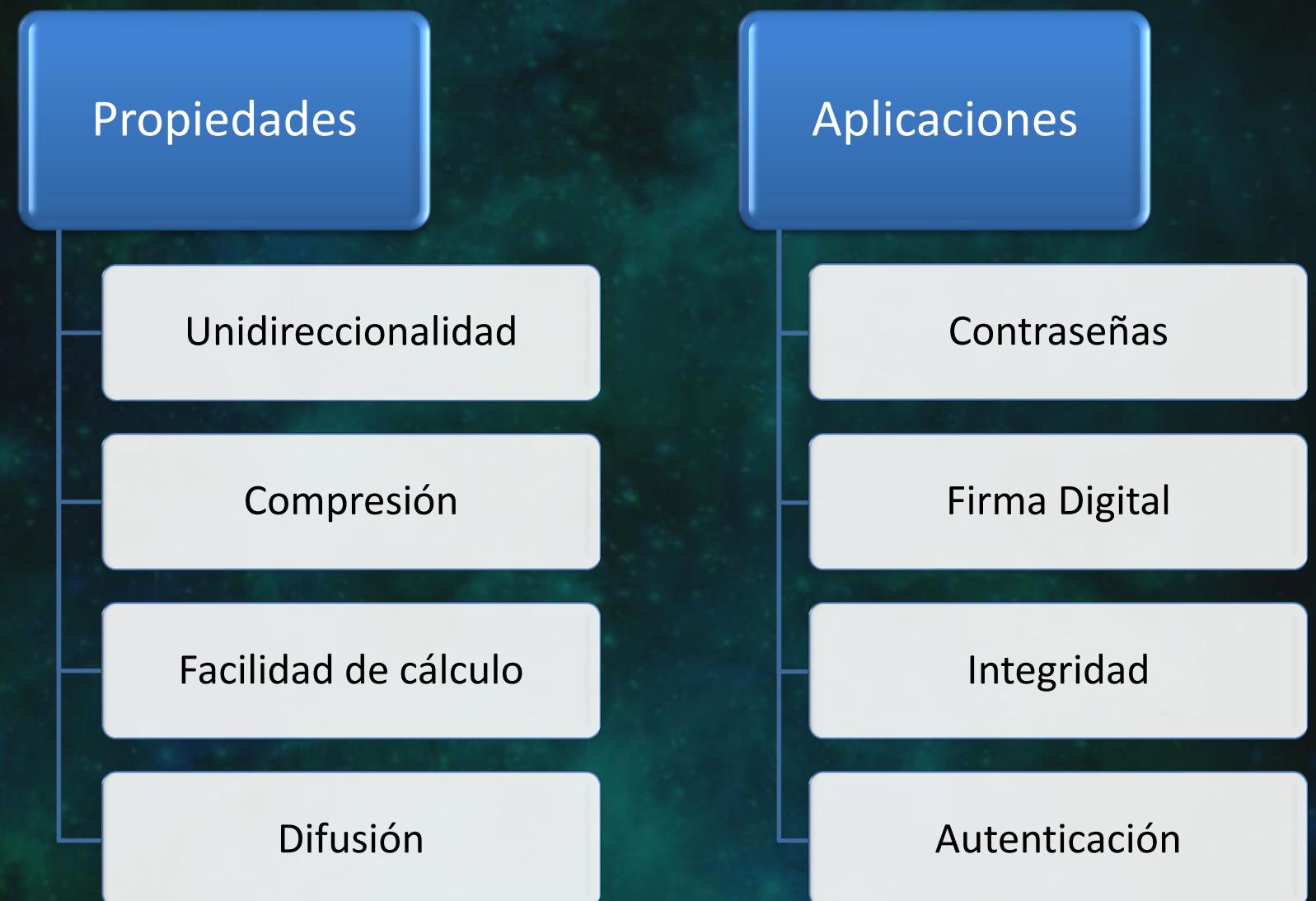
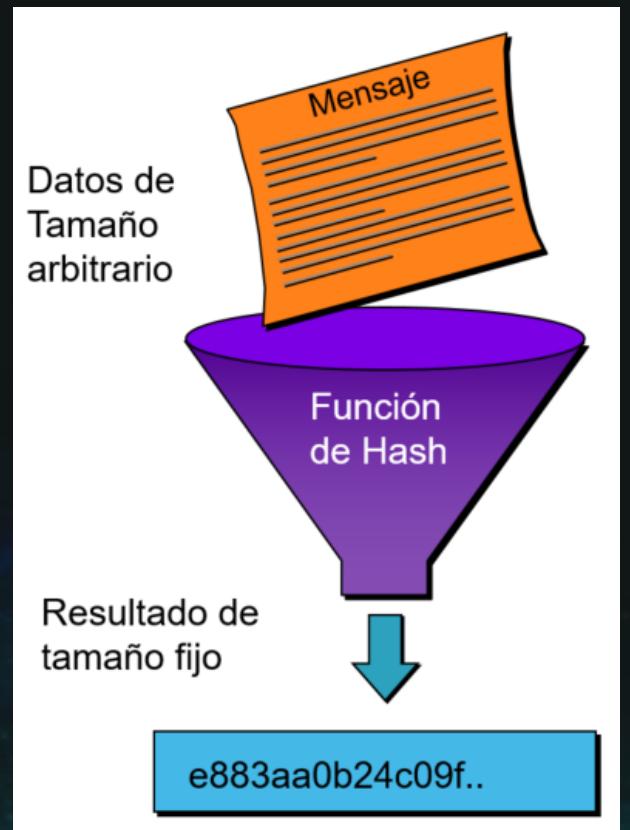
- El atacante obtiene texto cifrado correspondiente a un texto plano conocido.

Texto cifrado elegido

- El atacante obtiene texto plano correspondiente a un texto cifrado predeterminado.

Algoritmos de Hash

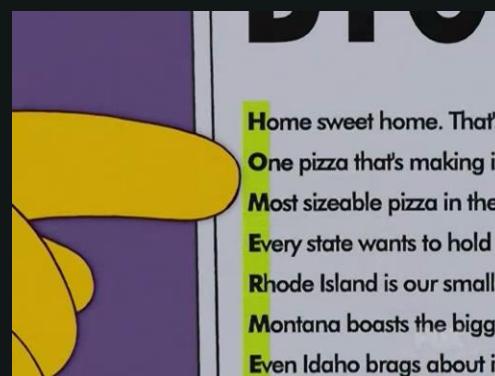
- Función criptográfica de una vía para generar salidas que representen de manera casi unívoca a la entrada.
 - “hash” es el resultado de la función y el tipo de algoritmo.
 - La salida debe tener tamaño fijo independientemente del tamaño de la entrada.
- Colisiones: Dos entradas producen la misma salida.
- Ejemplos de algoritmos:
 - MD5, SHA1, SHA2.



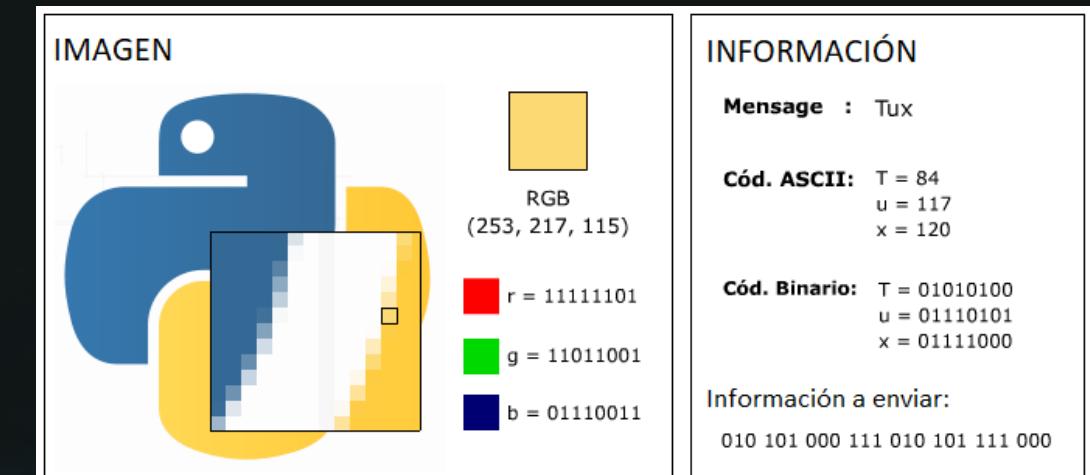
Sal, pimienta y semilla

- Sal
 - Agregar un valor a lo que se quiere cifrar para que produzca otro resultado.
 - Puede no ser secreto, pero debería ser único.
 - Se usa para guardar hashes de contraseñas.
 - Generalmente se guarda junto al hash.
- Pimienta
 - Similar a la sal, pero secreto.
 - Generalmente se usa 1 solo caracter al final de la contraseña.
 - Se puede combinar con la sal.
 - No se guarda con el hash.
- Semilla
 - Valor usado para iniciar un numero aleatorio.
 - Tiene que ser secreto.
 - Se usa para el vector inicial.

Esteganografía



- Conjunto de técnicas para comunicar un mensaje ocultando la información dentro de un conjunto de datos para que pase desapercibida.
 - fotografías, audio y video.
 - Puede ser muy difícil de detectar.
- Incluso si se considera que un archivo analizado no contiene información oculta, aun puede tenerla y no haber sido detectada.
- En el caso de encontrar la información, aun puede estar encriptada y resultar ilegible de manera directa.



Esteganografia		Información	Pixeles esteganografiados
Pixels	Información		
	0		r = 11111100 g = 11011001 b = 01110010
	1		r = 11111111 r = 11001100 r = 00111111
	0		:
	1		:
	:		:

jitsi.org Esteganografía en APTs 2019/2020 - una muestra mediática

- Ursnif (Feb, 2019) – C&C -> PNG (Lsb) -> Powershell
- Powload (Mar, 2019) – C&C -> PNG (Invoke-PSImage, Lsb) -> Powershell
 - <https://github.com/peewpw/Invoke-PSImage>
- Oceanlotus APT group – APT32 (Abr, 2019) – C&C -> PNG (Lsb) -> shellcode
- Scarcraft, Reaper... – APT37 (May, 2019) – C&C -> JPEG (EoF)
- LightNeuron/Turla (May, 2019) – C&C -> Adjunto a mail -> PDF o JPEG -> Comandos
- • Platinum APT Group (Jul, 2019) – C&C -> HTML -> Orden de tags y espacios/tabuladores -> Comandos
- Waterbug/Turla (Jun, 2019) & XMRig miner (Oct, 2019) – C&C -> fichero Wav (Lsb) -> Dll -> criptominer
- Lokibot (Ago, 2019) – Zipx file attachments -> PNG/JPEG (Lsb) -> binario
- Operation Ghost – The Dukes (Oct, 2019) – C&C (Ej. Dropbox) → PNG (Lsb)/BMP → Backdoor
- Titanium, Win10 Trojan backdoor (Nov, 2019) – C&C → PNG → Backdoor commands
- MyKings/DarkCloud/Smominru botnet (Dic, 2019) – JPEG (EoF) → SQL brute forcer
- New Magecart Skimmers (Dic-Ene, 2020) – JPEG (EoF) → Javascript code
- OilRig – APT34 (Jul-Ago, 2020) – [RDAT - BMP (Lsb)] y DoH -> info desde/hacia C2



Estegananálisis

- Debido a que la esteganografía deja huellas en el medio de transporte utilizado, las técnicas de estegananálisis intentan detectar estos cambios, usando incluso complejos mecanismos estadísticos.
- Tipos:
 - **Estegoanálisis manual:** Buscar de forma manual diferencias entre el fichero original y el esteganografiado, identificando cambios en la estructura para localizar datos ocultos.
 - Se necesita tener un fichero original.
 - Es casi imposible descifrar el mensaje.
 - **Estegoanálisis estadístico:** Consiste en el cotejo de la frecuencia de distribución de colores en el caso de un fichero de imagen esteganografiada.
 - Es una técnica lenta para la que se deben emplear software especializado.

¡Gracias!