

Criptografía

Fernando Martínez
fernando.martinez@upc.edu

Departament de Matemàtiques • Universitat Politècnica de Catalunya

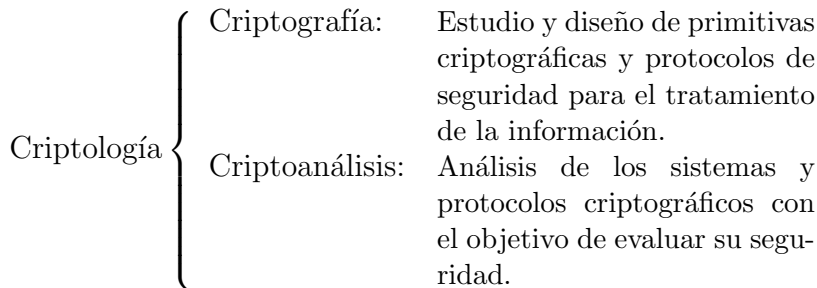
1 de septiembre de 2023

Ejemplos de necesidad de seguridad

- Comunicaciones digitales: Mensajería instantánea, telefonía, EFT (Electronic Fund Transfer), correo electrónico,...
- Acceso a información reservada: cuentas bancarias, bases de datos personales, GPS (Global Position System), historial médico,...
- Integridad de la información: bases de datos, cuentas bancarias,...
- Acceso a recursos *limitados*: Wifi, juegos on line, audio and video on demand (AVOD)...
- Comercio electrónico.

Medidas de seguridad

- Protección física contra daños accidentales o intencionados.
- Control físico de accesos:
 - Identificación de los usuarios por características físicas (biometría).
 - Protección de los componentes del sistema (terminales, cables,...) para evitar intrusiones.
- Medidas administrativas: Políticas de seguridad.
- Medidas legales:
 - Elaboración de leyes que permitan perseguir las conductas delictivas.
 - Derogación de leyes que impidan la investigación en seguridad.
- Medidas lógicas: Sistemas que proporcionan seguridad a base de transformar la información: CRIPTOGRAFÍA.



Criptoanálisis

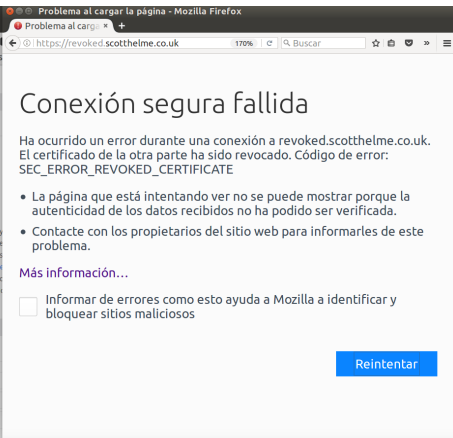
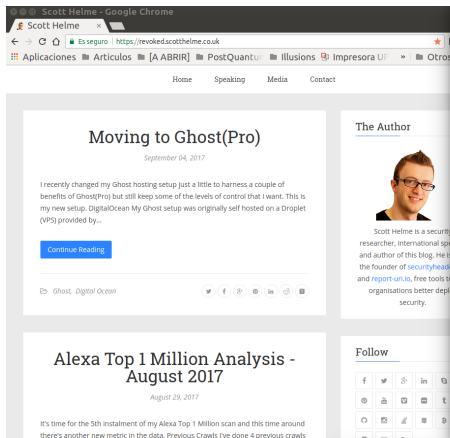
Objetivo: Ser capaz de realizar transformaciones criptográficas (cifrado, descifrado, firma...) sin necesidad de conocer la clave (romper el sistema).

Suposición: **Principio de Kerckhoff:** El criptoanalista (atacante) conoce el algoritmo criptográfico. La seguridad reside en el secreto de la clave.

- ~~Security by Obscurity~~ Los sistemas que ocultan los algoritmos criptográficos usados no son seguros por definición: pueden contener puertas traseras o no haber sido suficientemente estudiados.¹
- Muchas veces la seguridad no depende del algoritmo criptográfico empleado sino de sus implementaciones.²

¹ Researchers find deliberate backdoor in police radio encryption algorithm

² Ver captura de pantalla siguiente



Criptografía: Tipos de ataques

Según el material disponible:

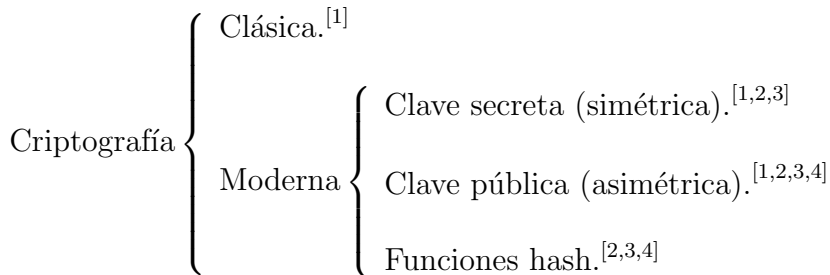
- Texto cifrado (o criptograma).
- Criptograma y texto en claro correspondiente.
- Textos seleccionados y los criptogramas correspondientes (CPA: chosen-plaintext attack)
- Criptogramas seleccionados y los textos en claro correspondientes. (CCA: chosen ciphertext attack)

Según el nivel de éxito:

- Obtención de la clave.
- Descifrado un texto sin la clave.
- Obtención de alguna información parcial del texto o la clave.

Específico del sistema criptográfico:

- Factorización.
- Cálculo logaritmo discreto.
- Criptoanálisis diferencial...



- ❶ Confidenciabilidad.
- ❷ Integridad.
- ❸ Autenticación.
- ❹ No repudio.

Primitiva criptográfica: Sistema criptográfico

$(\mathcal{M}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ es un sistema criptográfico si:

- 1 \mathcal{M} es el conjunto de los posibles mensajes,
- 2 \mathcal{C} es el conjunto de los posibles mensajes cifrados o criptogramas,
- 3 \mathcal{K} es el conjunto de las posibles claves,
- 4 $\forall k \in \mathcal{K}$ existe una transformación de cifrado $e_k \in \mathcal{E}$ y otra de descifrado $d_k \in \mathcal{D}$ tales que:

$$e_k : \mathcal{M} \longrightarrow \mathcal{C} \qquad d_k : \mathcal{C} \longrightarrow \mathcal{M}$$

$$d_k(e_k(m)) = m \quad \forall m \in \mathcal{M}.$$

César.

$$\mathcal{M} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_n$$

$$e_k(m) = m + k \pmod{n}, \qquad d_k(c) = c - k \pmod{n}.$$

Criptografía clásica

- Anterior a la aparición de los ordenadores modernos.
- Tiene por objetivo la confidenciabilidad.
- Usos militares y diplomáticos.
- Generalmente trabaja con el alfabeto.
- Las transformaciones básicas que utiliza son:
 - Sustituciones:
 - Monoalfabéticas: la misma permutación para cada letra.
 - Polialfabética: distintas letras, distintas permutaciones.
 - Permutaciones.

Criptografía clásica: César

Cada letra se sustituye por otra que ocupa k posiciones más allá en el alfabeto.

A \rightarrow Z, B \rightarrow A, C \rightarrow B, ..., Z \rightarrow Y
IBM \rightarrow HAL

- $\mathcal{M} = \mathbb{Z}_n$
- $\mathcal{C} = \mathbb{Z}_n$
- $\mathcal{K} = \mathbb{Z}_n$
- $e_k(m) = m + k \pmod n$
- $d_k(c) = c - k \pmod n$.

Criptografía clásica: Escítala



Figure: Escítala espartana, consistente en una vara sobre la que se enrolla una tira estrecha de cuero en la que hay escritas unas letras. Estirada, las letras sobre la cinta de cuero carecen de sentido). [From Wikimedia Commons, the free media repository](#)

Escítala

NO OS ASUSTEIS \rightarrow

N	O	S	O	S
	A		U	
T	E	I	S	

 \rightarrow N TOAE SIOUSSS

Criptografía clásica: Escítala

- $\mathcal{M} = (\mathbb{Z}_n)^r$
- $\mathcal{C} = (\mathbb{Z}_n)^r$
- $\mathcal{K} = \mathcal{A}$, \mathcal{A} conjunto de matrices de permutación $r \times r$
- $e_k(M) = AM$
- $d_k(C) = A^{-1}C$, A^{-1} matriz inversa de A .

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ \dots & & & & & & & & & & & & & & \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Criptografía clásica: Vigenère

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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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

Criptografía clásica: Vigenère

- $\mathcal{M} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_n \times \cdots \times \mathbb{Z}_n = (\mathbb{Z}_n)^r$
- $e_k(\mathbf{m}) = \mathbf{m} + \mathbf{k} \pmod n$
- $d_k(\mathbf{c}) = \mathbf{c} - \mathbf{k} \pmod n$

- Mensaje a cifrar:

MENSAJESECRETO – 12,4,13,18,0,9,4,18,4,2,17,4,19,14

- Clave de cifrado: CLAVE – 2,11,0,21,4

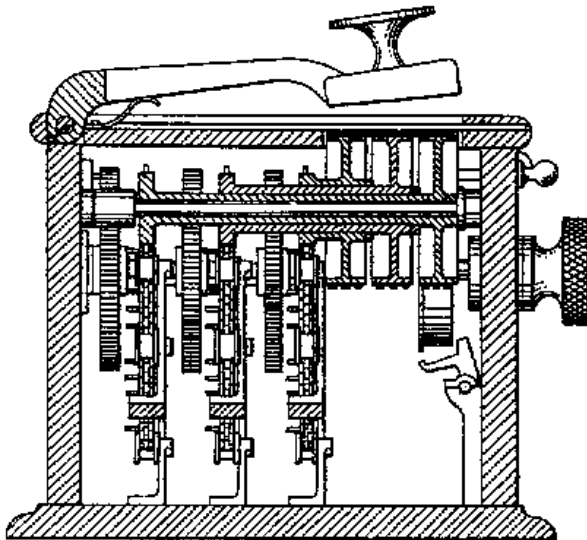
- Cifrado:

12	4	13	18	0	9	4	18	4	2	17	4	19	14
2	11	0	21	4	2	11	0	21	4	2	11	0	21
<hr/>													
14	15	13	13	4	11	15	18	25	6	19	15	19	9

- Criptograma:

OPNNELPSZGTPTJ

Hill Lester S, Louis Weisner, US Patent 1845947
Filed 14 Feb 1929.



Criptografía clásica: Hill

- $\mathcal{M} = (\mathbb{Z}_n)^r$
- $\mathcal{C} = (\mathbb{Z}_n)^r$
- $\mathcal{K} = \mathcal{A} \times (\mathbb{Z}_n)^r$, \mathcal{A} conjunto de matrices $r \times r$ invertibles módulo n ,
 $k = (A, B)$
- $e_k(M) = AM + B \pmod n$
- $d_k(C) = A^{-1}(C - B) \pmod n$, A^{-1} matriz inversa de A módulo n .

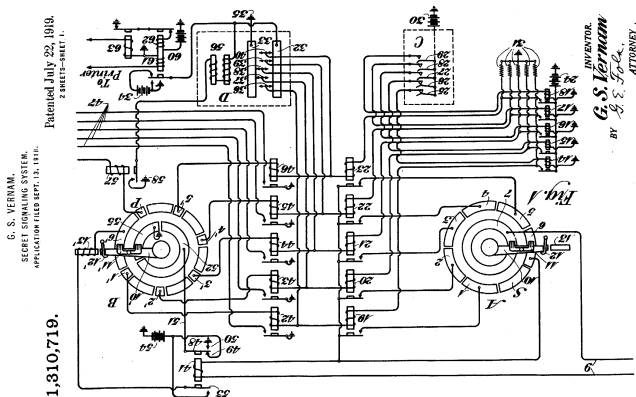
$$n = 26, r = 2$$

$$A = \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}, \quad A^{-1} = \begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix}.$$

No todos los pares (A, B) son posibles.

Gilbert S. Vernam, US Patent 1310719

Filed 13 September 1918.



Criptografía clásica: Vernam

También conocido como *one time pad*.

- Propuesto en 1917 para transmisiones telegráficas. Utiliza un alfabeto de 32 letras representadas por 5 bits.
- Su funcionamiento es igual que el criptosistema de Vigenère pero con una clave de longitud igual a la del mensaje.
- Las claves sólo se pueden utilizar una única vez.
- Es el único que es **incondicionalmente seguro**.

Seguridad

- **Incondicionalmente seguro:** La probabilidad de que un criptograma provenga de un mensaje determinado es igual a la probabilidad a priori del mensaje.

César

- Criptograma: TJ
- Posibles mensajes: UK, VL, WM, XN, YO, ZP, AQ, BR, CS, DT, EU, FV, GW, HX, IY, JZ, KA, LB, MC, ND, OE, PF, QG, RH, SI.

Vernam

- Criptograma: TJ
 - Posibles mensajes: TK, TL,..., TI, UK, UL,..., UI,..., NO,..., SI.
- **Computacionalmente seguro:** Si con *recursos limitados* no puede ser *roto*.



Shannon, Claude E.

Communication Theory of Secrecy Systems

Bell System Technical Journal (USA: AT&T Corporation) 28 (4):
656–715, (1949).

[doi:10.1002/j.1538-7305.1949.tb00928.x](https://doi.org/10.1002/j.1538-7305.1949.tb00928.x)