

# Cifrado simétrico

Mikel Egaña Aranguren

[mikel-egana-aranguren.github.io](https://mikel-egana-aranguren.github.io)

[mikel.egana@ehu.eus](mailto:mikel.egana@ehu.eus)



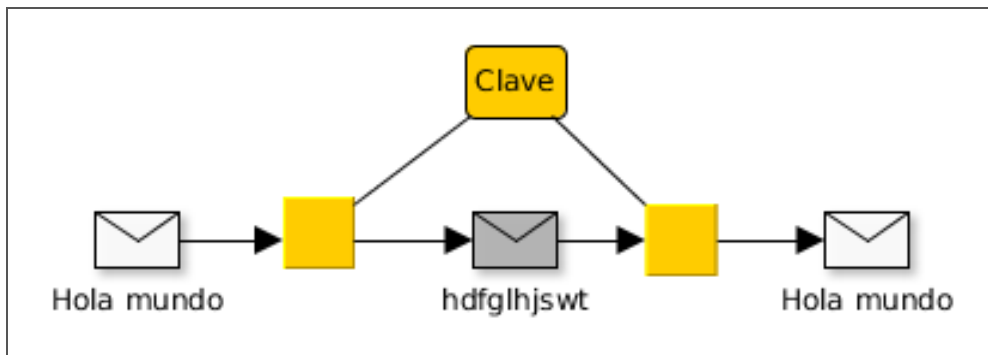
# Cifrado simétrico

<https://doi.org/10.5281/zenodo.4302267>

<https://github.com/mikel-egana-aranguren/EHU-SGSSI-01>



# Criptosistemas de clave privada



# Criptosistemas de clave privada

**Cifrado en flujo:** cifrar un flujo continuo de bits

**Cifrado en bloque:** dividir el mensaje en bloques del mismo tamaño y aplicar el algoritmo a cada uno

# Criptosistemas de clave privada: Objetivos

- Convertir el mensaje en ininteligible
- Recuperar la información cifrada
- Implementación lo más sencilla posible

# Criptosistemas de clave privada

Técnicas básicas en criptografía clásica

- Transposición (los caracteres originales simplemente cambian de posición)
- Sustitución (los caracteres originales se sustituyen por otros)

# Historia de la Criptografía

- Hasta 1948, criptografía pre científica
- En 1948, Claude Shannon sienta las bases de la Teoría de la Información y de la criptografía moderna
- En 1976 Diffie & Hellman introducen el concepto de criptografía de clave pública

# Método de Escitalo de Esparta

Enrollar una tira de papel en un bastón y escribir el mensaje

Desenrollar el papel y enviarlo al destino



# Método de Escitalo de Esparta



EE\_LSV\_TAVASE\_ONE\_ENAN\_ZOEU\_LL

# Método de Escitalo de Esparta

Se necesita un bastón exactamente igual para descifrar el mensaje

Enrollar la tira de papel alrededor del bastón y leer el mensaje

La clave de este sistema es el diámetro del bastón

# Método de Escitalo 2.0


Distribuir el mensaje en columnas

La clave viene determinada por la cantidad y orden de las columnas

# Método de Escitalo 2.0

Clave 32154

1	2	3	4	5
E	L		P	E
R	R	O		D
E		S	A	N
	R	O	Q	U
E		N	O	T
I	E	N	E	
R	A	B	O	.



3	2	1	5	4
	L	E	E	P
O	R	R	D	
S		E	N	A
O	R		U	Q
N		E	T	O
N	E	I		E
B	A	R	.	O

\_OSONNBLR\_R\_EAERE\_EIR\_EDNUT\_.P\_AQOEO

# Método de Escitalo 2.0

## Criptoanálisis

- Basado en combinatoria
- Calcular el tamaño de los bloques
- Combinar los bloques en distinto orden hasta encontrar alguno con sentido

# Método César

Cifrado monoalfabético

Empleado por Julio César

Consiste en sumar 3 a la posición de cada letra en el alfabeto

# Método César

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
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	C

Los galos se resisten → Ñrv jdñrv vh uhvhwph

# Método de Atbash (Espejo)

Cifrado monoalfabético

Técnica proveniente del alfabeto hebreo

Consiste en sustituir cada carácter por su "contrario"



# Método de Atbash (Espejo)

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

Quedamos a las dos → Jfvwzñlh z ozh wlh

# Método Afín

Cifrado monoalfabético

Generalización método César

$$E_{(a;b)}(M) = (aM + b) \bmod N$$

N es el número de caracteres del alfabeto

César es una transformación afín con  $E(1,3)$

# Método Diccionario

Cifrado monoalfabético

Generar la tabla de correspondencias de manera "manual"

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

Desordenado

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

En base a una palabra

# Método Polybius

Cifrado monoalfabético

Pueden ser caracteres o dígitos



# Métodos de Sustitución monoalfabéticos

Criptoanálisis basado en estadística

Método establecido por Al-Kindi en el siglo 9

Un carácter "original" siempre se sustituye por el mismo carácter/es

Se sabe cuáles son los caracteres más frecuentes en cada idioma

Se sabe las palabras de dos/tres/cuatro caracteres (bigramas, trigramas y tetragramas) más frecuentes en cada idioma

# Métodos de Sustitución monoalfabéticos

Se va "probando" y deduciendo

Cuanto más largo es el texto cifrado, mejor

Hay que saber el idioma del texto original

# Métodos de Sustitución monoalfabéticos

Porcentaje de aparición de caracteres en castellano

e - 16,78%	r - 4,94%	y - 1,54%	j - 0,30%
a - 11,96%	u - 4,80%	q - 1,53%	ñ - 0,29%
o - 8,69%	i - 4,15%	b - 0,92%	z - 0,15%
l - 8,37%	t - 3,31%	h - 0,89%	x - 0,06%
s - 7,88%	c - 2,92%	g - 0,73%	k - 0,00%
n - 7,01%	p - 2,776%	f - 0,52%	w - 0,00%
d - 6,87%	m - 2,12%	v - 0,39%	

Ejemplo de descifrado por análisis de frecuencias

# Métodos de Sustitución monoalfabéticos

Técnicas para dificultar el criptoanálisis

- Eliminar los espacios en blanco
- Alterar el texto original manteniendo su significado (Ej. SMS, WhatsApp, ...)
- Usar pictogramas con significado (Libro de códigos)
- Evitar la correspondencia 1-1 usando el mismo carácter en más de una ocasión (Sistemas polialfabéticos)



# El disco de Alberti

Primer sistema polialfabético

Dos discos concéntricos, el interior móvil

Durante el cifrado, se va moviendo, por lo que en el cifrado se usan  $X$  alfabetos (correspondencias) distintas

La clave es la posición inicial, cada cuántos caracteres se gira el disco, cuánto se gira y en qué dirección

# El disco de Alberti

The Alberti and Jefferson Code Disks



# La máquina Enigma

Es probablemente el elemento criptográfico más conocido de la historia

Originalmente diseñada para uso civil

Modificada para uso militar y usada por los nazis

# La máquina Enigma

158,962,555,217,826,360,000 (Enigma Machine) - Numberp...



# La máquina Enigma

El matemático polaco Marian Rejewski estableció las bases para descryptar Enigma

- Crearon máquinas electromecánicas llamadas "bombas"
- Los nazis añadieron 2 nuevos rotores y las "bombas" polacas no daban abasto con el nuevo número de posibilidades

# La máquina Enigma

El equipo de [Alan Turing](#) partió de esta información para crear su propia "bomba" más eficiente y resistente a cambios de configuración

Flaw in the Enigma Code - Numberphile



# Métodos de sustitución polialfabéticos

## Criptoanálisis

- Usando métodos estadísticos
- Se buscan patrones para deducir tamaños de las claves, orden de los distintos trozos, etc.
- Hace falta más texto encriptado que en los sistemas monoalfabéticos

# Métodos de cifrado de flujo

En vez de cifrar un mensaje, cifran bit a bit

Usado para comunicaciones en tiempo real (No se puede esperar a tener el mensaje completo para cifrarlo y transmitirlo)

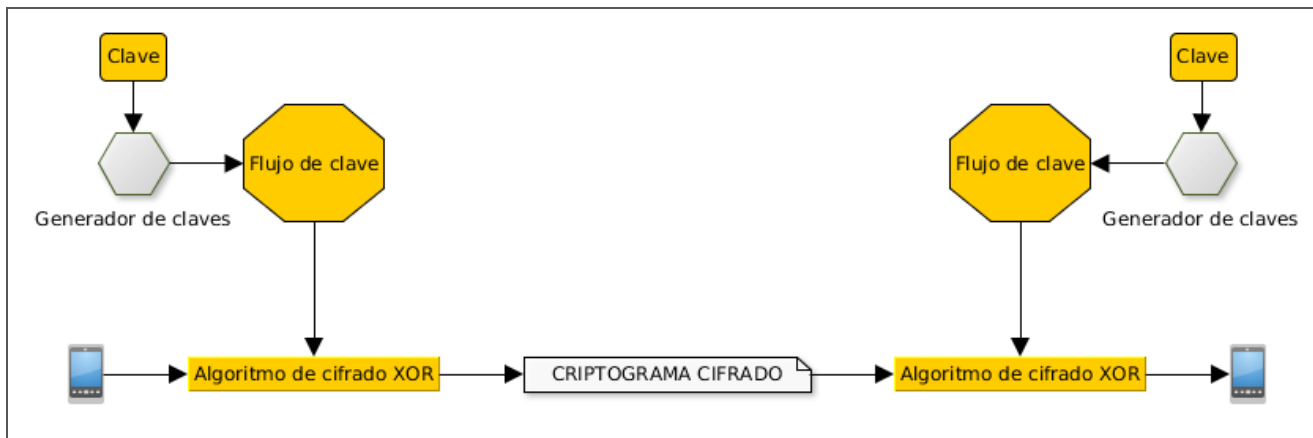


# Métodos de cifrado de flujo

A partir de la clave, se usa un generador "pseudoaleatorio" que genera el flujo de clave

La operación XOR entre el bit a cifrar y el flujo de clave, genera el criptograma

# Métodos de cifrado de flujo



# Método de Vernam

Realiza el cifrado XOR entre el texto y una clave aleatoria de la misma longitud

El generador es realmente aleatorio

# Método de Vernam

La clave (el flujo de clave) es lo denominado "libreta de un solo uso":

- Sólo se usa una vez
- Hay que enviársela al receptor del mensaje
- Está demostrado matemáticamente que es irrompible

No es práctico

# Otros métodos de cifrado de flujo

Basados en el método de Vernam

Usar claves pseudoaleatorias generadas a partir de una semilla y un algoritmo de generación

Con la semilla y el algoritmo de generación se podría reconstruir la clave pseudoaleatoria (Depende del número de posibles semillas distintas)

# Otros métodos de cifrado de flujo

No son matemáticamente irrompibles

Ejemplos:

- RC4 (ARC4) usado en TLS/SSL , WEP y WPA entre otros (Roto)
- A5/1 (y distintas versiones) usado en comunicaciones GSM (A5/1 y A5/2 rotos)

# Métodos de cifrado por bloques

Partir el mensaje original en bloques de tamaño fijo:

- Si el tamaño es suficientemente pequeño, puede considerarse cifrado de flujo
- Existen algoritmos de rellenado para aquellos casos en los que el tamaño del mensaje no sea múltiplo del tamaño del bloque

# Métodos de cifrado por bloques

Cada bloque de mensaje original genera un bloque de mensaje cifrado

Se pueden añadir iteraciones, permutaciones y operaciones entre los distintos bloques



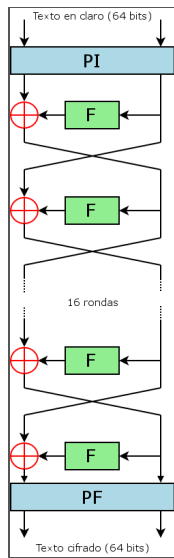
# Métodos de cifrado por bloques

- DES
- Triple DES
- AES
- IDEA
- KASUMI

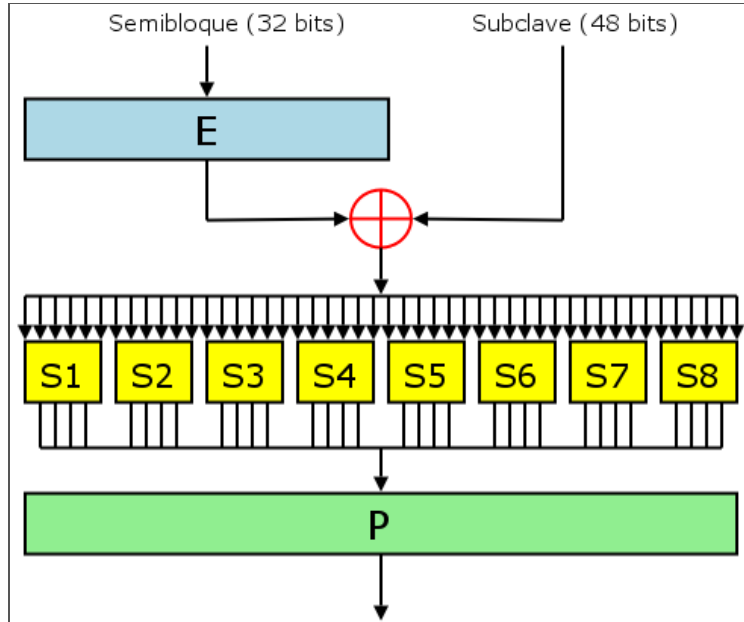
# DES (Data Encryption Standard)

- 1975
- Primer estándar
- Bloques de 64 bits
- Clave de 56 bits (64 - 8 como propuesta de la NSA para asegurarse de que podían romperlo -???)
- 16 rondas
- Se puede romper en menos de 24 horas

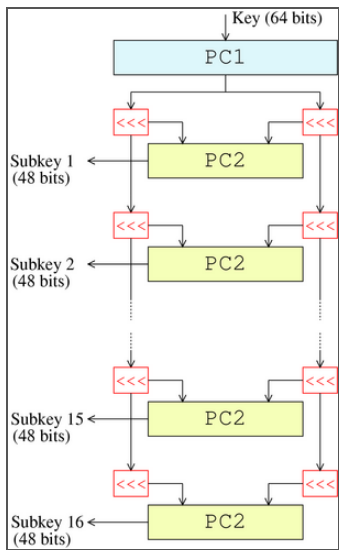
# DES (Data Encryption Standard)



# DES (Data Encryption Standard)



# DES (Data Encryption Standard)



<https://commons.wikimedia.org/wiki/File:DES-key-schedule.png>

# Triple DES

- Concebido como sucesor de DES, pero en desuso
- Todavía se usa en tarjetas de crédito
- Basado en realizar 3 ejecuciones de DES (Cifrar – Descifrar - Cifrar)
- Bloques de 64 bits
- Claves de 168 bits ( $3 \cdot 56$ ), clave efectiva 112 bits

# AES (Advanced Encryption Standard)

- Rijndael
- Estandarizado por el Instituto Nacional de Normas y Tecnología (NIST), EEUU
- Sustituto de (Triple) DES
- Muy usado en todo tipo de comunicaciones y transacciones
- Bloques de 128 bits
- Claves de 128, 192 ó 256 bits
- 8 rondas (claves de 128) , 12 rondas (claves de 192), 14 rondas (claves de 256)

# IDEA (International Data Encryption Algorithm)

- Bloques de 64 bits
- Clave 128 bits
- 8 rondas y media
- Está considerado seguro (excepto algunas claves débiles)
- Incluido en OpenPGP



# KASUMI (A5/3)

- Bloques de 64 bits
- Clave de 128 bits
- 8 rondas
- Usado en las redes 3G (con alguna variación)
- El original se puede [romper fácilmente](#) (probado en 2010)

# Ataques por fuerza bruta

Siempre encuentra la solución

Consiste en probar todas las claves posibles

Hay que conocer el algoritmo de cifrado y el espacio de claves

No siempre es posible por su coste temporal

# Ataques por fuerza bruta

Espacio de claves:

- 56 bits:  $2^{56}$  posibilidades
- 128 bits:  $2^{128}$  posibilidades
- 256 bits:  $2^{256}$  posibilidades

# Ataques por fuerza bruta

Tiempo que se tardaría con un superordenador:

- 56 bits: 0,04 segundos
- 128 bits: 7.193.522.047 milenios (año arriba, año abajo)
- 256 bits: ...

# Ataques por fuerza bruta

Se puede hacer un ataque por fuerza menos bruta y más "inteligente":

- Usando un diccionario
- Usando datos del dueño de la clave
- ...

# Claves débiles

- Pueden presentarse según las características de cada algoritmo
- Claves cuyo comportamiento no es el deseado
  - $E_K(M)=M$
  - $E_K(E_K(M))=M$
  - $D_{K2}(E_{K1}(M))=M$