

Cifrado

Mikel Egaña Aranguren

mikel-egana-aranguren.github.io

mikel.egana@ehu.eus



Cifrado

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

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



Indice

- Introducción
- Esteganografía
- Métodos de encriptación
 - Ataques por fuerza bruta
 - Algoritmos de resumen
 - Contraseñas en Sistemas Operativos
- Encriptación asimétrica

Introducción

Criptografía: cifrar la información

Mecanismo de seguridad muy antiguo

Asegura

- Confidencialidad (Cifrado)
- Integridad (Algoritmos resumen)
- Autenticidad (Certificados digitales)

Introducción

Esteganografía: **ocultar** la información

Criptografía: **cifrar** la información

Introducción

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

Introducción

Criptoanálisis: técnicas para descifrar mensajes encriptados

- Sin conocer la clave
- Obteniendo la clave a partir de uno o varios mensajes encriptados
- El algoritmo es público - [Principio de Kerckhoffs \(1883\)](#)

Criptología: Criptografía + Criptoanálisis

Introducción

Criptosistema: $D_K (E_K (M)) = M$

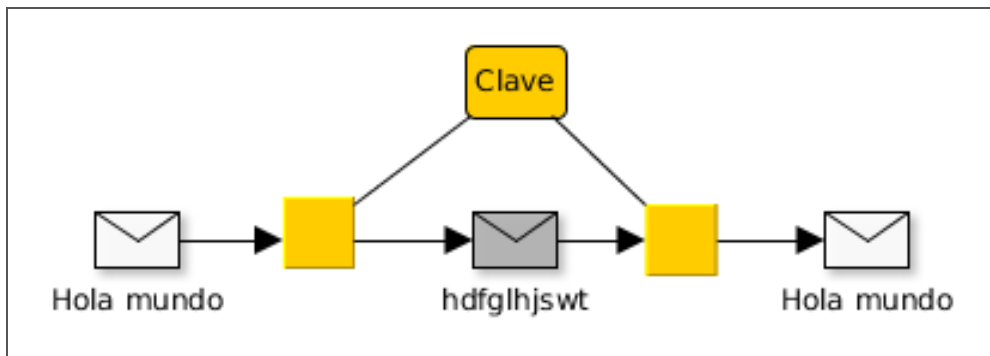
- M: Conjunto de todos los mensajes sin cifrar
- C: Conjunto de todos los mensajes encriptados (criptogramas)
- K: Conjunto de claves posibles
- E: algoritmo de encriptación
- D: algoritmo de desencriptación

Introducción

Criptosistemas

- Simétricos o de clave privada
 - Una clave para encriptar y desencriptar
 - Cifrado en bloque o cifrado en flujo
- Asimétricos o de clave pública
 - Una clave para encriptar y otra para desencriptar
 - Lo que una encripta, la otra lo desencripta

Criptosistemas de clave privada



Criptosistemas de clave privada

Claves débiles

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

Esteganografía

Consiste en ocultar información de forma que no sea “visible” para quien no sepa la clave

Sin saber la clave, puede parecer que no hay información oculta

Es la técnica precursora de la criptografía

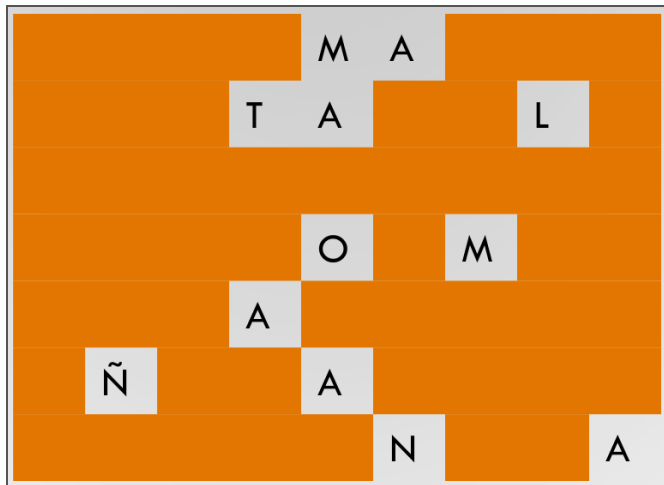
Esteganografía

Histaiaeo (gobernador de Mileto) buscaba aliados para sublevarse contra el rey persa Darío I

Necesitaba enviar mensajes que nadie detectara

- Rapaba el pelo a los mensajeros
- Les grababa el mensaje en la cabeza
- Esperaba a que les creciera el pelo, y los mandaba al destino
- En el destino les volvían a rapar la cabeza y leían el mensaje

Esteganografía



Esteganografía

Seleccionando unos caracteres determinados

Los asirios tenían amarrados los caballos a anclajes mientras los olmecas sólo ajustaban largos amarres sobre octogonales calesas que se hacían ocultar.

Clave: primera letra de cada palabra no monosílaba

Los **A**sirios **T**enían **A**marrados los **C**aballos a **A**ncclajes **M**ientras los **O**lmecas **S**ólo
Ajustaban **L**argos **A**marres **S**obre **O**ctogonales **C**alesas que se **H**icían **O**cultar.

Esteganografía

Ocultación de información en archivos multimedia (normalmente imágenes)

En formato BMP cada pixel en RGB son 3 bytes

LSB (Less Significant Bit): Modificar el último bit de cada byte es inapreciable

Esteganografía

Por ejemplo, para ocultar texto, insertamos el código ASCII del carácter deseado

A → 65 → 01000001

```
(11011010) (01001001) (01000010)
(00011110) (01011010) (11011110)
(00001110) (01000111) (00000111)
```

Método de encriptación

Objetivos

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

Método de encriptación

Técnicas básicas en criptografía clásica

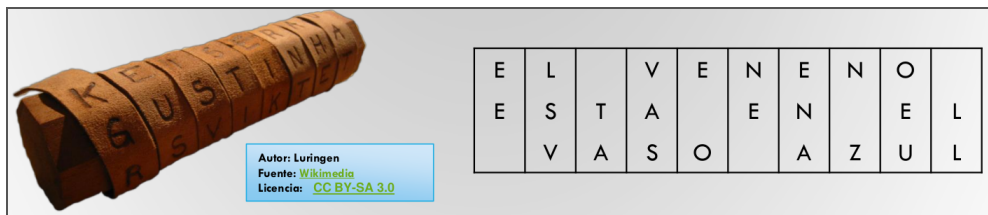
- Transposición (los caracteres originales simplemente cambian de posición)
- Sustitución (los caracteres originales se sustituyen por otros)

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 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 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 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

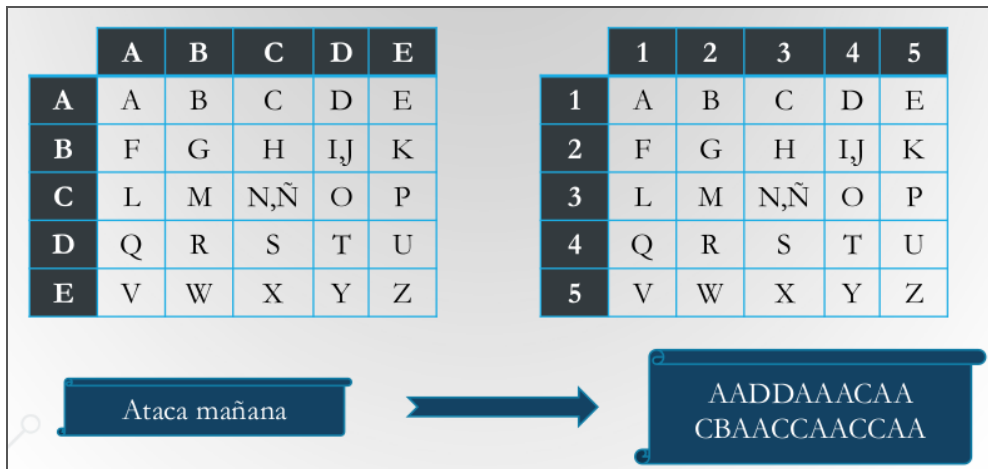
a	b	c	d	e	f	g	h	i	j	k	l	m	n	ñ	o	p	q	r	s	t	u	v	w	x	y	z
M	U	R	C	I	E	L	A	G	O	B	D	F	H	J	K	N	Ñ	P	Q	S	T	V	W	X	Y	Z

En base a una palabra

Método Polybius

Cifrado monoalfabético

Pueden ser caracteres o dígitos



Métodos de Sustitución monoalfabéticos

Criptografía 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 codigos)
- Evitar la correspondencia 1-1 usando el mismo carácter en más de una ocasión (Sistemas polialfabeticos)

El disco de Alberti

Primer sistema polialfabetico

Dos discos concentricos, el interior movil

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 maquina 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 maquina enigma

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



La maquina 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 maquina 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

