Criptografía Aplicada

Ing Germán Bollmann

1

AGENDA

Criptografía Clásica
Steganografía
Esquema de Cifrado Simétricos
Cifrado en Bloque Block Ciphers
AES

2

Criptografía Clásica y Steganografía

3

¿Para qué sirve la criptografía?

De esta tríada, ¿de qué me protege la criptografía?

- **CONFIDENCIALIDAD** … ¿qué es?
- **INTEGRIDAD** … ¿qué es?
- **DISPONIBILIDAD** … ¿qué es?
- ¿Por qué hay que cuidar y proteger a la información? … activos
- Hay otros servicios de seguridad donde la criptografía también juega un papel importante:
  - **AUTENTICACIÓN + CONTROL DE ACCESO**
  - **NO REPUDIO**
  - **TRAZABILIDAD** … ¿en cuáles interviene la criptografía?

4

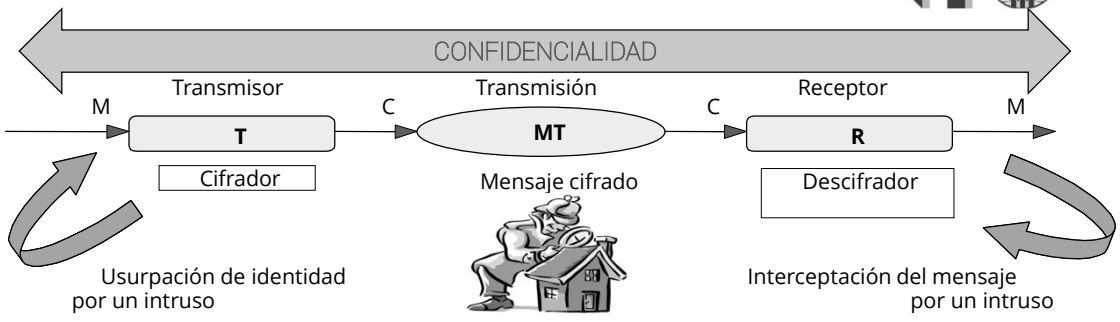
CRIPTOLOGÍA
Criptografía + Criptoanálisis

- **Definiciones**
- **Criptografia:**
- **studia el diseño y propiedades de algoritmos y mecanismos que ofrecen confidencialidad e integridad**
- **Criptoanálisis:**
- **busca vulnerabilidades y desarrolla ataques a los mecanismos criptográficos.**

- **Antiguamente eran consideradas campos de conocimiento diferentes. Sin embargo el criterio actual es considerarlos complementarios: para comprender las fortalezas de un cifrado es importante también conocer los ataques que resiste y viceversa.**

5

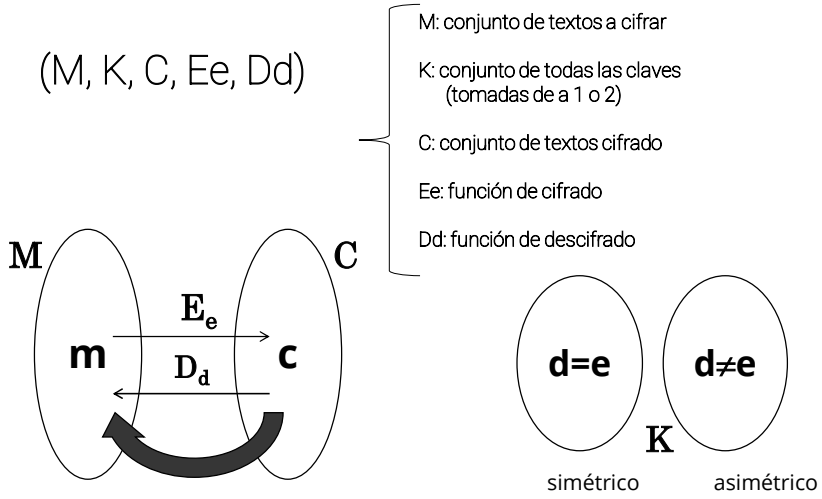
Necesidad del cifrado



- El canal por definición es inseguro.
- Texto en claro, texto cifrado, espacio de claves, algoritmo de cifrado, algoritmo de descifrado, tipos de claves, claves débiles, ...

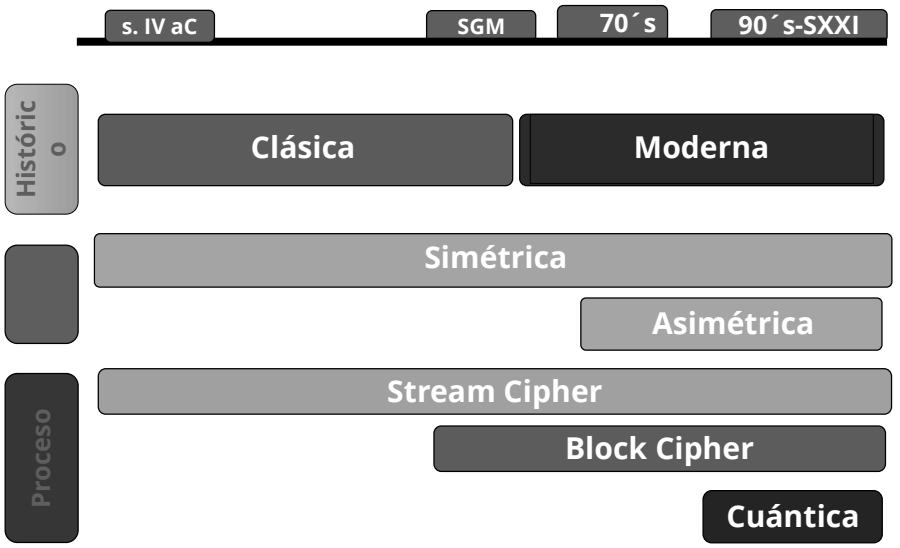
6

Modelo Matemático de un Criptosistema



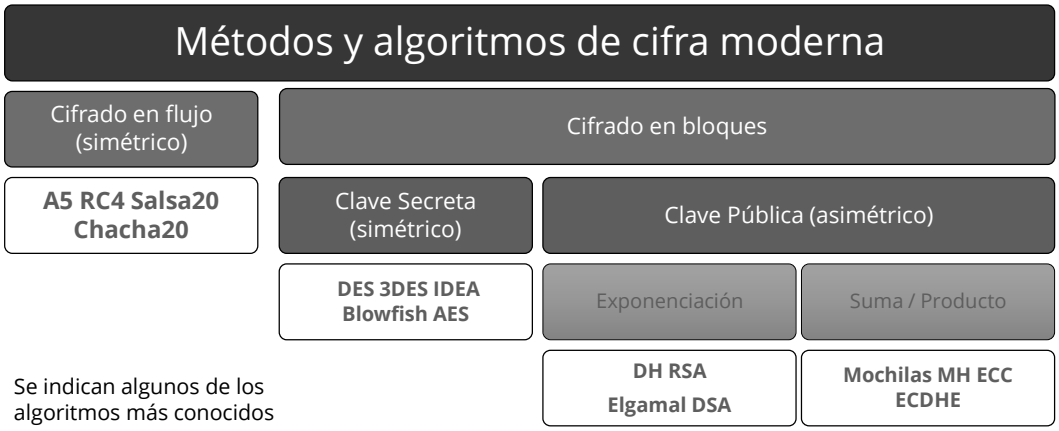
7

Historia y Clasificación



8

Métodos de cifra



Se indican algunos de los algoritmos más conocidos

9

Clasificación de la cifra moderna

Según el tipo de claves

1. **Simétricos o con clave secreta**: Existirá una única clave (secreta) que deben compartir emisor y receptor. Con la misma clave se cifra y se descifra.
2. **Asimétricos o con clave pública**: Cada usuario crea un par de claves, una privada y otra pública, inversas dentro de un cuerpo finito. Lo que se cifra en emisión con una clave, se descifra en recepción solamente con la clave inversa.

Según el tratamiento del mensaje en claro

1. **Cifrado en flujo**: El mensaje en claro se cifra bit a bit con la clave.
2. **Cifrado en bloque**: El mensaje en claro se divide en bloques de algunos bytes, aplicando a continuación la cifra a cada uno de ellos.

10

Cifra simétrica CS o de clave secreta

El emisor toma el mensaje en claro M que transforma mediante un algoritmo E_k utilizando la clave k para obtener el mensaje cifrado C.

Posteriormente el mensaje cifrado C se transmite al receptor, que recibe el criptograma C.

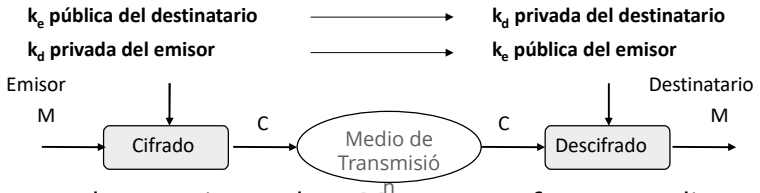
El receptor para la operación de descifrado, toma como entrada el mensaje cifrado C y le aplica el algoritmo D_k igual que el de emisión E_k pero para descifrado, utilizando la misma clave k, para obtener el mensaje en claro M.

D_k es el proceso inverso a E_k.

Simétrico: Se usa la misma clave k en ambos extremos.

11

Cifra asimétrica o de clave pública



El emisor toma el mensaje en claro M que transforma mediante un algoritmo utilizando, por ejemplo, **la clave pública del destinatario** para obtener el mensaje cifrado C, obteniendo así confidencialidad.

El mensaje cifrado se transmite al receptor, que recibe el criptograma C.

El receptor para la operación de descifrado, toma como entrada el mensaje cifrado C y **su propia clave privada** para recuperar M secreto.

También podría haberse cifrado con la clave privada del emisor, obteniéndose en este segundo caso autenticidad en destino.

Asimétrico: Se usan claves diferentes (inversas) en ambos extremos.

12

Criptografía Clásica

13

Cifrado Simétrico o de Clave Privada

La misma clave se utiliza para cifrar y para descifrar

Cada interlocutor tiene que estar en posesión de una copia de la clave

Si se compromete la seguridad de la clave (copiada, robada, extraviada) el sistema es inseguro.

Debe existir la posibilidad de usar muchas claves diferentes

El modelo es igual a las cerraduras tradicionales:

La misma llave que sirve para cerrar la cerradura, también sirve para abrir.

Cada usuario que quiere abrir o cerrar, tiene que tener una copia de la llave.

Si la llave se pierde, es robada o copiada, la seguridad de la cerradura queda comprometida.

Cada cerradura debe tener una llave única, sino se podría abrir las cerraduras de “otros”

14

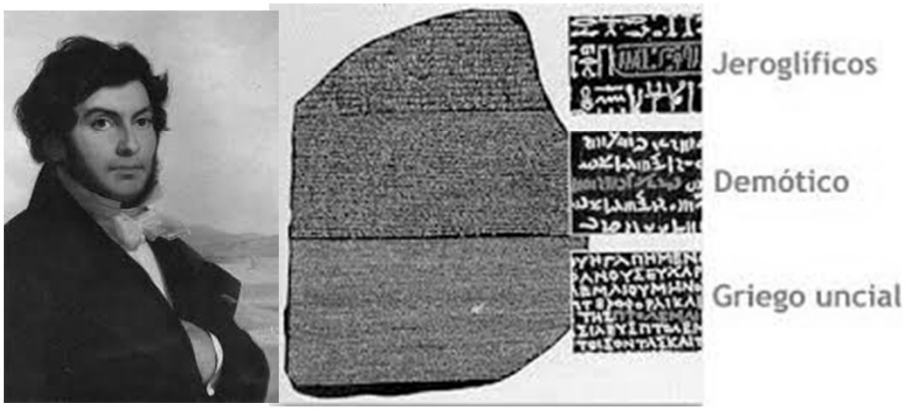
Criptografía Simétrica o de Clave Privada

La misma clave que sirve al emisor para cifrar o "cerrar" el mensaje o texto en claro , es utilizada por el receptor para descifrar o "abrir" el texto cifrado.
El equivalente en la vida cotidiana es la llave de una puerta, que sirve tanto para abrirla como para cerrarla. Dicha clave debe permanecer secreta.

Texto Claro (plain text) → Texto Cifrado (cipher text) → Texto Claro (plain text)

15

Desciframiento de los Jeroglíficos Par texto_claro-texto_cifrado



16

Técnicas Clásicas de Cifrado Transposición

Se mezclan o desordenan las letras del mensaje de acuerdo a un cierto patrón (no aleatorio). Al reordenarlas se recupera el mensaje original.

Transposición
Escítala (Esparta, siglo V a.C)

m: Enviar tropas al amanecer. Leónidas

1	2	3	4	5	6
e	n	v	i	a	r
t	r	o	p	a	s
a	l	a	m	a	n
e	c	e	r	l	e
o	n	i	d	a	s

c: etaeonrlcnvoaeiipmrdaaalarsnes

17

Técnicas Clásicas de Cifrado Sustitución

Sustitución: se sustituye cada caracter o símbolo del mensaje por otro.

Claro	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
Cifrado	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

Usado por Julio César en la llamada Guerra de las Galias siglo I aC.

m: divide y obtendrás el poder. Cayo Julio César
glylgh b rewhpguáv hñ srghu fdbr mxñlr fevdu

c: glylg hbrew hpgua vhñsr ghufd brmxñ lrfev du

https://es.planetcalc.com/1434/?license=1

18

Descripción Matemática del Criptosistema de César

(M, K, C, E, D)

M: el alfabeto de entrada
K: conjunto de todos los "corrimientos" de 1 a 26
C: el alfabeto de salida (podrían ser otros símbolos).
E: k corrimientos a la derecha. (+3)
D: k corrimientos a la izquierda (-3)

CRIPTOANÁLISIS

FUERZA BRUTA
probar una a una las claves hasta encontrar un texto legible. Aquí la cantidad de claves posibles es 26, nada difícil de probar.

ESTADÍSTICAS DEL LENGUAJE
Análisis de Frecuencia (monografo, digrafo, trigrafo).
Las letras tienen distinta frecuencia de aparición en las palabras. Algunas más que otras. El mismo análisis puede hacerse para grupos de dos letras (rr, ll, qu,), tres (cía; etc).

19

¿Cifrar o Codificar?

¿

Si se sustituyen palabras o nombres enteros por otros, entonces se trata de un código y no una cifra.

Por ejemplo el Código Navajo usado en la 2da Guerra Mundial. Se reclutaron más de 400 operadores de radio de ese pueblo originario, a los que se llamó "windtalkers".

Asignaron nombres de animales para distintos artefactos de guerra.

En 2001 el Congreso de EEUU condecoró a los 5 últimos operadores navajos aún con vida.

En 2014 falleció el último de ellos.

20

Cifrado “Indescifrable”

Giovan Battista Bellaso
(*La Cifra del Sig. Giovan Battista Bellaso.* 1553)

Blaise
de Vigenere
1586

Tabla 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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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

21

Vigenere en la práctica

Disco de Alberti
(De Cifris - 1467)

K	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
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	j	k
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	s	t
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	g	h
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	q	r

k:	L	U	I	S	L	U	I	S	L	U	I	S	L	U	I
m:	e	n	v	i	e	n	t	r	o	p	a	s	h	o	y
c:	o	h	d	a	o	h	b	k	z	k	i	s	r	j	g

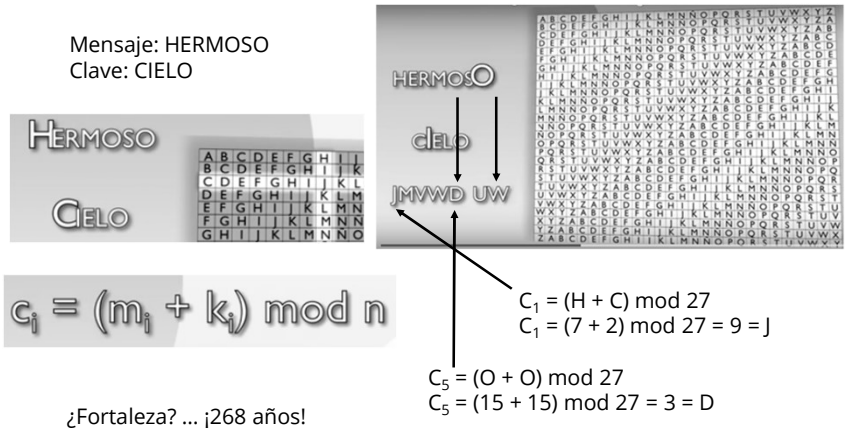
Babbage
1854

Friedrich Wilhelm
Kasiski
1863

Fuente imagen: https://www.mateureka.it/notizie/grafometro-incertezza-dimensionale-disco-cifrante-le-nuove-acquisizioni-di-mateureka.html/attachment/disco-cifrante-leon-battista-alberti

22

La cifra de Vigenère (1586)

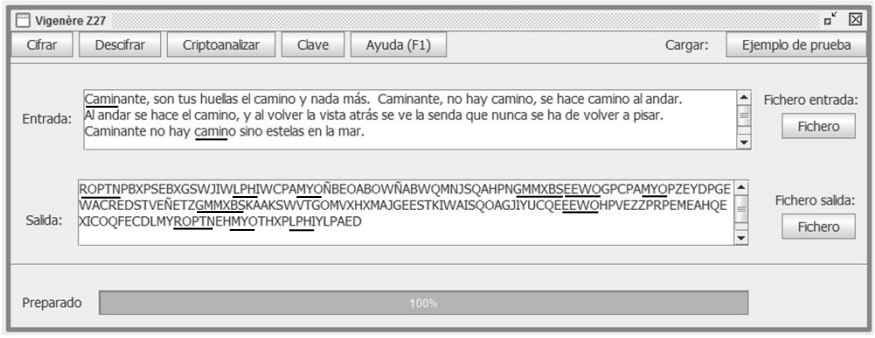


23

Vulnerabilidad de la cifra de Vigenère

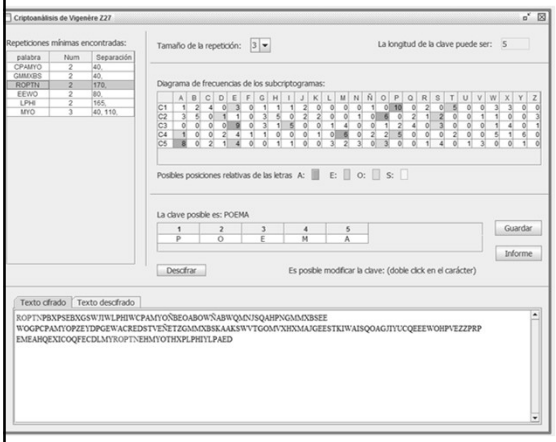
¿Por qué se rompe? Porque se puede transformar en una cifra monoalfabeto por la redundancia del lenguaje.

Clave: POEMA



24

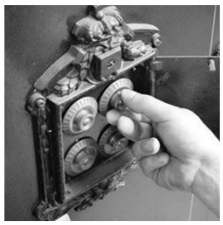
Ataque de Kasiski (1854)

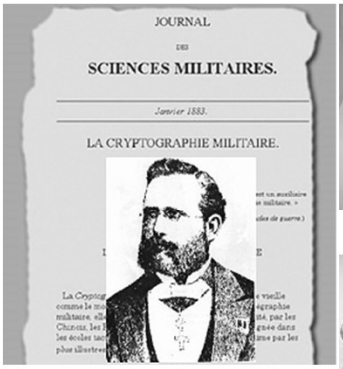


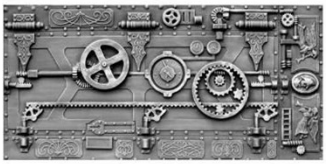
1. Buscar repeticiones de al menos 3 caracteres o más en el criptograma.
2. Encontrar todas las distancias que separan a las repeticiones de caracteres.
3. Hallar el máximo común divisor mcd de todas esas repeticiones.
4. Este número dará la posible longitud L de la clave.
5. Dividir el criptograma en L subcriptogramas leyendo las letras cada L espacios.
6. Cada subcriptograma estará cifrado por una letra: monoalfabeto.
7. Contabilizar los caracteres de cada subcriptograma.
8. Buscar las posiciones relativas de la A, la E y la O (separaciones 0 => +4 => +11) en ese subcriptograma, de acuerdo a la frecuencia de caracteres encontrada.
9. La posición relativa de la letra A en el subcriptograma entrega la letra de la clave.
10. Repetir esta operación para los L subcriptogramas para encontrar la clave.

25

La era de las máquinas
Principios de Kerckhoffs







26

ENIGMA

General Heinz Wilhelm Guderian leyendo un parte recientemente descifrado

Patentada en 1918 por la empresa alemana Scherbius & Ritter, cofundada por Arthur Scherbius, quien compró la patente de un inventor holandés. Se puso a la venta en 1923 para un uso comercial ("comercial" por las restricciones impuestas por la PGM). La Armada alemana la adoptó en 1926. Poco después se extendió a las demás fuerzas alemanas.

C3 del General Heinz Wilhelm Guderian I

Arthur Scherbius

https://www.networkworld.es/archive/pda-para-el-sector-militar-de-aca
https://www.defensa.com/ayer-noticia/misterio-de-la-maquina-enigma

27

The Codebreakers

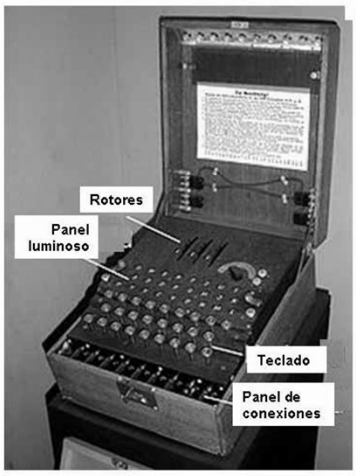
En Bletchley Park, diversos profesionales como ser matemáticas y criptógrafos fueron convocados y asignados al desciframiento de la máquina Enigma. No había una única configuración de la máquina, sino muchas.
Contrariamente a lo que se creía, lograron romper la mayoría de ellas.

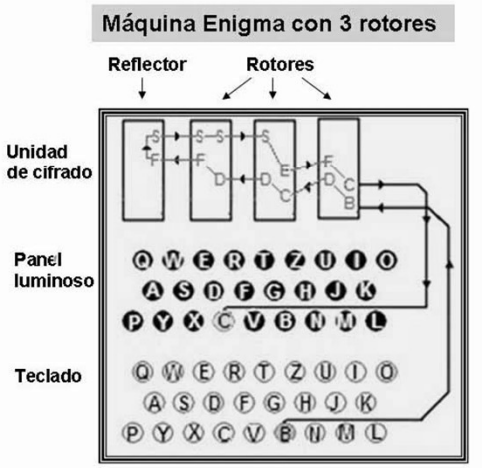
Alan Turing

Sin embargo, las Enigma fueron usadas hasta los años 60, ya que muchas de ellas, recuperadas tras la guerra fueron vendidas a varios países, quienes aún creían que eran seguras.

28

ENIGMA

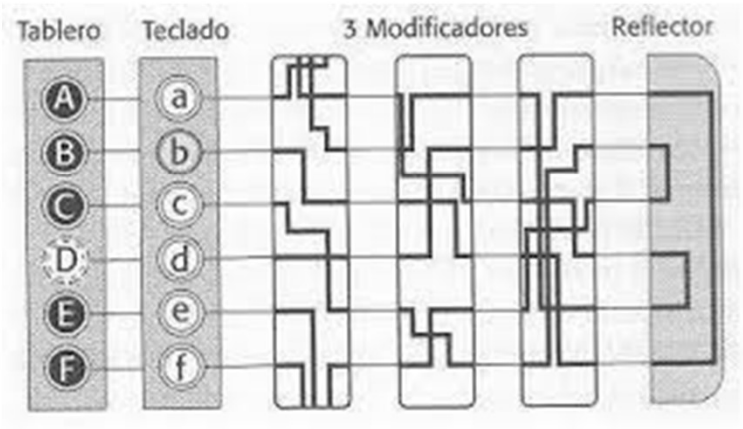




29

ENIGMA

ENIGMA



30

Cifrados sin resolver Manuscrito Voynich

31

Cifrados sin resolver Asesino del Zoodíaco

32

Steganografía

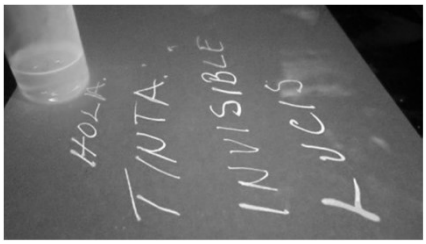
33

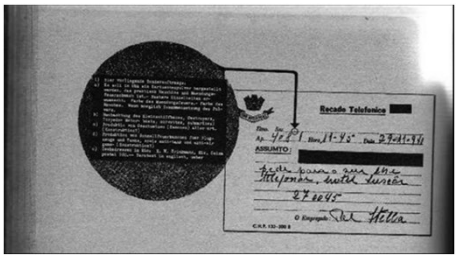
Esteganografía o el Ocultamiento del mensaje

El monje Johannes Trithemius (1462-1516) considerado el más significativo precursor de la esteganografía, escondía sus mensajes ocultos en textos religiosos.

34

Esteganografía - Escritura Invisible





35

San Martín y sus conocimientos en Criptografía

Sobre su época de servicio en España

"Siendo Ayudante de campo del ejercito que comandaba el general Antonio Malet, marqués de Coupigny, es donde aprende y perfecciona su oficio de Oficial de Inteligencia. Toma conocimientos sobre diversos métodos de criptografía y esteganografía."

Víctor Podberezski.

Batalla de Bailén (obra deAugusto Ferrer Dalmau).

Hay registros que San Martín usaba "tintas invisibles"

Víctor Podberezski
http://inside-the-trash-can.blogspot.com/2019/08/el-papel-de-la-criptografia-en-las.html

36

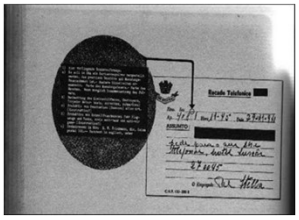
Esteganografía en la Grecia antigua

Heródoto en el siglo V a.C.
El historiador cómo el general ateniense Histieo trataba de animar a su yerno Aristágoras de Mileto para que se rebelara contra el padre de Jerjes, el famoso rey persa.
Para evitar que su mensaje fuera interceptado, Histeio afeitó la cabeza de uno de sus criados y escribío en ella. Y lo envió (obviamente) cuando el pelo le hubo crecido.
Llegado a su destino, el mensajero se rapó para mostrar el recado, logrando así que el complot no fuera descubierto.

37

Esteganografía "Clásica"

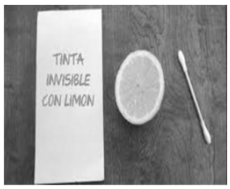
Heródoto en el siglo V a.C. explica como el general Histieo usaba este método para ocultar mensajes.



Agentes alemanes reducían texto a un punto de menos de 1 milímetro de diámetro y lo pegaban a una carta. El FBI descubrió el 1er micropunto en 1941,

Tintas invisibles (jugo de limón, naranja) tintas ultravioletas (discotecas).

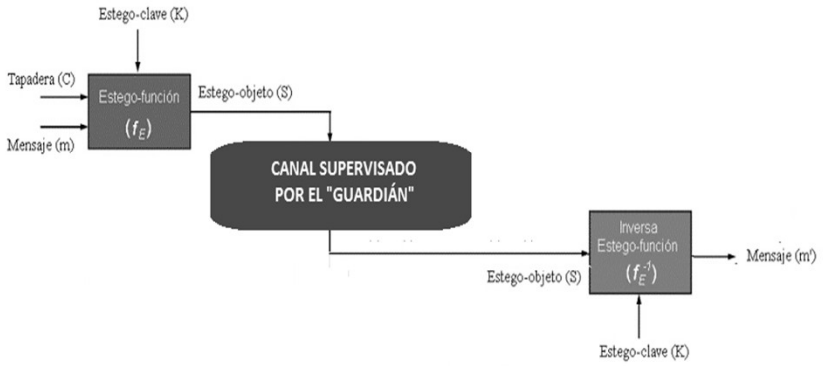
Los griegos escribian en tablillas con cera. Ocultaban mensajes escritos sobre la madera, arriba de las cuales untaban la cera.
En apariencia no portaban ningún mensaje.



https://www.facebook.com/225941097904719/photos/micropuntoforma-de-esteganograf%C3%ADa-que-se-hizo-popular-durante-la-segunda-guerra-/266843043814524/
https://www.sellosdecauchoaxarquia.com/home/TINTA-NORIS-110-UV-INVISIBLE-25ml-p190938240
https://www.pats.cl/detalle-soluciones.php?id=19#prettyPhoto

38

Esquema de Esteganografía



39

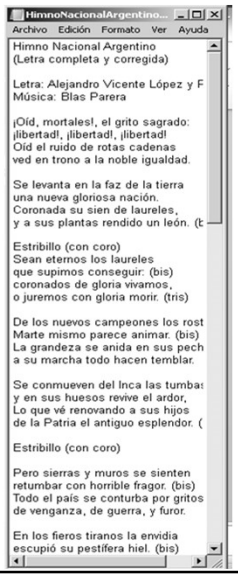
Esteganografía "Moderna"

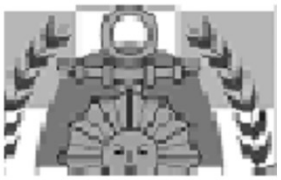
La imagen de la izquierda no contiene mensajes ocultos, la de la derecha contiene los 10 primeros capítulos de la novela Lolita de Nabokov

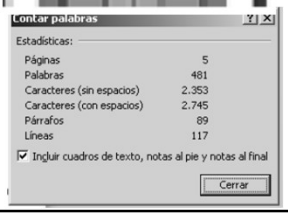
https://www.kaspersky.es/blog/digital-steganography/18791/

40

Esteganografía "Moderna" Aplicada

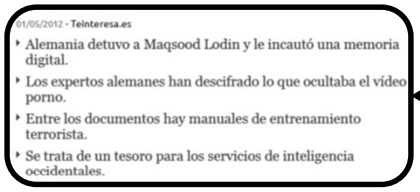






41

Steganografía Contemporánea y terrorismo internacional



42

Preocupación Internacional

https://rsa2018.deep-secure.com

43

Referencias

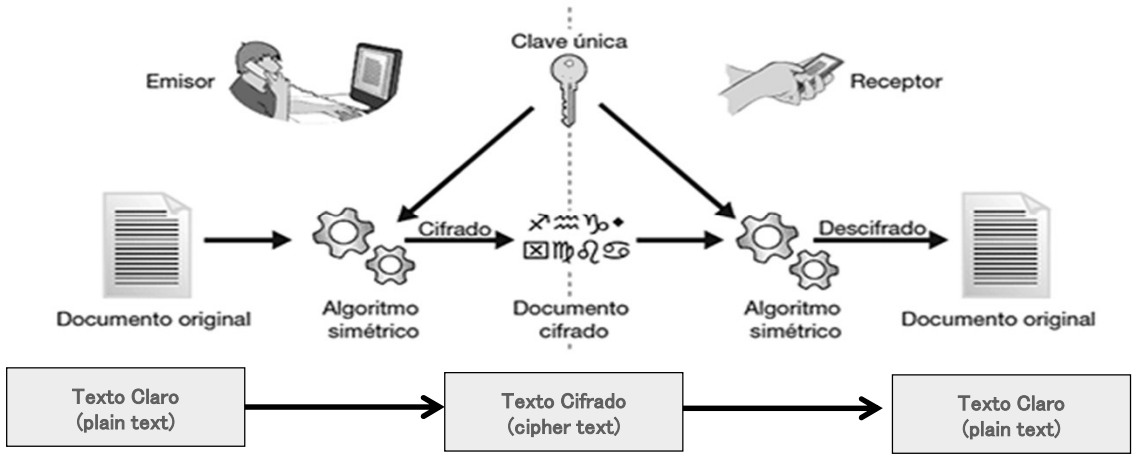
- https://es.planetcalc.com/1434/?license=1
- Víctor Podberezski http://inside-the-trash-can.blogspot.com/2019/08/el-papel-de-la-criptografia-en-las.html
- https://www.facebook.com/225941097904719/photos/micropuntoforma-de-esteganograf%C3%ADa-que-se-hizo-popular-durante-la-segunda-guerra-/266843043814524/
- https://www.sellosdecauchoaxarquia.com/home/TINTA-NORIS-110-UV-INVISIBLE-25ml-p190938240
- https://www.pats.cl/detalle-soluciones.php?id=19#prettyPhoto
- https://www.kaspersky.es/blog/digital-steganography/18791
- https://rsa2018.deep-secure.com

44

Esquema de Cifrado Simétricos

45

Esquema de Cifrado Simétricos



Misma clave para realizar los 2 procesos y en posesión de ambos interlocutores

46

Cifrado Simétrico o Clave Secreta

La importancia de la clave

- La misma clave sirve para cifrar y descifrar (simetría).
- La clave debe permanecer secreta (almacenamiento seguro).
- Habrá tantas claves simétricas como sea la cantidad de emisores y receptores de mensajes (gestión de claves).
- Cuando una clave se debe cambiar, el receptor de los mensajes también debe tenerla (distribución de la clave)

47

Teorías de la Información y la Comunicación Secreta

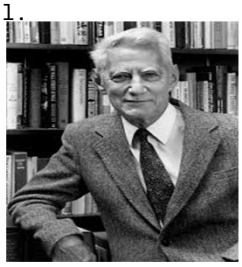
48

Claude Shannon

Claude Elwood Shannon (1916 -2001). Matemático, ingeniero eléctrico y criptógrafo estadounidense «*el padre de la teoría de la información*».

Sentó las bases de la teoría del diseño de circuitos digitales en 1937, con 21 años de edad. Mientras realizaba su maestría en el *Massachusetts Institute of Technology (MIT*), demostró en su tesis que las aplicaciones electrónicas de álgebra booleana podrían construir cualquier relación lógico-numérica.

También contribuyó al campo del criptoanálisis para la defensa de Estados Unidos durante la Segunda Guerra Mundial.



49

Teorías de la Información y la Comunicación Secreta

Claude Shannon (1916-2001)

Reprinted with corrections from *The Bell System Technical Journal*, Vol. 27, pp. 379–423, 623–656, July, October, 1948.

A Mathematical Theory of Communication

By C. E. SHANNON

INTRODUCTION

THE recent development of various methods of modulation such as PCM and PPM which exchange bandwidth for signal-to-noise ratio has intensified the interest in a general theory of communication. A basis for such a theory is contained in the important papers of Nyquist[1] and Hartley[2] on this subject. In the present paper we will extend the theory to include a number of new factors, in particular the effect of noise in the channel, and the savings possible due to the statistical structure of the original message and due to the nature of the final destination of the information.

Communication Theory of Secrecy Systems*

By C. E. SHANNON

1. INTRODUCTION AND SUMMARY

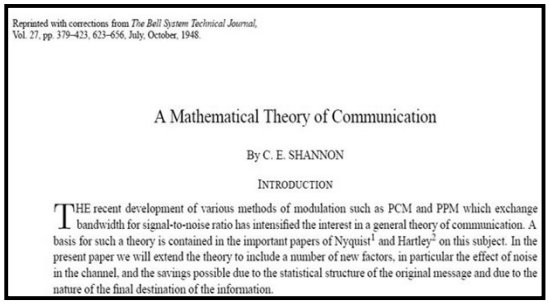
THE problems of cryptography and secrecy systems furnish an interesting application of communication theory.[1] In this paper a theory of secrecy systems is developed. The approach is on a theoretical level and is intended to complement the treatment found in standard works on cryptography.[2] There, a detailed study is made of the many standard types of codes and ciphers, and of the ways of breaking them. We will be more concerned with the general mathematical structure and properties of secrecy systems.

The treatment is limited in certain ways. First, there are three general

Shannon, Claude "A Mathematical Theory of Communication". Bell System Technical Journal, vol. 27 (4), pg. 623–656. 1948.
Shannon, Claude. ""Communication Theory of Secrecy Systems". Bell System Technical Journal, vol. 28 (4), pg.656–715, 1949.

50

Teoría Matemática de la Comunicación



Reprinted with corrections from *The Bell System Technical Journal*,
Vol. 27, pp. 379–423, 623–656, July, October, 1948.

A Mathematical Theory of Communication

By C. E. SHANNON

INTRODUCTION

THE recent development of various methods of modulation such as PCM and PPM which exchange bandwidth for signal-to-noise ratio has intensified the interest in a general theory of communication. A basis for such a theory is contained in the important papers of Nyquist[1] and Hartley[2] on this subject. In the present paper we will extend the theory to include a number of new factors, in particular the effect of noise in the channel, and the savings possible due to the statistical structure of the original message and due to the nature of the final destination of the information.

Conceptos de

- **Información**
- **Entropía**

En 1948 se publica el trabajo fundacional de la Teoría Matemática de la Comunicación.

Trabajos previos y posteriores también se alinearon en esta corriente.

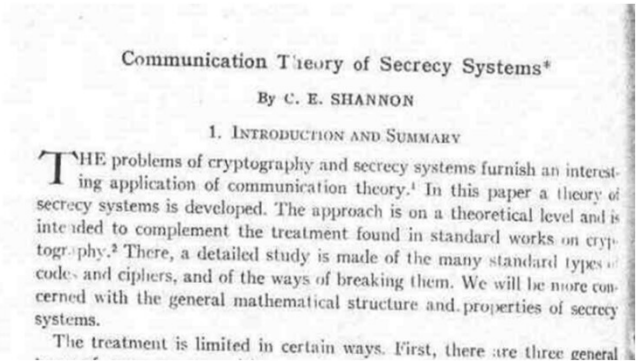
Logró definir los conceptos que hoy son claves en la Sociedad del Conocimiento en la que vivimos, donde las Tecnologías de la Información y la Comunicación han cambiado nuestra forma de ver el mundo.

51

Teoría de la Comunicación de Sistemas Secretos

En 1949 se publica el trabajo fundacional de la Criptología Matemática.

Logró reconocer y definir las reglas que permiten definir los principios con los que se construye la fortaleza de los criptosistemas (secreto perfecto) y las formas de atacarlos: el criptoanálisis.



Communication Theory of Secrecy Systems*

By C. E. SHANNON

1. INTRODUCTION AND SUMMARY

THE problems of cryptography and secrecy systems furnish an interesting application of communication theory.[1] In this paper a theory of secrecy systems is developed. The approach is on a theoretical level and is intended to complement the treatment found in standard works on cryptography.[2] There, a detailed study is made of the many standard types of codes and ciphers, and of the ways of breaking them. We will be more concerned with the general mathematical structure and properties of secrecy systems.

The treatment is limited in certain ways. First, there are three general

Conceptos

- **Confusión**
- **Difusión**

52

STREAM CIPHERS VS BLOCK CIPHERS

Filosofías de Cifrado

Stream Ciphers

Toman cada bit del texto en claro y lo cifran convirtiéndolos en bits del texto cifrado.

Block Ciphers

Toman bloques de bits del texto en claro y los cifran convirtiéndolos en bloques del texto cifrado.

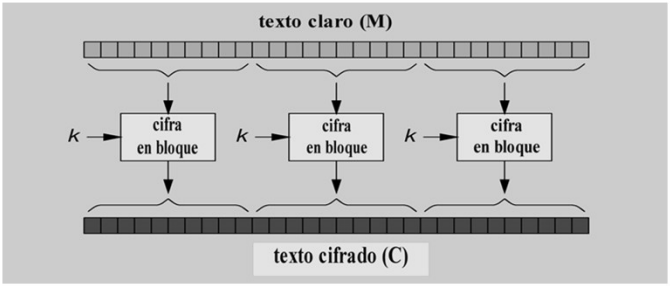
53

Cifrado en Bloque
Block Ciphers

54

Cifrado en Bloque o Block Cipher

El texto claro se fracciona en porciones llamadas "bloques", usualmente de 128 bits de longitud para la mayoría de los algoritmos modernos.

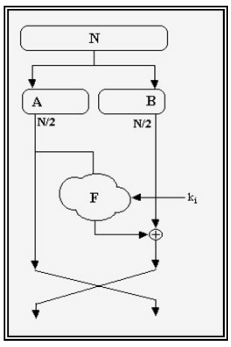


La clave *k* también se ingresa al algoritmo, al igual que cada bloque del texto claro.
La salida del algoritmo, es el bloque correspondiente al texto cifrado.

55

Cifrado tipo Feistel

Horst Feistel: inventor (IBM) del algoritmo LUCIFER a comienzos de los años 70. El algoritmo fue utilizado por el Reino Unido. En 1974 se propone a la NSA como estándar y en ese año dará origen al DES.



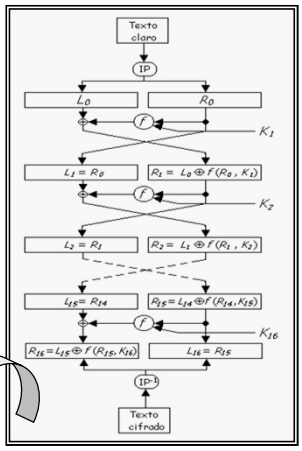
- Dado un bloque de N bits (típico 64) éste se dividirá en dos mitades.
- Existirá una función unidireccional F (muy difícil de invertir).
- Se realizan operaciones con la clave k_i sólo con una mitad del bloque, y se permutan en cada vuelta las dos mitades, operación que se repite durante n vueltas.

http://en.wikipedia.org/wiki/Feistel_network

56

Visión general del DES

- Cifrador de bloque
- Tipo Feistel
- Longitud de clave de 56 bits
- **Realiza 16** vueltas.
- El cifrado del bloque derecho usa técnicas de sustituciones y permutaciones.
- Para poder realizar las sumas or exclusivo, usará permutaciones con expansión y compresión para igualar el número de bits.



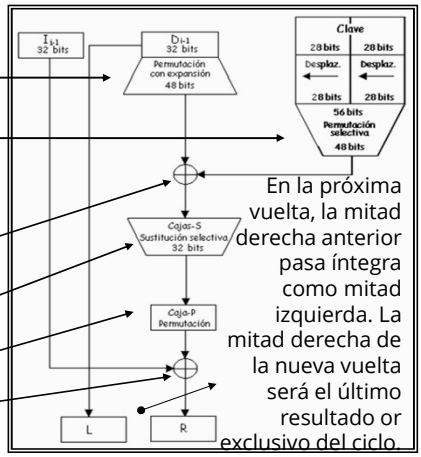
En el descifrado se aplican claves y desplazamientos en sentido inverso

57

Operaciones en cada ciclo del DES

EN CADA CICLO:

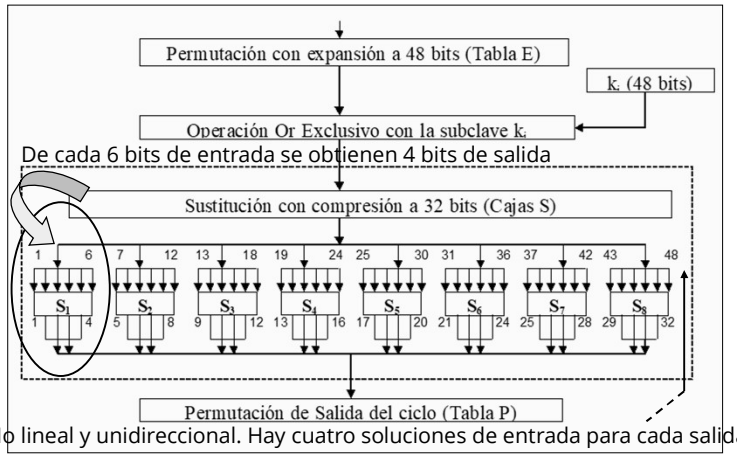
- Se permuta la mitad derecha R_i aplicando expansión a 48 bits
- La clave de 56 bits se desplaza, permuta y se seleccionan los 48 bits de K_i de cada vuelta.
- La nueva mitad derecha R_i y la clave K_i se suman XOR
- Se reducen los 48 bits de salida a 32 bits mediante las Cajas-S
- Se permuta el resultado
- El resultado se suma XOR con la mitad izquierda L_i



En la próxima vuelta, la mitad derecha anterior pasa íntegra como mitad izquierda. La mitad derecha de la nueva vuelta será el último resultado or exclusivo del ciclo.

58

Operación de las cajas S en el DES



De cada 6 bits de entrada se obtienen 4 bits de salida

No lineal y unidireccional. Hay cuatro soluciones de entrada para cada salida

59

R0 = 000000 000001 011111 111100 000101 010100 000100 000000
K1 = 111100 001011 011011 101110 100000 110000 001110 000001

111100 001010 000100 010010 100101 100100 001010 000001

111100 | 001010 | 000100 | 010010 | 100101 | 100100 | 001010 | 000001

10=2 **1110 = 14**

	0 1 2 3	**4 5 6 7**	**8 9 10 11**	**12 13 14 15**
0	14 4 13 1	2 15 11 8	3 10 6 12	5 9 0 7
1	0 15 7 4	14 2 13 1	10 6 12 11	9 5 3 8
2	4 1 14 8	13 6 2 11	15 12 9 7	3 10 5 0
3	15 12 8 2	4 9 1 7	5 11 3 14	10 0 6 13

60

Modos de cifra

Todos los algoritmos pueden usarse aplicando diversos modos de cifra, entre ellos:

- ECB: Electronic CodeBook (libro electrónico de códigos)
- CBC: Cipher Block Chaining (encadenamiento de bloques)
- CFB: Cipher FeedBack (realimentación de bloques)
- OFB: Output FeedBack (realimentación bloque de salida)

Analizaremos cada uno de ellos para el caso del DES, aunque el estudio es extensible a todos los demás ya que en estos modos el cifrador se considera una caja negra.

http://www.itl.nist.gov/fipspubs/fip81.htm

61

ECB

Cifra bloques B de longitud 64 bits

Descifra bloques C de longitud 64 bits

62

Modo de cifra ECB

Recuerde que estos modos son válidos para todos los cifradores en bloque

Electronic CodeBook: cifra cada bloque con la clave k de forma independiente. Por lo tanto, el resultado es como si se codificase mediante un gran libro electrónico de códigos.

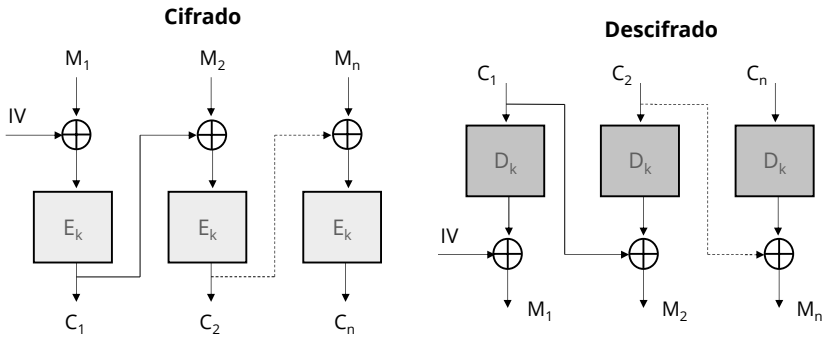
- ☞ Recuerde: codificar no es lo mismo que cifrar.

Debilidades:

- ☹ Se podría reconstruir ese libro electrónico sin necesidad de conocer la clave.
- ☹ Aparece el problema denominado de comienzos y finales fijos que permiten un tipo de ataque sencillo.
- ☹ Se ataca a través de la repetición de bloques similares.

63

Modo de cifra CBC



64

CBC – Cipher Block Chaining Mode

❖**Modo CBC – Cipher Block Chaining Mode**

• Agrega un mecanismo de feedback al algoritmo.

• El resultado del cifrado de un bloque se utiliza en el cifrado del próximo bloque.

• En CBC, al texto plano de un bloque, antes del cifrado, se le realizado un XOR con el texto cifrado del bloque anterior.

•El cifrado de cada bloque depende de TODOS los bloques anteriores.

65

CBC – Cipher Block Chaining Mode

❖**Modo CBC – Cipher Block Chaining Mode**

• DESVENTAJAS:

- **Si al transmitir el texto cifrado, debido a ruido de línea se agregan o pierden bits, el error se propaga a TODOS los bloques.**
- **Un intruso podría agregar bloques al final del texto cifrado.**

• Ventajas:

•En CBC, al texto plano de un bloque, antes del cifrado, se le realizado un XOR con el texto cifrado del bloque anterior.
•El cifrado de cada bloque depende de TODOS los bloques anteriores.

66

Modos de un Algoritmo

❖**Modo OFB – Output FeedBack Mode**

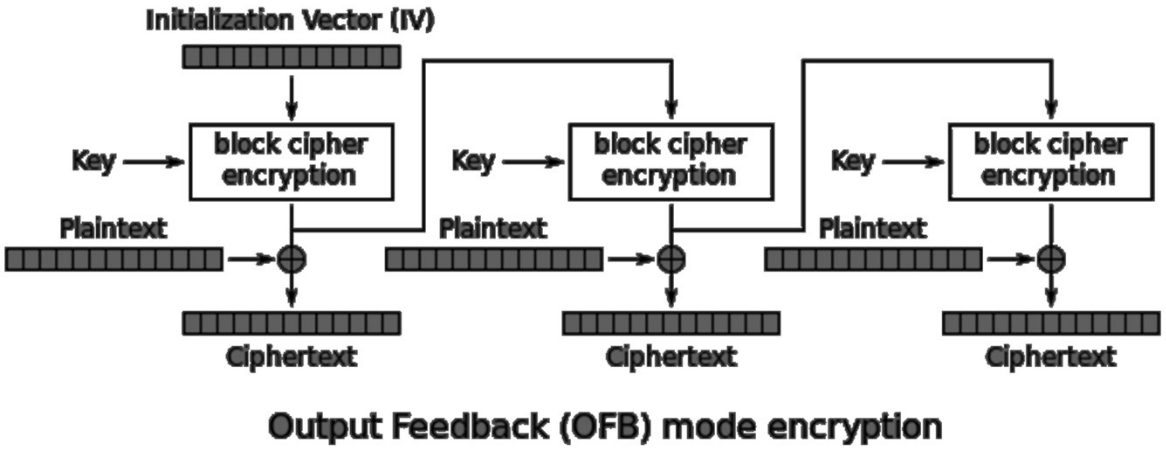
• Consiste en correr un cifrado de bloques como si fuera un *synchronous stream cipher.*

•Es similar al CFB sólo que NO DEPENDE del texto cifrado anterior ni del texto plano.

•Una vez que se genera un I.V. , se puede precomputar el flujo a utilizar ANTES de tener el texto plano. Cuando los bytes del texto plano se obtienen, se les realiza un XOR con este flujo y se transmiten.

67

OFB Cifrado

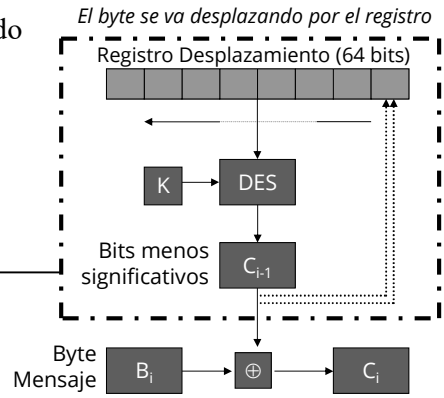


68

Modo de cifra OFB en DES

Output FeedBack: cifrado por realimentación de bloques de salida

La realimentación de la señal se realiza antes de la operación XOR.

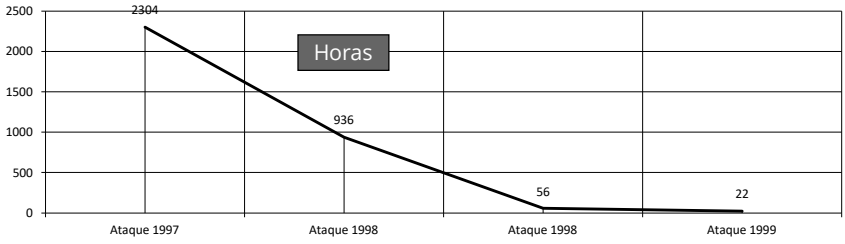


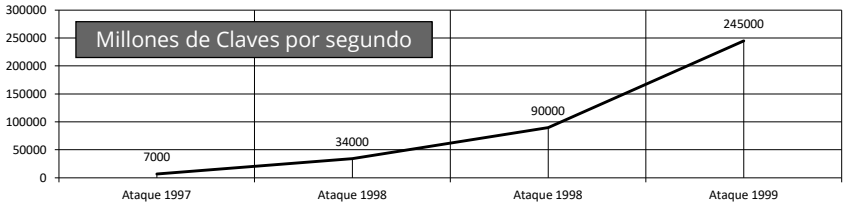
El DES, la clave y el Registro RD actúan como un generador de secuencia cifrante.

Si la cifra se realiza bit a bit, OFB se convierte en cifrador de flujo.

69

DES: Challenge I, II-1, II-2 y III





70

Claves débiles y semidébiles

Claves débiles en hexadecimal:
Una clave es débil si se verifica que: $E_k[E_k(M)] = M$
Además de `0000000000000000` y `FFFFFFFFFFFFFFFF` (que son obvias) serán débiles estas cuatro claves:

```
0101010101010101   FEFEFEFEFEFEFEFE
EOEOEOEOF1F1F1F1   1F1F1F1F0E0E0E0E
```

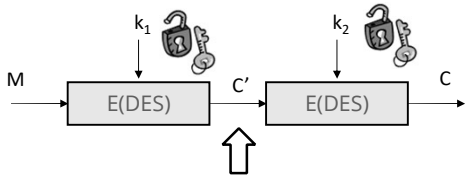
Los bloques C y D de la clave son todos 0s ó 1s.

Claves semidébiles en hexadecimal:
Una clave es semidébil si se verifica que: $E_{k1}[E_{k2}(M)] = M$
Son claves k_1,k_2 semidébiles las siguientes seis parejas:

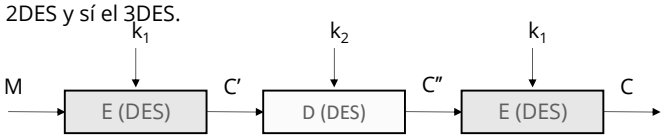
```
(01FE01FE01FE01FE, FE01FE01FE01FE01)
(1FE01FE00EF10EF1, E01FE01FF10EF10E)
(01E001E001F101F1, E001E001F101F101)
(1FFE1FFE0EFE0EFE, FE1FFE1FFE0EFE0E)
(011F011F010E010E, 1F011F010E010E01)
(E0FEE0FEF1FEF1FE, FEE0FEE0FEF1FEF1)
```

Además de éstas, hay otras ecuaciones que verifican dichas claves.

Doble DES y 3DES (1998)



El ataque meet in the middle hace que en un cifrado doble, la fortaleza de de la clave aumente en solo 1 bit. Por ello no existe el 2DES y sí el 3DES.



Modo EDE con Claves k_1-k_2-k_1 un modo compatible con DES simple si $k_1 = k_2$.
Hoy en día si se usa 3DES, se hace con k_1-k_2-k_3 y una fortaleza 56x3 = 168 bits.

AES

73

¿Por qué nace el AES?

En 1997 el NIST ya no certifica al DES.

El 3DES se consideraba seguro pero era muy lento en sus implementaciones en software.

Y llama a concurso público para en nuevo estándar de cifra simétrica: Advanced Encryption Standard.

Características del nuevo algoritmo:

- Longitud de bloque de 128 bits.
- Longitud estándar de clave de 128, 192 y 256 bits.
- Aumento de bloques y claves en incrementos de 32 bits.
- Debería poder utilizarse hasta mitad del siglo XXI.

En octubre de 2000, NIST elige el algoritmo Rijndael de los belgas de Vincent Rijmen y Joan Daemen como estándar para cifrado simétrico del siglo XXI.

74

Características del algoritmo AES

Rijndael: autores Vincent Rijmen & Joan Daemen

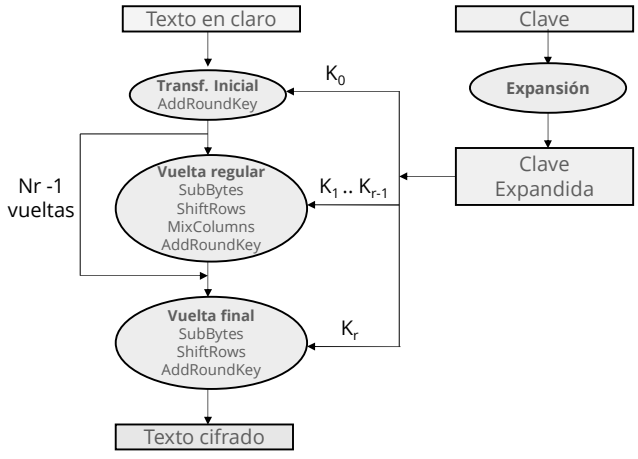
- No es de tipo Feistel.
- Implementado para trabajar en los procesadores de 8 bits usados en tarjetas inteligentes y en CPUs de 32 bits.
- Tamaño de clave variable: 128, 192 y 256 bits (estándar) o bien múltiplo de 4 bytes.
- Tamaño del bloque de texto: 128 bits o múltiplo de 4 bytes.
- Operaciones modulares a nivel de byte (representación en forma de polinomios) y de palabra de 4 bytes: 32 bits.
- Número de etapas flexible según necesidades del usuario.
- Usa un conjunto de Cajas S similares a las del DES.

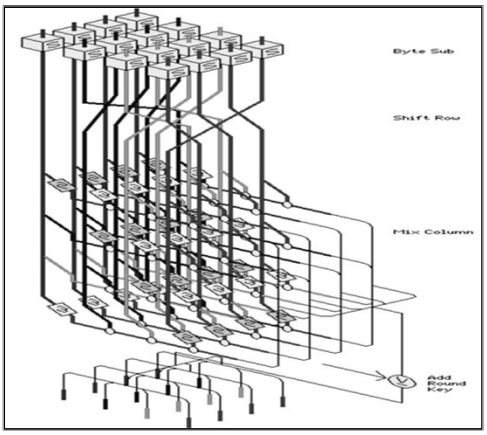
http://www.iaik.tu-graz.ac.at/research/krypto/AES/old/%7Erijmen/rijndael/

https://youtu.be/tzj1RoqRnv0

75

AES (2001) Esquema de cifrado





- Nr = 10 vueltas para clave de 128 bits
- Nr = 12 vueltas para clave de 192 bits
- Nr = 14 vueltas para clave de 256 bits

76

Transformaciones o capas del AES

- Hay tres transformaciones distintas llamadas capas en las que se tratan los bits. Estas constan de:
  - Capa de Mezcla Lineal: en ella se busca la difusión de los bits.
  - Capa No Lineal: se trata de una zona similar a las cajas S del DES.
  - Capa Clave: operaciones con una función or exclusivo de la subclave y la información de esta etapa intermedia.
- Las transformaciones realizadas en cada paso del algoritmo se denominan estados. Estos estados se representa por una matriz de 4 filas y Nb = 4 columnas para el texto en claro y 4 filas y Nk = 4, 6 u 8 columnas para las claves.

En la siguiente página web encontrará una extensa explicación de las operaciones en el algoritmo Rijndael con interesantes ilustraciones.

http://www.quadibloc.com/crypto/co040401.htm

77

AES: matriz de estado

Estado: resultado obtenido en cada uno de los pasos del algoritmo. Los bits se organizan en grupos de 8 bits (1 byte), formando una tabla de 4 filas y 4 columnas (128 bits = 16 bytes).

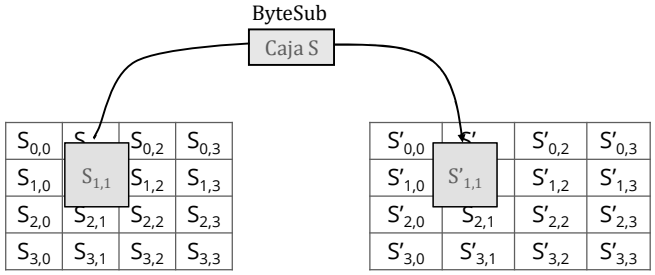
$S_{0,0}$	$S_{0,1}$	$S_{0,2}$	$S_{0,3}$
$S_{1,0}$	$S_{1,1}$	$S_{1,2}$	$S_{1,3}$
$S_{2,0}$	$S_{2,1}$	$S_{2,2}$	$S_{2,3}$
$S_{3,0}$	$S_{3,1}$	$S_{3,2}$	$S_{3,3}$

- Los bytes se almacena y leen por columnas:
  S0,0 - S1,0 - S2,0 - S3,0 - S0,1 - S1,1 - S2,1 - S3,1
  S0,2 - S1,2 - S2,2 - S3,2 - S0,3 - S1,3 - S2,3 - S3,3

78

AES: función ByteSub

Cada uno de los bytes es sustituido a través de una Caja S de 8 x 8, es decir 8 bits de entrada y los mismos 8 bits de salida.



79

AES: ejemplo función ByteSub

Para aplicar la Caja S sobre un byte XY en hexadecimal:

X representa la fila

Y representa la columna

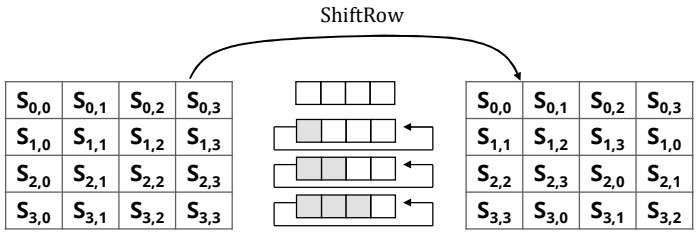
Por ejemplo: ByteSub 5a = be

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

80

AES: función ShiftRow

La fila 0 no desplaza, la fila 1 desplaza un byte, la fila 2 desplaza dos bytes y la fila 3 desplaza tres bytes.



81

AES: función MixColumns

Cada columna i se modifica de la siguiente manera

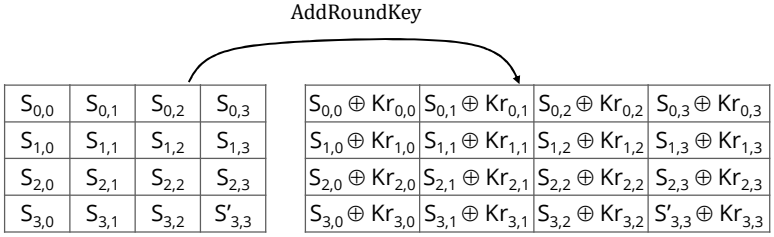
$$\begin{pmatrix} S'_{0,i} \\ S'_{1,i} \\ S'_{2,i} \\ S'_{3,i} \end{pmatrix} = \begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \begin{pmatrix} S_{0,i} \\ S_{1,i} \\ S_{2,i} \\ S_{3,i} \end{pmatrix}$$

- Se trata de operaciones con polinomios (cada byte es considerado como un polinomio de grado 8).
- Cada columna se multiplica módulo $x^4 + 1$ con el polinomio
- $a(x) = \{03\}x^3 + \{01\}x^2 + \{01\}x + \{02\}$
- Donde $\{03\} = x + 1$; $\{02\} = x$; $\{01\} = 1$

82

AES: función AddRoundKey

Se realiza una suma módulo 2 (XOR) del estado con la subclave Kr, que es la última de las subclaves obtenidas a partir de la clave maestra K.



83

AES: expansión de claves

La longitud estándar de la clave es 128, 192, 256 bits.

El algoritmo utiliza un total de Nr + 1 subclaves de 128 bits (16 bytes).

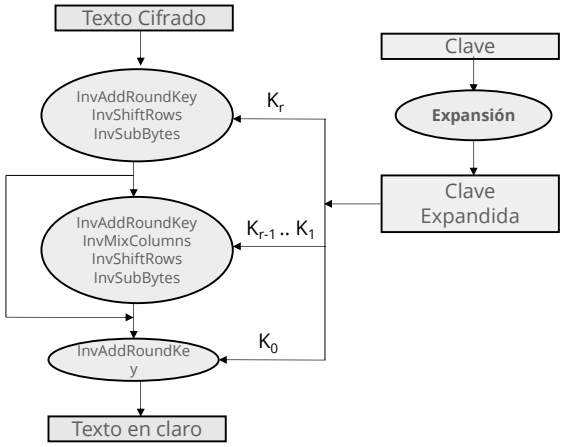
Para ello, AES en primer lugar expande la clave mediante una serie de transformaciones hasta obtener una clave expandida de 16 (Nr + 1) bytes.

A partir de la cual se obtienen las Nr + 1 subclaves.

Clave AES	Subclaves (Nr + 1)	Clave expandida
128 bits	11	1.408 bits (176 bytes)
192 bits	13	1.664 bits (208 bytes)
256 bits	15	1.920 bits (240 bytes)

84

AES: esquema de descifrado



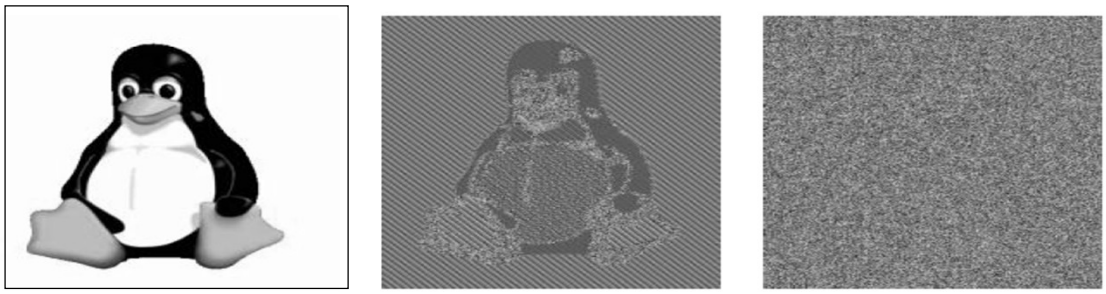
85

AES: tasas de cifra

Algoritmo	Texto claro	Tiempo	MBytes/seg.
Blowfish	256 Mbytes	3,9	64,4
AES 128	256 Mbytes	4,2	61,0
AES 128 CBC	256 Mbytes	4,6	55,4
AES 192	256 Mbytes	4,8	53,1
AES 256	256 Mbytes	5,3	48,2
DES	128 Mbytes	6,0	21,3
3DES EDE	64 Mbytes	6,5	9,8

86

Cifrando “mal” con AES 256

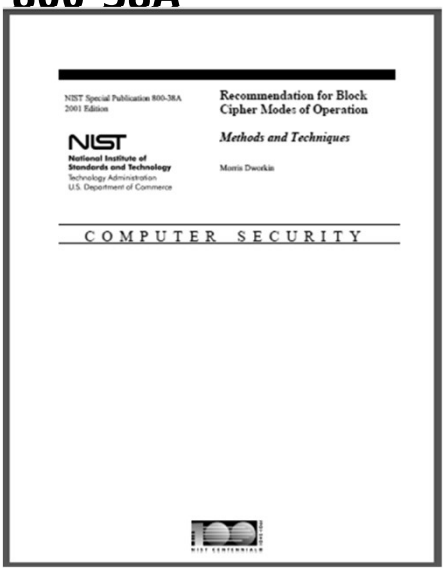


(a) (b) (c)

(a) Imagen original
(b) Cifrado sin encadenar (Electronic Code Book)
(c) Cifrado encadenado (Cipher-Block Chaining)

87

SP800-38A



Los primeros modos de operación, *ECB, CBC, OFB y CFB* se remontan a 1981 y se especificaron en ***FIPS 81*** *“Modos de operación DES”.*

En 2001, el Instituto Nacional de Estándares y Tecnología (NIST) emite el ***SP800-38A*** “*Recomendación para los modos de operación del cifrado en bloque”.. A*ctualizó la lista , ahora para el AES, agregando modos., por ejemplo CTR en.

En 2010, NIST agregó *XTS-AES* en ***SP800-38E*** “*Recomendación para modos de operación de cifrado en bloque: el modo XTS-AES para la confidencialidad en dispositivos de almacenamiento“.*

Existen otros modos de confidencialidad que no han sido aprobados por NIST. Por ejemplo, CTS es un modo de robo de texto cifrado y está disponible en muchas bibliotecas criptográficas populares. Modo de operación de cifrado en bloque

https://es.abcdef.wiki/wiki/Block_cipher_mode_of_operation

88

Laboratorio 1: OpenSSL

Descargar OpenSSL para Windows desde el siguiente link:
http://downloads.sourceforge.net/gnuwin32/openssl-0.9.8h-1-bin.zip

Una vez descargado, abrir el comprimido y extraer los archivos en un directorio.

Abriendo un cmd y posicionándonos en el directorio donde descomprimimos **OpenSSL** debemos ingresar al directorio **bin**

Por ejemplo:

C:\Users\Elliot\Documents\openssl\bin>

Aquí dentro se encontrarán todos los binarios que vienen con la solución.
Particularmente nosotros trabajaremos con el comando **openssl.exe.**

OpenSSL
Cryptography and SSL/TLS Toolkit

Para cifrarlo simétricamente debemos ejecutar:

```
openssl enc -aes-256-cbc -in hola.txt -out hola.enc
```

En este caso le estamos pasando al comando **openssl** los siguientes parámetros:

enc: esto le indica que vamos utilizar un algoritmo para cifrar.

-aes-256-cbc: en este caso le estamos indicando que queremos utilizar AES256 utilizando el modo CBC.

-in hola.txt: le indicamos cuál es nuestro archivo a cifrar.

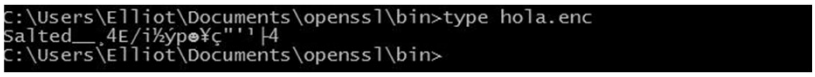
-out hola.enc: le indicamos el archivo dónde queremos que deje los datos cifrados.

Una vez presionado enter nos solicitará la contraseña en dos oportunidades:

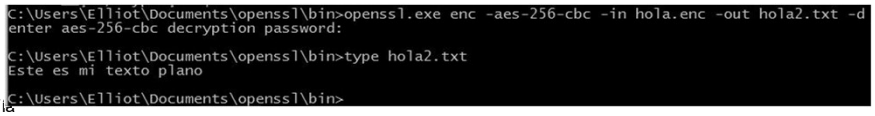

```
C:\Users\Elliot\Documents\openssl\bin>openssl.exe enc -aes-256-cbc -in hola.txt -out hola.enc
enter aes-256-cbc encryption password:
Verifying - enter aes-256-cbc encryption password:

C:\Users\Elliot\Documents\openssl\bin>
```

Con ello ya tenemos nuestro primer archivo cifrado, podemos corroborarlo viendo su contenido.



Para descifrarlo, muy sencillo: ejecutamos el mismo comando pero agregándole el parámetro **-d**, el cual indica que queremos *descifrar.* Obviamente debemos invertir los archivos ya que nuestro input será el archivo cifrado y nuestro output el archivo descifrado. Una vez ejecutado el comando nos solicitará la contraseña que habíamos puesto al momento de cifrar.



Con esto, hemos aprendido a cifrar y descifrar simétricamente utilizando OpenSSL.

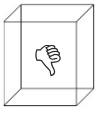
Resumen de los sistemas de clave secreta

Pros y contras de los Sistemas de Clave Secreta

- El emisor y el receptor comparten una misma clave.
- La seguridad depende sólo del secreto de la clave.
- La velocidad de cifra es muy alta y los sistemas con un espacio de clave con cientos de bits son muy seguros.
- Permitirán autenticar los mensajes con MACs.

... pero

- Es imposible establecer un sistema de distribución y gestión de claves eficiente entre emisor y receptor.
- Carecen de una firma digital, al menos en un sentido amplio y sencillo.



¡Gracias!

93