



6669 Criptografía y Seguridad Informática

Elementos de Criptografía



Conceptos iniciales

Acceso a los Sistemas de Información



Para asegurar el acceso a la información, se deben realizar tres pasos fundamentales:

→ Identificación

Indicarle al sistema cuál es la cuenta de usuario a utilizar.

→ Autenticación

Demostrarle al sistema, por ejemplo mediante la introducción de una clave, que el usuario es quien dice ser.

→ Autorización

Probar que el usuario tiene permiso para acceder al recurso.



Acceso a los Sistemas de Información



Para que el sistema autentique a un usuario hay que disponer y exhibir:

- Algo que se conoce
(*Nombre de Usuario y Clave de Acceso*)
- Algo que se posee
(*Por Ejemplo: una tarjeta magnética*)
- Algo que se es, una
característica personal y única
(*Por ejemplo: la huella digital*)

Lo ideal es hacer una combinación de 2 factores





SUD-LAUNCH-DETECTION, DEFENSE ANALYSIS
UNITED STATES OF AMERICA
INIT XPER1 SEQ002-9645

ON DTA PMD: 3215



MATTHEW BRODERICK
AS DAVID LIGHTMAN

ALLY SHEEDY
AS JENNIFER KATHERINE MACK

DABNEY COLEMAN
AS MCOTTERICK

WARGAMES

IS IT A GAME, OR IS IT REAL?



METROPOLITAN

Signalnoise

Skuzzles

WARGAMES TM & © 1983 - 2005 METRO-GOLDWYN-MAYER STUDIOS INC. ALL RIGHTS RESERVED.
POSTED BY JAMES WHITE FOR SKUZZLES, CANADA. WWW.SKUZZLES.COM



Conceptos iniciales

- ¿Cuáles son los factores de autenticación detectados?
- ¿Existe algún mensaje codificado? ¿Cuál?
- ¿Utilizan algún mecanismo de monitoreo y control?





Conceptos iniciales

Autenticación

- Credenciales frente al espejo.
- Código de acceso para la apertura de la puerta.
- Código de candado. Cada uno abre uno.
- Único código de lanzamiento
- Llave de lanzamiento. Cada uno posee una



Conceptos iniciales

Codificación

Pájaro celeste, aquí cuarto menguante.

Con un mensaje rojo-alfa en dos partes.

Pausa.

Pausa.

Rojo-alfa. Rojo-alfa.



Conceptos iniciales

Control y monitoreo

- Registro de acceso
- Cada uno agarra de su lado del primer estante tarjetas y cada uno verifica los códigos escritos con los de las tarjetas





Elementos de Criptografía

Definiciones



Criptografía

Ciencia que hace uso de métodos y herramientas matemáticas con el objetivo principal de cifrar, por lo tanto proteger, un mensaje o archivo por medio de un algoritmo, utilizando para ello una o más claves, con lo que se logra en algunos casos la confidencialidad, en otros la autenticidad, o bien ambas simultáneamente



Codificar vs Cifrar

Codificar es una acción estática en donde un elemento se representará siempre por el mismo elemento. Ejemplos de codificación: ASCII, hexadecimal, base64, entre otros.



Representación

$$E_K(M) = C$$

$$D_K(C) = M$$

E: Función de Cifrado

D: Función de Descifrado

K: Clave

M: Mensaje en texto claro o plano

C: Mensaje cifrado o criptograma



Terminología

Texto plano

Se entiende por texto plano o claro a cualquier información que resulta legible y comprensible por sí misma.

Criptograma

Cuando hablamos de un criptograma nos referimos a un texto que resulta de la cifra de cualquier información que no es legible ni comprensible salvo por el destinatario legítimo de la misma.

Cifrar

Al momento de querer transformar el texto plano en un criptograma estamos cifrando dicho texto plano.



Terminología

Descifrar

Es el proceso que permite transformar el criptograma en texto plano.

Criptología

Se conoce como Criptología a la ciencia que estudia la Criptografía y el Criptoanálisis.

Criptógrafo

El criptógrafo, también conocido como criptólogo es la persona que se dedica al estudio de la criptología.



Tipos de Ataques

Solo texto cifrado

- Se conoce algoritmo

Texto conocido

Texto elegido

Texto cifrado elegido



Más definiciones

Seguridad Incondicional

- No importa cuanta potencia computacional se disponga, el cifrador no se puede romper, ya que, no hay información suficiente para determinar el texto dado el texto cifrado

Seguridad Computacional

- Dado la limitación en los recursos computacionales (Ej. el tiempo necesario para los cálculos es muy grande), el cifrador no puede ser roto en términos prácticos.



SUD-LAUNCH-DETECTION, DEFENSE ANALYSIS
UNITED STATES OF AMERICA
INIT XPER1 SEQ002-9645

ON DTA PMD: 3215



MATTHEW BRODERICK
AS DAVID LIGHTMAN

ALLY SHEEDY
AS JENNIFER KATHERINE MACK

DABNEY COLEMAN
AS MCOTTERICK

WARGAMES

IS IT A GAME, OR IS IT REAL?



METROPOLITAN

Signalnoise

Skuzzles

WARGAMES TM & © 1983 - 2005 METRO-GOLDWYN-MAYER STUDIOS INC. ALL RIGHTS RESERVED.
POSTED BY JAMES WHITE FOR SKUZZLES, CANADA. WWW.SKUZZLES.COM



Fuerza Bruta

Faster supercomputer (as per Wikipedia):

$$10.51 \text{ Petaflops} = 10.51 \times 10^{15} \text{ Flops}$$

No. of Flops required per check: 1000

No. of combination checks per second =

$$(10.51 \times 10^{15}) / 1000 = 10.51 \times 10^{12}$$

No. of seconds in one Year =

$$365 \times 24 \times 60 \times 60 = 31536000$$

Key Size	Possible combinations
1-bit	2
2-bit	4
4-bit	16
8-bit	256
16-bit	65536
32-bit	4.2×10^9
56-bit (DES)	7.2×10^{16}
64-bit	1.8×10^{19}
128-bit (AES)	3.4×10^{38}
192-bit (AES)	6.2×10^{57}
256-bit (AES)	1.1×10^{77}

No. of Years to crack AES with 128-bit Key =

$$(3.4 \times 10^{38}) / [(10.51 \times 10^{12}) \times 31536000]$$

$$= (0.323 \times 10^{26}) / 31536000$$

$$= 1.02 \times 10^{18}$$

Key size	Time to Crack
56-bit	399 seconds
128-bit	1.02×10^{18} years
192-bit	1.872×10^{37} years
256-bit	3.31×10^{56} years



Criptosistemas simétricos y asimétricos

Criptosistemas simétricos:

Existirá una única clave (secreta) que deben compartir emisor y receptor. Con la misma clave se cifra y se descifra por lo que la seguridad reside sólo en mantener dicha clave en secreto.

Criptosistemas asimétricos:

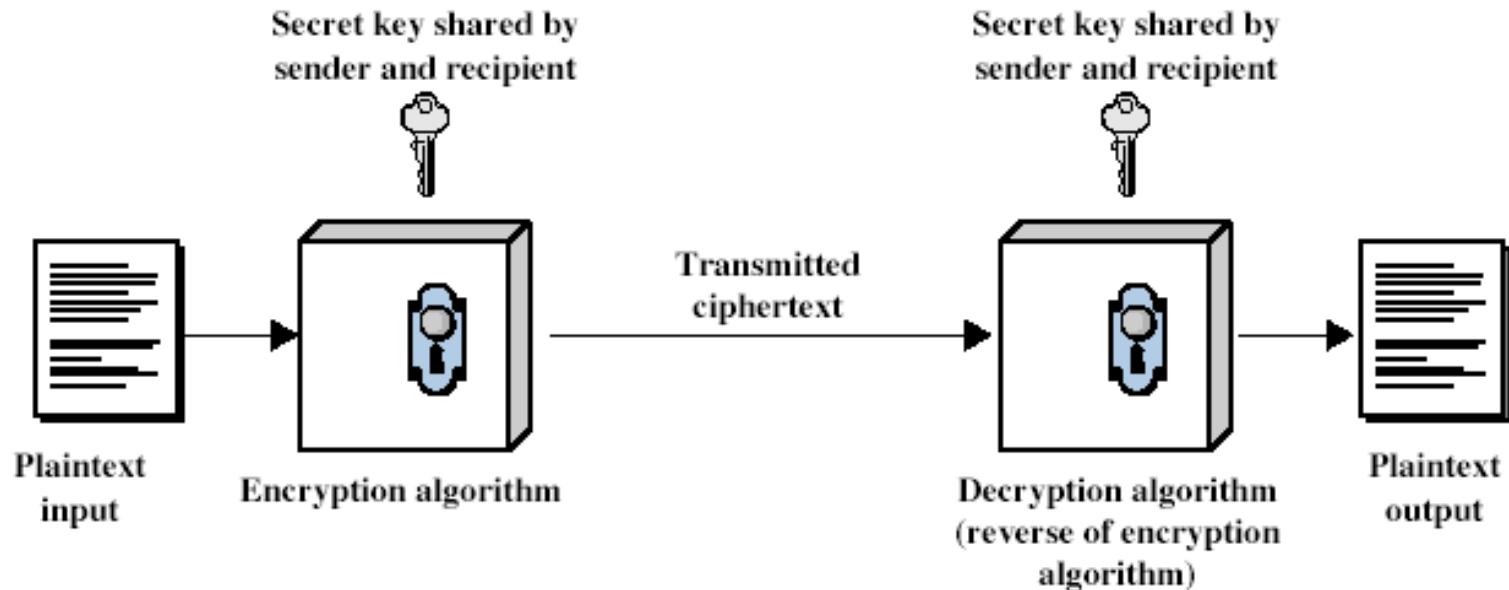
Cada usuario crea un par de claves, una privada y otra pública, inversas dentro de un cuerpo finito. Lo que se cifra en emisión con una clave, se descifra en recepción con la clave inversa. La seguridad del sistema reside en la dificultad computacional de descubrir la clave privada a partir de la pública.



Elementos de Criptografía

Cifradores Simétricos “Clásicos”

Los clásicos son simétricos



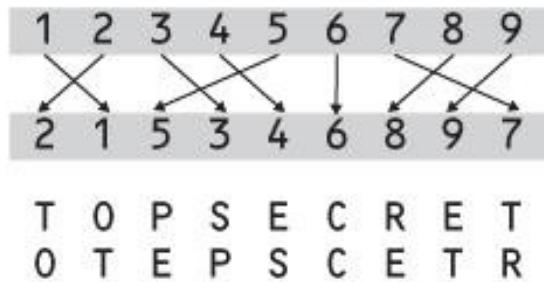


Operaciones



GRAY FOX HAS ARRIVED
UKQN YGB IQL QKKOCTR

Sustitución



Transposición

Escítala





El cifrador del César

En el siglo I a.d.C., Julio César usaba este cifrador.

El algoritmo consiste en el desplazamiento de tres espacios hacia la derecha de los caracteres del texto en claro.

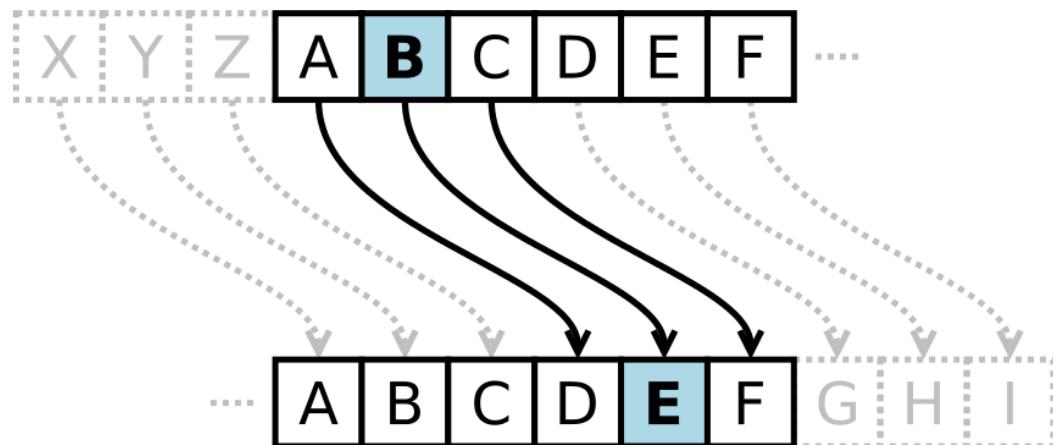
Es un cifrador por sustitución monoalfabético en el que las operaciones se realizan módulo n , siendo n el número de elementos del alfabeto (en aquel entonces el latín).



El cifrador del César

	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	C

Alfabeto de cifrado del César para castellano mod 27





Criptoanálisis del cifrador por sustitución

C: IXHHÑMHİHGHDULDHÑUHVSRPVDEÑH

- Busco los símbolos mas frecuentes: H (8 veces), D (3 veces)
- Pruebo si coinciden con los símbolos mas frecuentes:
 - H → E
 - D → A

M: ...EE..E.E.E.....E..E.....E

M: ...EE..E.E.E.A..AE..E.....A..E

- Continúo, con un poco de prueba y error...

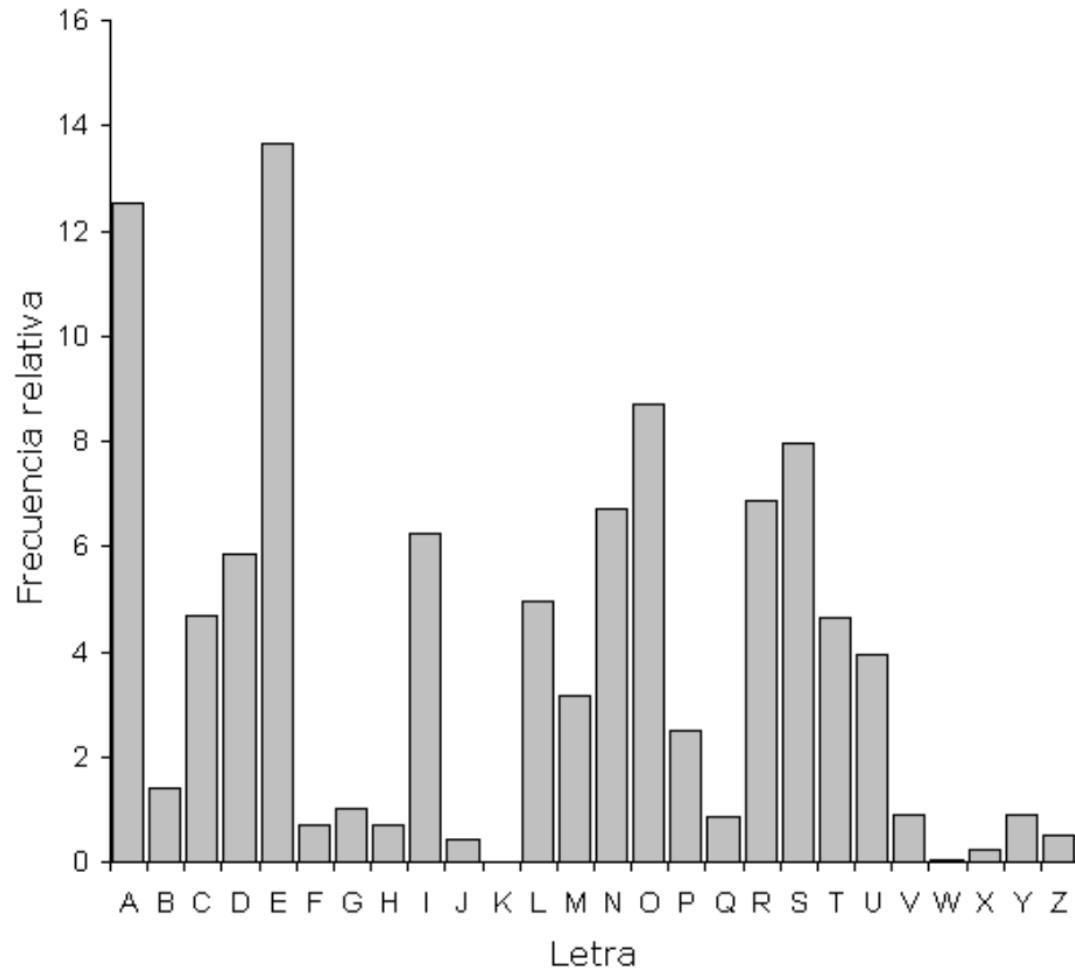
M: FUEELJEFEDEMARIAELRESPONSABLE



Frecuencias de letras

Letra	Porcentaje
A	12,53
B	1,42
C	4,68
D	5,86
E	13,68
F	0,69
G	1,01
H	0,70
I	6,25
J	0,44
K	0,01
L	4,97
M	3,15
N	6,71
O	8,68
P	2,51
Q	0,88
R	6,87
S	7,98
T	4,63
U	3,93
V	0,90
W	0,02
X	0,22
Y	0,90
Z	0,52

Tabla de Frecuencias del Idioma Español

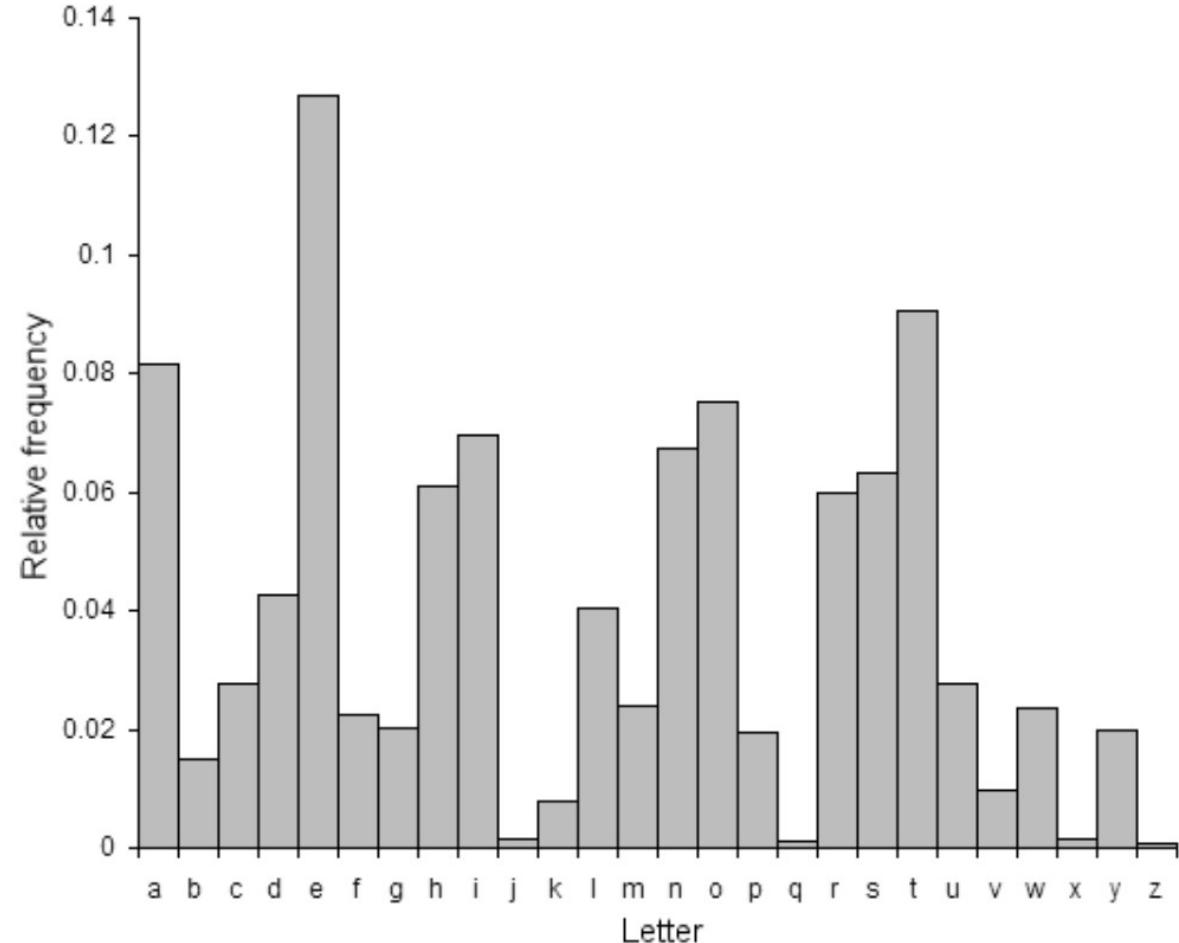




Frecuencias de letras

Letra	Porcentaje
A	8.167
B	1,492
C	2.782
D	4.253
E	12.702
F	2.228
G	2.015
H	6.094
I	6.966
J	0.153
K	0.772
L	4.025
M	2.406
N	6.749
O	7.507
P	1.929
Q	0.095
R	5.987
S	6.327
T	9.056
U	2.758
V	0.978
W	2.360
X	0.150
Y	1.974
Z	0.074

Tabla de Frecuencias del idioma Inglés





Ejercicio criptoanálisis

A partir de la técnica vista, sabiendo que se utiliza el cifrado del Cesar, criptoanalizar el siguiente mensaje con el fin de llegar al texto plano del mismo:

EIMAXLFTGIMMXTGÑGBWIMJILKÑXXMTXMETEXRJLBFXLTNXGZ
TGÑGBIGOXLWTWXLTXGVÑTEKÑBXLNBFJIKÑXMXTJILKÑXMBX
GNLXXEEIMMXJXEXTGEIMWXOILTGEIMWXTYÑXLT



Sustitución por di-gramas



Vigenère

Cifrador polialfabético. Soluciona la debilidad del cifrado del César en que una letra se cifra siempre igual.

Se usa una clave K de longitud L y se cifra carácter a carácter sumando módulo n el texto en claro con los elementos de esta clave.

$$C_i = M_i + K_i \bmod 27$$

↑
Sustitución lineal



Vigenère

$$C_i = M_i + K_i \bmod 27$$

Sea $K' = \text{CIFRA}$ y el mensaje $M = \text{HOLA AMIGOS}$

$M = H O L A A M I G O S$	Periódico: Repite la clave
$K = C I F R A C I F R A$	
$C = J W P R A \tilde{N} P L G S$	

Más de un alfabeto: la letra O se cifra de formas distintas ($O+I = W$, $O+R = G$)

Notar que la P se obtiene de una L y de una I, por corresponder a distinta letra de la clave



Cuadro de Vigenère

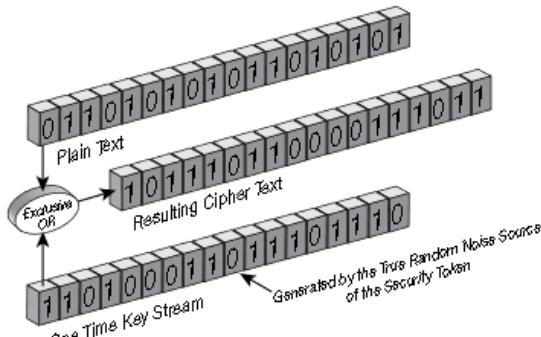
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z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

$$E_D("H") = "K"$$

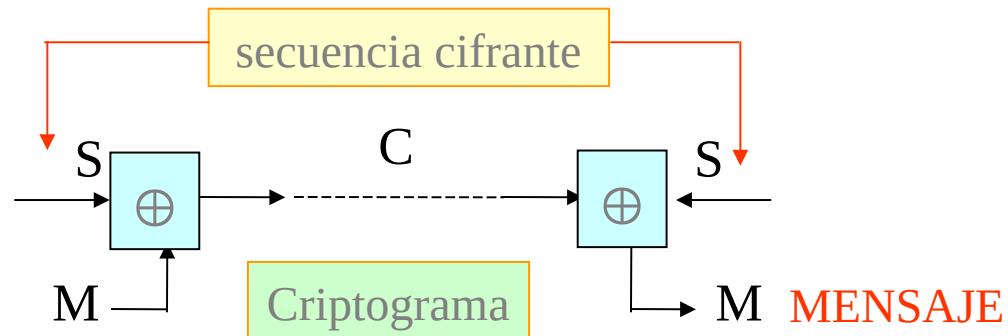
Vernam: One Time Pad

En 1917 Gilbert Vernam propone un cifrador por sustitución binaria con clave de un solo uso (one-time pad) basado en el código Baudot de 5 bits:

- La operación de cifra es la función XOR.
- Usa una secuencia cifrante binaria y aleatoria S
- El algoritmo de descifrado es igual al de cifrado por la involución de la función XOR.
- La clave será tan larga o más que el mensaje y se usará una sola vez.



MENSAJE



Ejemplo de cifrado de Vernam



M = BYTES

K = VERNAM

Solución:

$$B \oplus V = 11001 \oplus 11110 = 00111 = U$$

$$Y \oplus E = 10101 \oplus 00001 = 10100 = H$$

$$T \oplus R = 10000 \oplus 01010 = 11010 = G$$

$$E \oplus N = 00001 \oplus 01100 = 01101 = F$$

$$S \oplus A = 00101 \oplus 00011 = 00110 = I$$

C = UHGFI

El cifrador de Vernam es el único “matemáticamente” seguro y, por tanto, imposible de criptoanalizar pues la clave K se usa una sola vez (one-time pad), es aleatoria y tanto o más larga que el propio mensaje. En este caso, no cabe ningún ataque por estadísticas del lenguaje o por correlación de bits.

http://www.pro-technix.com/information/crypto/pages/vernam_base.html





The 'Sigsaly' system

Since then, One Time Pad systems have been widely used by governments around the world. Outstanding examples of a One Time Pad system include the 'hot line' between the White House and the Kremlin and the famous Sigsaly speech encryption system.

Another development was the paper pad system. Diplomats had long used codes and ciphers for confidentiality. For encryption, words and phrases were converted to groups of numbers and then encrypted by using a One Time Pad.



A 'One Time Pad'



Aleatorio vs Pseudoaleatorio

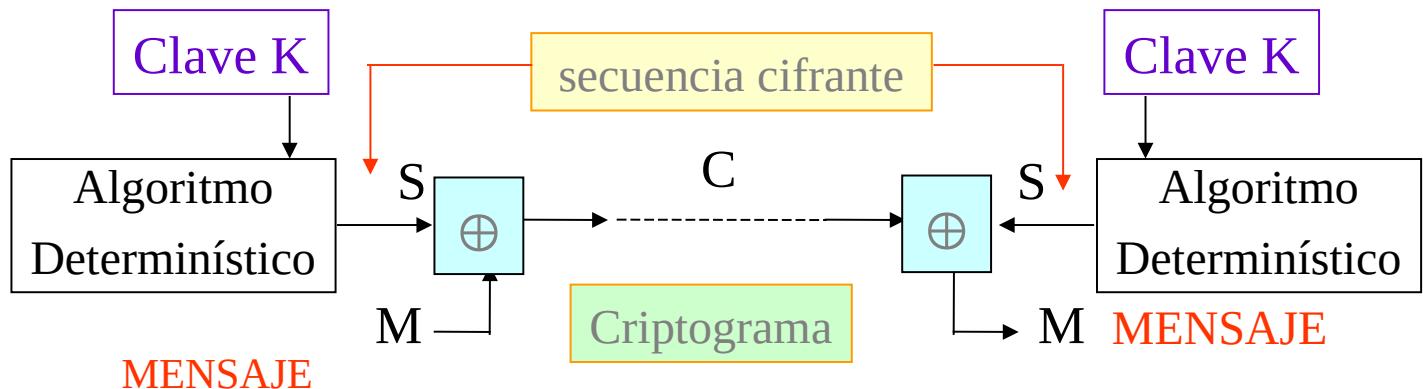
Los verdaderos generadores de números aleatorios (TRNG) usan un medio físico impredecible para generar números (como el ruido atmosférico)

y los generadores de números pseudoaleatorios (PRNG) usan algoritmos matemáticos (completamente generados por computadora).

Vernam: One Time Pad

Implementación con generadores pseudorandom:

- Obtener la secuencia cifrante a partir de una clave secreta K compartida por emisor y receptor.
- La clave será tan larga o más que el mensaje y se usará una sola vez.



no es lo mismo!! Deja de tener seguridad incondicional

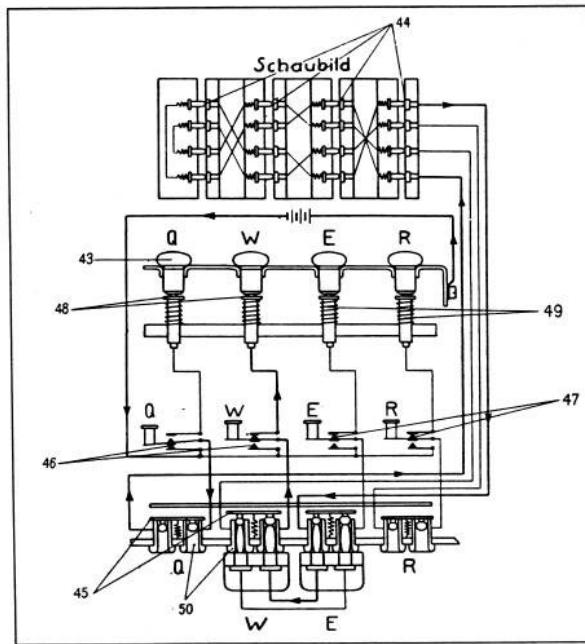
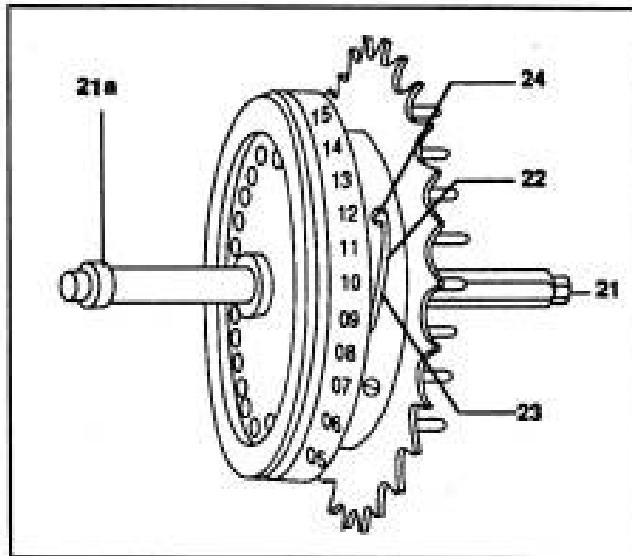


Enigma



Enigma

Máquina electromecánica compuesta por rotores



"BENEDICT CUMBERBATCH IS OUTSTANDING"

RADIO TIMES

"THE BEST BRITISH FILM OF THE YEAR"



THE INDEPENDENT

"AN INSTANT CLASSIC"



GLAMOUR

"A SUPERB THRILLER"



EMPIRE



TIME OUT



THE TIMES

THE IMITATION GAME

BENEDICT
CUMBERBATCH

KEIRA
KNIGHTLEY

12A
MILD
SEX
REFERENCES

BASED ON THE INCREDIBLE TRUE STORY

BLACK BEAR PICTURES PRESENTS IN ASSOCIATION WITH AFRAMONT ENTERTAINMENT & BLACK BEAR PICTURES IN CO-PRODUCTION WITH POSTER AUTOMOTIVE. DIRECTOR: GUY RITCHIE. SCREENPLAY: GUY RITCHIE. PRODUCED BY: GUY RITCHIE. EXECUTIVE PRODUCER: CLAUDIO MARCHETTI. EDITOR: JONATHAN DAVIS. MUSIC: MARK STRONG. CINEMATOGRAPHY: ANDREW HEDDERLEY. PROPS: SAMMY SHELTON. COSTUME DESIGN: MARINA CLOJARU. PROPS: ALEXANDRA DEPLAT. PROPS: WILLIAM SCHNEIDER. PROPS: OSCAR FALBA. PROPS: PETER HESLIP. MUSIC: GRAHAM NOONE.

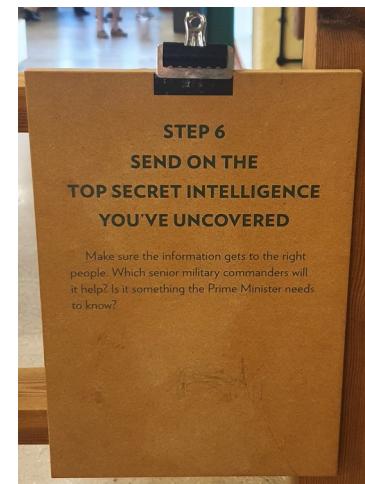
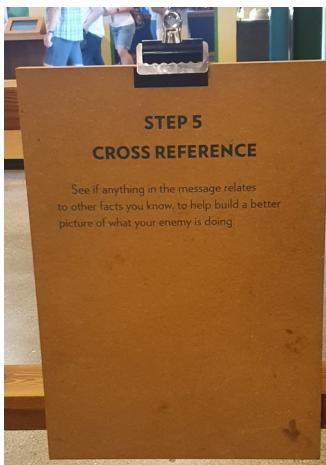
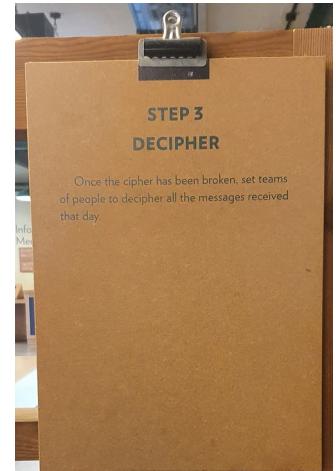
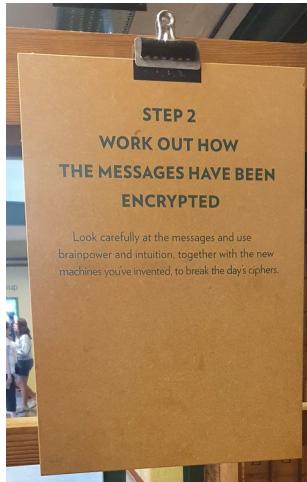
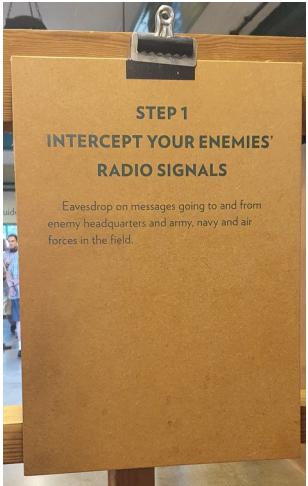
f / ImitationGameUK

IN CINEMAS NOVEMBER 14

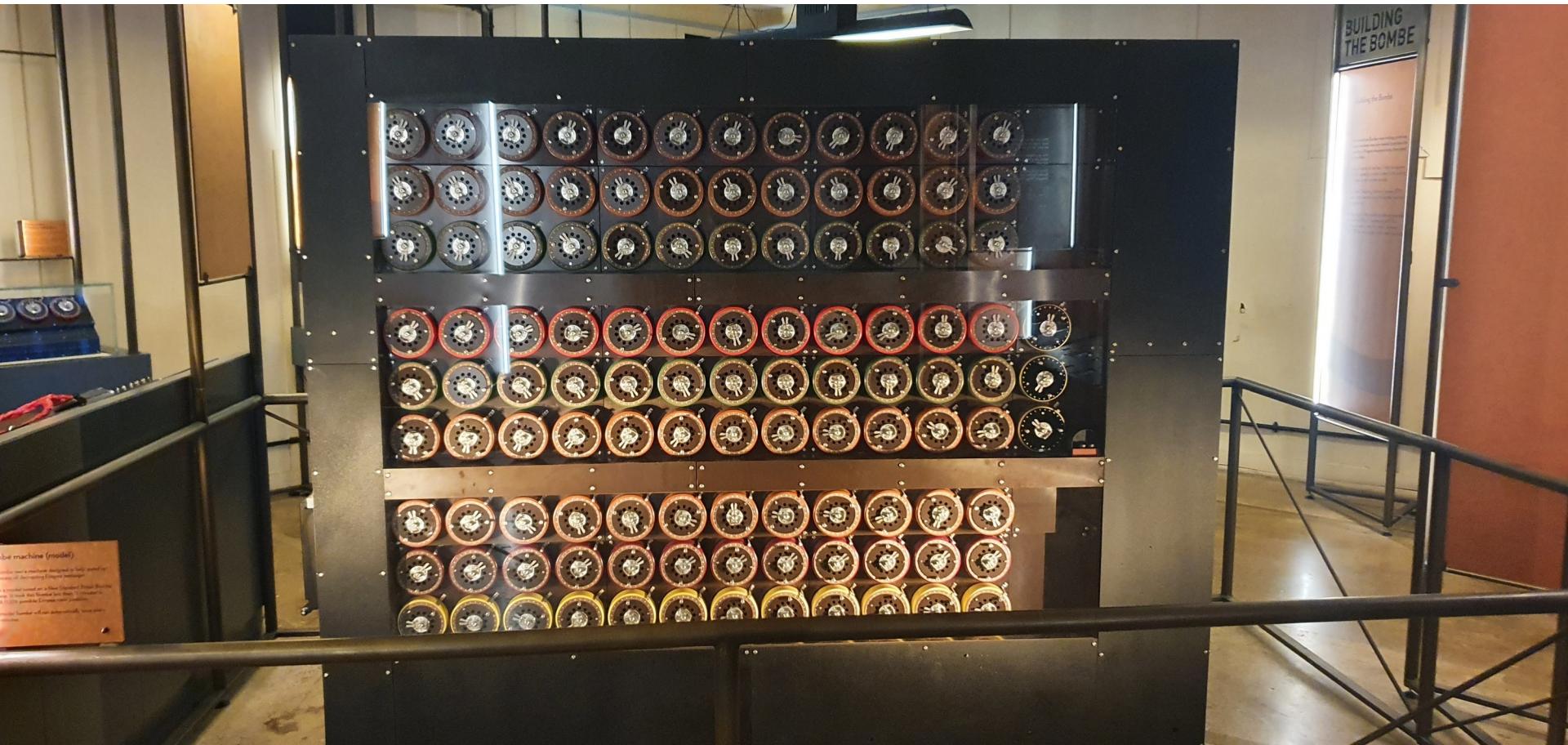




The Codebreaking process



The bombe





Principios de Kerckhoff

1. Si el sistema no es teóricamente irrompible, al menos debe serlo en la práctica.
2. La efectividad del sistema no debe depender de que su diseño permanezca en secreto.
3. La clave debe ser fácilmente memorizable de manera que no haya que recurrir a notas escritas.
4. Los criptogramas deberán dar resultados alfanuméricos.
5. El sistema debe ser operable por una única persona.
6. El sistema debe ser fácil de utilizar.





SUD-LAUNCH-DETECTION, DEFENSE ANALYSIS
UNITED STATES OF AMERICA
INIT XPER1 SEQ002-9645

ON DTA PMD: 3215



MATTHEW BRODERICK
AS DAVID LIGHTMAN

ALLY SHEEDY
AS JENNIFER KATHERINE MACK

DABNEY COLEMAN
AS MCOTTERICK

WARGAMES

IS IT A GAME, OR IS IT REAL?



METROPOLITAN

Signalnoise

Skuzzles

WARGAMES TM & © 1983 - 2005 METRO-GOLDWYN-MAYER STUDIOS INC. ALL RIGHTS RESERVED.
POSTED BY JAMES WHITE FOR SKUZZLES, CANADA. WWW.SKUZZLES.COM

Confusión y Difusión

Shannon propone dos métodos para frustrar ataques estadísticos:

- **Confusión**

Relación compleja entre texto claro y texto cifrado: Sustitución.

- **Difusión**

Disipación de los cambios de manera de “estirar” la estadística:
Permutación.

