

# Criptosistemes Clàssics

Carlos Borrego

Carlos.Borrego@uab.cat

Departament d'Enginyeria de la Informació i de les Comunicacions  
Universitat Autònoma de Barcelona

Criptografia i Seguretat

# Content

1 Clasificación

2 Escítala

3 Polybios

4 Cesar

5 Vigenère

6 Playfair

7 Hill

8 Vernam

9 Enigma

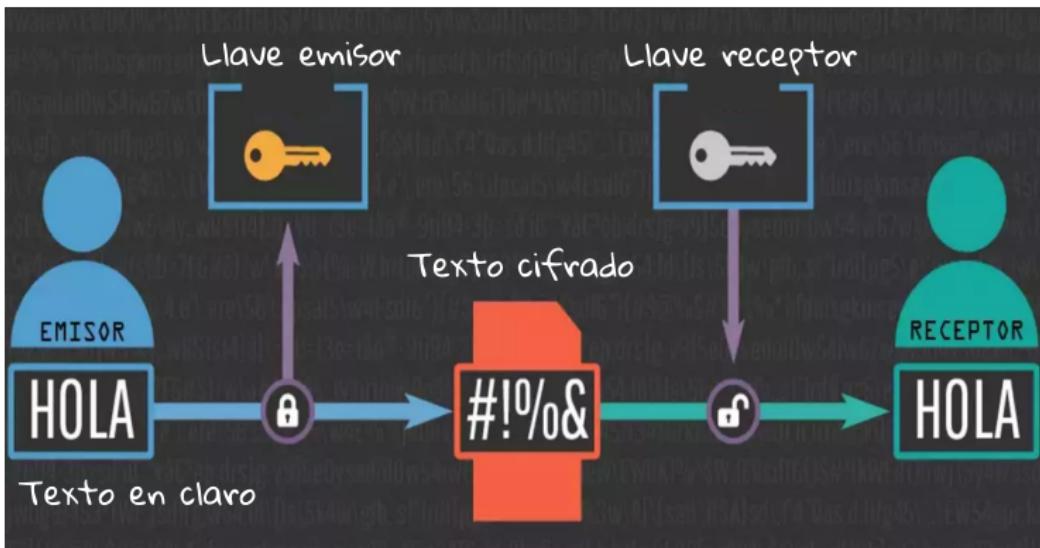
Material adaptat de:

## **Curso de Seguridad Informática y Criptografía**

Dr. Jorge Ramió Aguirre

Universidad Politécnica de Madrid

*<http://jramio.etsisi.upm.es/>*



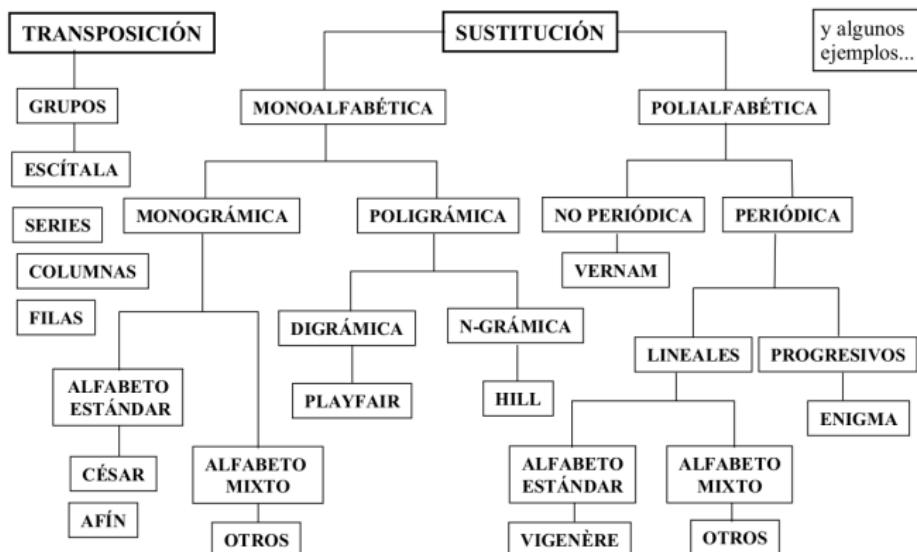
# Confusión y Difusión

- Claude Shannon propuso dos métodos en los algoritmos de cifra para:
  - **Difuminar** la redundancia del lenguaje.
  - Dificultar el **descubrimiento** de la llave utilizada.
- Los dos métodos son:
  - El método de **difusión** pretende difundir las características del texto en claro en todo el texto cifrado ocultando la relación entre el texto en claro y el texto cifrado.
    - El método de **confusión** pretende confundir al atacante que no le sea fácil poder establecer una relación sencilla entre el texto cifrado y la llave empleada

# Herramientas de la criptografía clásica

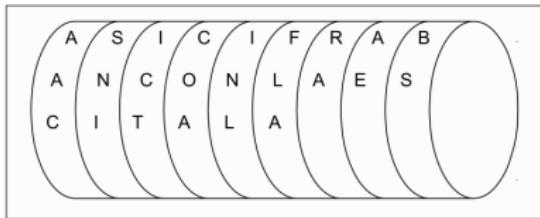
- Tanto máquinas, artilugios de cifra, como los algoritmos que trabajaban matemáticamente dentro de un cuerpo finito  $n$ , hacen uso de dos técnicas básicas orientadas a caracteres y que, muchos siglos después, las propondrá Shannon como herramientas para fortalecer la cifra:
  - Técnicas de sustitución: Los caracteres o letras del mensaje en claro se modifican o sustituyen por otros elementos o letras en la cifra. El criptograma tendrá entonces caracteres distintos a los que tenía el mensaje en claro.
  - Técnicas de transposición o permutación: los caracteres o letras del mensaje en claro se redistribuyen sin modificarlos y según unas reglas, dentro del criptograma. El criptograma tendrá entonces los mismos caracteres del mensaje en claro pero con una distribución o localización diferente.

# Clasificación de los criptosistemas clásicos



# Método de cifra de la escítala

## Bastón y cinta para cifrar



El texto en claro es:

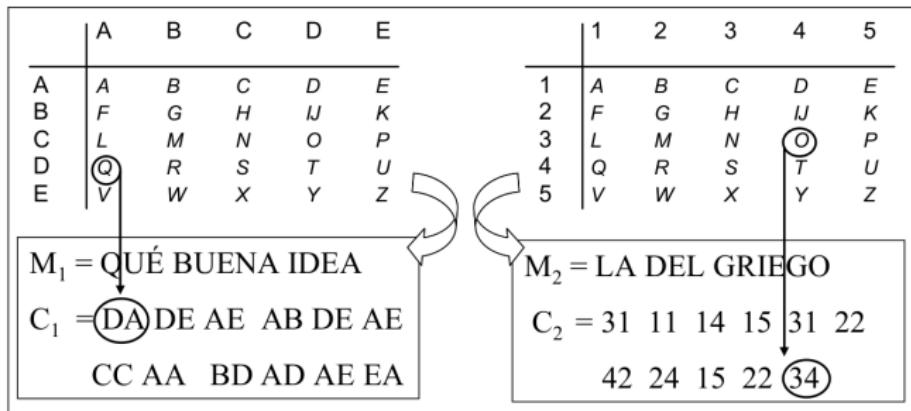
M = ASI CIFRABAN CON LA ESCITALA

El texto cifrado o criptograma será:

C = AAC SNI ICT COA INL FLA RA AE BS

# Primer cifrador por sustitución: Polybios

Es el cifrador por sustitución de caracteres más antiguo que se conoce (siglo II a.d.C.) pero como duplica el tamaño del texto en claro, con letras o números, ... no fue tan buena la idea.



## 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).

	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 <sub>i</sub>	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 <sub>i</sub>	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	

Alfabeto de cifrado del César para castellano mod 27

## Ejemplo de cifra del César en mod 27

M <sub>i</sub>	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 <sub>i</sub>	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

Cifrado:  $C_i = M_i + 3 \text{ mod } 27$

Descifrado:  $M_i = C_i - 3 \text{ mod } 27$

M = EL PATIO DE MI CASA ES PARTICULAR

C = HÑ SDWLR GH OL FDVD HV SDUWLFXÑDU

Cada letra se cifrará siempre igual. Es una gran debilidad y hace que este sistema sea muy vulnerable y fácil de atacar, simplemente usando las estadísticas del lenguaje. Puede ver la tabla de frecuencias típicas del lenguaje castellano en el capítulo 21 de este libro.

# Criptoanálisis del cifrador por sustitución

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
00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

$$\text{Cifrado: } C_i = (M_i + b) \bmod 27 \quad \text{Descifrado: } M_i = (C_i - b) \bmod 27$$

La letra más frecuente del criptograma la hacemos coincidir con la más frecuente del lenguaje, la letra E, y encontramos así b.

C = LZAHL ZBTHW YBLIH XBLKL ILYOH ZLYCH ROKH

Frecuencias observadas en el criptograma: L (7); H (6); Z (3); B (3); Y (3); I (2); K (2); O (2); A (1); T (1); W (1); X (1); C (1); R (1).

Es posible que la letra E del lenguaje se cifre como L. Comprobamos además si la letra A (segunda más frecuente) se cifra como H:

$$E + b \bmod 27 = L \Rightarrow b = L - E \bmod 27 = 11 - 4 \bmod 27 = 7 \quad \text{👉}$$

$$A + b \bmod 27 = H \Rightarrow b = H - A \bmod 27 = 7 - 0 \bmod 27 = 7 \quad \text{👉}$$

M = ESTA ES UNA PRUEBA QUE DEBERIA SER VALIDA

## Cifrador por sustitución afín mod 27

Cifrado:  $C_i = a \cdot M_i + b \pmod{27}$

Descifrado:  $M_i = (C_i - b) * a^{-1} \pmod{27}$  donde  $a^{-1} = \text{inv}(a, 27)$

- El factor de multiplicación  $a$  deberá ser primo relativo con el cuerpo  $n$  (en este caso 27) para que exista el inverso  $a^{-1}$ .
- El factor de desplazamiento puede ser cualquiera:  $0 \leq b \leq 26$ .

El ataque a este sistema es también muy elemental. Se relaciona el elemento más frecuente del criptograma a la letra E y el segundo a la letra A, planteando un sistema de 2 ecuaciones. Si el texto tiene varias decenas de caracteres este ataque prospera; caso contrario, podría haber ligeros cambios en esta distribución de frecuencias.

# Criptoanálisis a la cifra afín mod 27

C: NAQÑF EKNDP NCIVU FPUAN EJUIP FCNER NFRÑF UNPLN  
 AFPFQ TFPEI JRTÑE FPKÑI KTAPF LIKIÑ AIPÑU RCUJI  
 PCIVU CUNER IRLNP TJIAF NEOIÑ CFLNC NLUFA TEF

Caracteres más frecuentes en el criptograma: F = 14; N = 13; I = 12

Con E y A las más frecuentes, el ataque falla. En un segundo intento suponemos la letra A más frecuente que la E, luego:

$$F = (a*A + b) \text{ mod } 27 \Rightarrow (a*0 + b) \text{ mod } 27 = 5 \Rightarrow b = 5$$

$$N = (a*E + b) \text{ mod } 27 \Rightarrow (a*4 + 5) \text{ mod } 27 = 13$$

$$\text{Entonces } a = (13-5) * \text{inv}(4, 27) \text{ mod } 27 = 8 * 7 \text{ mod } 27 = 2$$

$$C_i = (2*M_i + 5) \text{ mod } 27 \Rightarrow M_i = (C_i - 5) * \text{inv}(2, 27) = (C_i - 5) * 14 \text{ mod } 27$$

M: EL GRAN PEZ SE MOVÍA SILENCIOSAMENTE A TRAVÉS DE LAS AGUAS NOCTURNAS, PROPULSADO POR LOS RÍTMICOS MOVIMIENTOS DE SU COLA EN FORMA DE MEDIA LUNA.

(Comienzo de la novela Tiburón de Peter Benchley)

## El cifrador de Vigenère

Este 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.

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

Sea K = CIFRA y el mensaje M = HOLA AMIGOS

M =	H	O	L	A	A	M	I	G	O	S	
K =	C	I	F	R	A	C	I	F	R	A	sumando mod 27...
C =	J	W	P	R	A	Ñ	P	L	G	S	Más de un alfabeto: la letra O se cifra de forma distinta.

Observe que el criptograma P se obtiene de un texto L y de un texto I.

# Cadenas repetidas en ataque de Kasiski

Sea el criptograma C de 404 caracteres que vamos a criptoanalizar el siguiente:

PBVRO VICAD SKAÑS DETSJ PSIED BGGMP SLRPW RÑPWY EDSDE ÑDRDP CRCPQ MNPWK  
UBZVS FNVRD MTIPW UEQVV CBOVN UEDIF QLONM WNUVR SEIKA ZYEAC EYEDS ETFPH  
LBHGU ÑESOM EHLBX VAEEP UÑELI SEVEF WHUNM CLPQP MBRRN BPVIÑ MTIBV VEÑID  
ANSJA MTJOK MDODS ELPWI UFOZM QMVNF OHASE SRJWR SFQCO TWVMB JGRPW VSUEX  
INQRS JEUEM GGRBD GNNIL AGSJI DSVSU EEINT GRUEE TFGGM PORDF OGTSs TOSEQ  
ÖNTGR RYVLP WJIFW XOTGG RPQRR JSKET XRNBL ZETGG NEMUO TXJAT ORVJH RSFHV  
NUEJI BCHAS EHEUE UOTIE FFGYA TGGMP IKTBW UEÑEN IEEU.

Entre otras, se observan las siguientes cadenas (subrayadas) en el criptograma:

- 3 cadenas GGMP, separadas por 256 y 104 posiciones.
- 2 cadenas YEDS, separadas por 72 espacios.
- 2 cadenas HASE, separadas por 156 espacios.
- 2 cadenas VSUE, separadas por 32 espacios.

Luego el período de la clave puede ser med (256, 104, 72, 156, 32) = 4. La clave tendrá cuatro caracteres, por lo tanto tomaremos del criptograma el carácter 1º, el 5º, el 9º, etc. para formar el primer subscriptograma  $C_A$ ; luego el 2º, el 6º, el 10º, etc. para formar el subscriptograma  $C_B$ , y lo mismo para subscriptogramas  $C_C$  y  $C_D$ .

# Paso a cifrado monoalfabético en Kasiski

Tenemos ahora 4 subscriptogramas de sólo 101 letras c/u (muy importante tenerlo en cuenta en las estadísticas) que han sido cifrados con la misma letra de la clave:

$$\begin{aligned}
 C_A &= PQAAEPDMR\tilde{N}EEDCNUSRIECNIONSAETLUOLAUIEULMNIIEAAOOLU \\
 &\quad MNARSOQRSISERNNAISIRTMDOORLIORRENENOAVSNIAEOFAMTEI \\
 C_B &= BVD\tilde{N}TSBPPPD\tilde{N}PPPBFDPQBUFNUEZCDFB\tilde{N}MBE\tilde{N}SFNPEB\tilde{N}B\tilde{N}NMKDPF \\
 &\quad QFSJFTBPUJMNBNGDUNUFPFSS\tilde{N}RPFPTJTBETTJFUBSUTFTPB\tilde{N}E \\
 C_C &= VISSSIIGSWWSDCQWZNMWVQEQMVIYESPHEEEXEEWMQRPMVISTMSWO \\
 &\quad MOEWQWJWEQEGDISETEGOOSETYWWGQSXLGMXOHHECEEIGGIWEE \\
 C_D &= RCKDJEGLRYDRRMKVVTUVVDLWRKEYEHGSHVPLVHCPRTVDJJDEIZ \\
 &\quad VHSRCVGXRUGGLJVEGEGRGTQGVJXGRKRZGUJRRVJHHUEYGKUNU
 \end{aligned}$$

La frecuencia relativa observada en cada uno de los subscriptogramas es:

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	\tilde{N}	O	P	Q	R	S	T	U	V	W	X	Y	Z
$C_A$	12	0	2	3	12	1	0	0	11	0	0	5	6	9	1	10	2	1	9	7	4	5	1	0	0	0	0
$C_B$	0	14	1	6	4	12	1	0	0	4	1	0	3	6	8	0	14	2	1	6	9	7	1	0	0	0	1
$C_C$	0	0	2	2	18	0	7	3	7	1	0	1	7	1	0	6	2	6	1	12	3	0	4	12	3	2	1
$C_D$	0	0	3	5	7	0	12	6	1	7	5	4	1	1	0	0	2	1	13	2	3	6	14	1	2	3	2

Luego, la letra más frecuente del subscriptograma debería corresponder a la letra E del texto en claro, la segunda a la letra A y la tercera a la letra O. →

## La regla AEO en el ataque de Kasiski

- Si la posición relativa de la letra A es el valor 0, entonces la letra E está cuatro espacios a la derecha de la A ( $m+4 \bmod 27$ ) y la letra O está 15 espacios a la derecha de la letra A ( $m+15 \bmod 27$ ) y a 11 de la letra E.
- Buscaremos en cada subscriptograma  $C_i$  las tres letras más frecuentes y que cumplan además con esa distribución:  $0 \rightarrow +4 \rightarrow +11 \bmod 27$ .
- Es suficiente contar con estas tres letras para que el ataque prospere. No obstante, podemos afinar un poco más el ataque si tomamos en cuenta la siguiente letra frecuente en castellano S, en la posición ( $m+19 \bmod 27$ ).

En el ejemplo para  $C_A$  se observa que la única solución que cumple con esto es la que coincide la AEO (12, 12, 10) luego la letra clave sería la A. Para  $C_B$  elegimos BFP (14, 12, 14) por lo que la letra clave sería B. Para  $C_C$  elegimos EIS (18, 7, 12) por lo que la letra clave sería E. Para  $C_D$  elegimos RVG (13, 14, 12) por lo que la letra clave sería R.

Con la clave K = ABER obtenemos “Para que la cosa no me sorprenda...”. Al ser éste un texto largo y con sentido, hemos encontrado la clave  (artículo del periodista Andrés Aberasturi sobre la Navidad, España, año 1995)

## El índice de coincidencia IC

El estudio del índice IC queda fuera del contexto de estos apuntes. Si bien tiene relación con el número de alfabetos, no es efectivo como Kasiski.

$$IC = \sum_{i=0}^{26} p_i^2 \quad \text{para castellano mod 27: } IC = p_A^2 + p_B^2 + \dots + p_Z^2 = 0,072$$

Si el IC es menor que 0,5 es muy probable que no se trate de un cifrador monoalfabético sino polialfabético con un periodo 2 o mayor.

Así, cuando encontramos una longitud L de la clave por el método de Kasiski y rompemos el criptograma en L subscriptogramas, aplicando el concepto del índice de coincidencia IC podemos comprobar que cada uno de ellos se trata efectivamente de un cifrado monoalfabético cuando para cada subscriptograma este valor se acerca a 0,072 o lo supera.

En el ejemplo anterior, una vez roto el criptograma en cuatro tenemos:  
 $IC_{CA} = 0,080$ ;  $IC_{CB} = 0,091$ ;  $IC_{CC} = 0,083$ ;  $IC_{CD} = 0,082$  ... perfecto ☺

## Cifrador poligrámico de Playfair

Los cifrados anteriores se hacían carácter a carácter, es decir eran monográmicos. Para aumentar la seguridad de la cifra y romper las estadísticas, podemos cifrar por poligramas, bloques de caracteres. Un cifrador inventado a finales del siglo XIX es el de Playfair que trabaja con una matriz de 5x5 letras, cifrando por digramas. Si el texto en claro tiene un número impar de elementos, se rellena con una letra preestablecida, por ejemplo la letra X.

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

- Si  $M_1M_2$  están en la misma fila,  $C_1C_2$  son los dos caracteres de la derecha.
- Si  $M_1M_2$  están en la misma columna,  $C_1C_2$  son los dos caracteres de abajo.
- Si  $M_1M_2$  están en filas y columnas distintas,  $C_1C_2$  son los dos caracteres de la diagonal, desde la fila de  $M_1$ .

## Ejemplo de cifra con Playfair

Si la clave K = BEATLES y eliminamos la letra Ñ (inglés), cifre el mensaje M = WITH A LITTLE HELP FROM MY FRIENDS.



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

Se rompe la doble  
MM agregando una  
X y se rellena al  
final también con X

M = WI TH AL IT TL EH EL PF RO MX MY FR IE ND SX  
C = EP BM TB ME LB BI AB RC UP KY RT MY PC KG DV

Estos sistemas también son criptoanalizables pues en el criptograma C persisten algunas propiedades del lenguaje; en este caso la distribución de digramas típicos; por ejemplo en el castellano en, de, mb, etc.

# El cifrador de matrices de Hill

En 1929 el matemático Lester Hill propone un sistema de cifra usando una matriz como clave, cifrando Ngramas de forma que:

$$\begin{pmatrix} C_1 \\ C_2 \\ C_3 \\ \dots \\ C_N \end{pmatrix} = \begin{pmatrix} k_{11} & k_{12} & k_{13} & \dots & k_{1N} \\ k_{21} & k_{22} & k_{23} & \dots & k_{2N} \\ k_{31} & k_{32} & k_{33} & \dots & k_{3N} \\ \dots & \dots & \dots & \dots & \dots \\ k_{N1} & k_{N2} & k_{N3} & \dots & k_{NN} \end{pmatrix} X \begin{pmatrix} M_1 \\ M_2 \\ M_3 \\ \dots \\ M_N \end{pmatrix} \text{ mod } n$$

La matriz clave K debe tener inversa  $K^{-1}$  en el cuerpo de cifra n.

Luego, como  $K^{-1} = T_{\text{ADJ}(K)}/|K| \text{ mod } n$ , en donde  $\text{ADJ}(K)$  es la matriz adjunta, T es la traspuesta y |K| el determinante, este último valor |K| no podrá ser cero ni tener factores en común con n puesto que está en el denominador (concepto de inverso ya visto).

Si el texto en claro no es múltiplo del bloque N, se rellena con caracteres predeterminados, por ejemplo la letra X o la Z.

## Ejemplo de cifrado de Hill

Sea  $M = \text{AMIGO CONDUCTOR}$  y la clave  $K$  la que se muestra:

$$\begin{pmatrix} C_1 \\ C_2 \\ C_3 \end{pmatrix} = \begin{pmatrix} 16 & 4 & 11 \\ 8 & 6 & 18 \\ 15 & 19 & 15 \end{pmatrix} \times \begin{pmatrix} 0 \\ 12 \\ 8 \end{pmatrix} \pmod{27}$$

$K = \text{PELIGROSO}$  será la clave simbólica. Se cifrará el primer trígrama:  $\text{AMI} = 0, 12, 8$ .

$M = \text{AMI GOC OND UCT ORZ}$

$$C_1 = (16*0 + 4*12 + 11*8) \pmod{27} = 136 \pmod{27} = 1 = \text{B}$$

$$C_2 = (8*0 + 6*12 + 18*8) \pmod{27} = 216 \pmod{27} = 0 = \text{A}$$

$$C_3 = (15*0 + 19*12 + 15*8) \pmod{27} = 348 \pmod{27} = 24 = \text{X}$$

$C = \text{BAX PMA BJE XAF EUM}$  (compruebe Ud. los demás trigramas)

Para descifrar encontramos  $K^{-1} = \text{inv}(K, 27) = K^{-1} = T_{\text{ADJ}(K)}/|K| \pmod{n}$

$$|K| = 16(6*15 - 19*18) - 4(8*15 - 15*18) + 11(8*19 - 15*6) \pmod{27} = 4$$

Encontramos luego la matriz adjunta de  $K$ , la trasponemos cambiando filas por columnas y la multiplicamos por  $\text{inv}(|K|, 27) = \text{inv}(4, 27) = 7$  con lo que se obtiene la matriz que se indica (hágalo Ud.) →

## Ejemplo de descifrado de Hill

$$[M] = [K^{-1}] \times [C] \bmod n \quad y \quad K^{-1} = \begin{pmatrix} 18 & 26 & 15 \\ 24 & 6 & 13 \\ 11 & 24 & 10 \end{pmatrix}$$

$C = BAX \text{ PMA } BJE \text{ XAF } EUM$  y la clave  $K^{-1}$  es la que se muestra:

$$\begin{pmatrix} M_1 \\ M_2 \\ M_3 \end{pmatrix} = \begin{pmatrix} 18 & 26 & 15 \\ 24 & 6 & 13 \\ 11 & 24 & 10 \end{pmatrix} \times \begin{pmatrix} 1 \\ 0 \\ 24 \end{pmatrix} \bmod 27 \quad \begin{array}{l} \text{Descifrado del primer trígrama} \\ \text{del criptograma: BAX = 1, 0, 24.} \end{array}$$

$C = BAX \text{ PMA } BJE \text{ XAF } EUM$

$$M_1 = (18*1 + 26*0 + 15*24) \bmod 27 = 378 \bmod 27 = 0 = A$$

$$M_2 = (24*1 + 6*0 + 13*24) \bmod 27 = 336 \bmod 27 = 12 = M$$

$$M_3 = (11*1 + 24*0 + 10*24) \bmod 27 = 251 \bmod 27 = 8 = I$$

M = AMI GOC OND UCT ORZ (compruebe Ud. los demás trigramas)

## Ataque al cifrado de Hill por Gauss Jordan

El método consiste en escribir una matriz  $2N$ -grámica con los elementos del texto en claro y los elementos del criptograma. En esta matriz realizamos operaciones lineales (multiplicar filas por un número y restar filas entre sí) con el objeto de obtener los vectores unitarios.

Por ejemplo podemos romper la matriz clave K teniendo:

M = ENU NLU GAR DEL AMA NCH ADE CUY ONO ...

C = WVX IDQ DDO ITQ JGO GJI YMG FVC UÑT ...

$$\left( \begin{array}{ccc|ccc} E & N & U & W & V & X \\ N & L & U & I & D & Q \\ G & A & R & D & D & O \\ D & E & L & I & T & Q \\ A & M & A & J & G & O \\ N & C & H & G & J & I \\ A & D & E & Y & M & G \\ C & U & Y & F & V & C \\ O & N & O & U & Ñ & T \end{array} \right) = \left( \begin{array}{ccc|ccc} 4 & 13 & 21 & 23 & 22 & 24 \\ 13 & 11 & 21 & 8 & 3 & 17 \\ 6 & 0 & 18 & 3 & 3 & 15 \\ 3 & 4 & 11 & 8 & 20 & 17 \\ 0 & 12 & 0 & 9 & 6 & 15 \\ 13 & 2 & 7 & 6 & 9 & 8 \\ 0 & 3 & 4 & 25 & 12 & 6 \\ 2 & 21 & 25 & 5 & 22 & 2 \\ 15 & 13 & 15 & 21 & 14 & 20 \end{array} \right)$$

## Operaciones en la matriz de Gauss Jordan

Vamos a dejar en la primera columna un número uno en la fila primera y todas las demás filas un cero. Luego multiplicamos el vector  $(4 \ 13 \ 21 \mid 23 \ 22 \ 24)$  por el  $\text{inv}(4, 27) = 7$ . Así obtenemos  $7(4 \ 13 \ 21 \mid 23 \ 22 \ 24) \bmod 27 = (1 \ 10 \ 12 \mid 26 \ 19 \ 6)$ . Si esto no se puede hacer con la primera fila movemos los vectores. Hecho esto vamos restando las filas respecto de esta primera como se indica:

$$\left( \begin{array}{ccc|ccc} 4 & 13 & 21 & 23 & 22 & 24 \\ 13 & 11 & 21 & 8 & 3 & 17 \\ 6 & 0 & 18 & 3 & 3 & 15 \\ 3 & 4 & 11 & 8 & 20 & 17 \\ 0 & 12 & 0 & 9 & 6 & 15 \\ 13 & 2 & 7 & 6 & 9 & 8 \\ 0 & 3 & 4 & 25 & 12 & 6 \\ 2 & 21 & 25 & 5 & 22 & 2 \\ 15 & 13 & 15 & 21 & 14 & 20 \end{array} \right)$$

- a) 2<sup>a</sup> fila = 2<sup>a</sup> fila – 13\*1<sup>a</sup> fila mod 27
- b) 3<sup>a</sup> fila = 3<sup>a</sup> fila – 6\*1<sup>a</sup> fila mod 27
- c) 4<sup>a</sup> fila = 4<sup>a</sup> fila – 3\*1<sup>a</sup> fila mod 27
- d) 5<sup>a</sup> fila ya tiene un 0
- e) 6<sup>a</sup> fila = 6<sup>a</sup> fila – 13\*1<sup>a</sup> fila mod 27
- f) 7<sup>a</sup> fila ya tiene un 0
- g) 8<sup>a</sup> fila = 8<sup>a</sup> fila – 2\*1<sup>a</sup> fila mod 27
- h) 9<sup>a</sup> fila = 9<sup>a</sup> fila – 15\*1<sup>a</sup> fila mod 27

## Matriz clave de Hill criptoanalizada

Repetimos este procedimiento ahora para algún vector en cuya segunda columna tenga un número con inverso en 27 y lo mismo para la tercera columna, moviendo si es preciso los vectores.

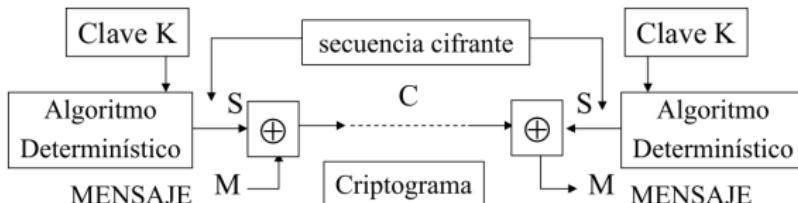
Como la mitad izquierda de la matriz 2N era el texto el claro, la parte derecha de la matriz con vectores unitarios corresponderá a la traspuesta de la clave.

$$\left( \begin{array}{ccc|ccc} 1 & 0 & 0 & 2 & 5 & 7 \\ 0 & 1 & 0 & 3 & 5 & 8 \\ 0 & 0 & 1 & 4 & 6 & 9 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{array} \right) \Rightarrow K = \begin{pmatrix} 2 & 3 & 4 \\ 5 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}$$

Compruebe que la clave es la utilizada en este cifrado.

# El cifrador de Vernam

- 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 que se obtiene a partir de una clave secreta K compartida por emisor y receptor.
  - 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.



## Ejemplo de cifrado de Vernam

Usando el código Baudot (vea los códigos en la tabla de Baudot que encontrará en el Capítulo 21) se pide cifrar:

M = BYTES

K = VERNAM

Solución:

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

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

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

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

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

$$C = UHGFI$$

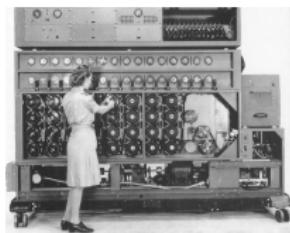
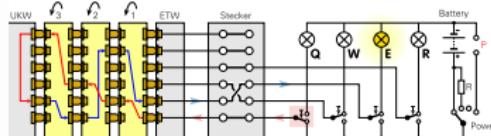
El esquema de Vernam es el único cifrador matemáticamente seguro y, por tanto, imposible de criptoanalizar pues la clave K se usa una sola vez (one-time pad), es aleatoria y tanto o más larga que el propio mensaje. En este caso, no cabe ningún ataque por estadísticas del lenguaje o por correlación de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

[http://www.pro-technix.com/information/crypto/pages/vernam\\_base.html](http://www.pro-technix.com/information/crypto/pages/vernam_base.html)



## El cifrador de la Máquina Enigma

- Enigma era el nombre de una máquina de rotores que permitía usarla tanto para cifrar como para descifrar mensajes.
- La máquina Enigma fue un dispositivo electromecánico que usaba una combinación de partes mecánicas y eléctricas.



# Criptosistemes Clàssics

Carlos Borrego

Carlos.Borrego@uab.cat

Departament d'Enginyeria de la Informació i de les Comunicacions  
Universitat Autònoma de Barcelona

Criptografia i Seguretat