

## CIFRADO EN BLOQUES

$$M = A^n$$

(EN LA PRÁCTICA  $n=m$ )

$$C = A^m$$

$$c_K = c(-, K) : A^n \rightarrow A^m$$

$m \mapsto c$

$$d_K = d(-, K) : A^m \rightarrow A^n$$

$c \mapsto m$

- LA MAYORÍA DE CRIPTOSISTEMAS SON DE BLOQUE
- PARA CADA CLAVE  $K$ ,  $c_K : A^n \rightarrow A^m$  ES UNA BIYECCIÓN. ES DECIR, TENEMOS UNA PERMUTACIÓN DE  $A^n$

- SE PODRÍA TOMAR COMO CONJUNTO DE CLAVES EL GRUPO DE PERMUTACIONES. PERO EN LA PRÁCTICA ES DEMASIADO GRANDE Y NO ES OPERATIVO  $n!$
- LA IDEA ES ELEGIR UNA FORMA ALTERNADA DE GENERAR PERMUTACIONES QUE PRODUZCAN MÉTODOS EFICIENTES Y SEGUROS DE CIFRADO

# CIFRADO EN FLUJO

$$M = C = A^*$$

PARA CIFRAR  $a_1 a_2 \dots a_n \in A^*$  SE HACE UN PROCESO SECUENCIAL QUE EMPIEZA EN  $a_1$  Y DONDE EL CIFRADO DE  $a_i$  DEPENDE DE  $a_1, \dots, a_i$

PARA  $i=1, \dots, n$

$c_i: A \rightarrow A$  BIYECCIÓN DEPENDE DE CLAVE  $K$   
Y LOS PARES  $(a_j, c_j(a_j))$   
CON  $j=1, \dots, i-1$

NORMALMENTE  $c_i$  ES UNA OPERACIÓN SENCILLA Y LA MISMA SIEMPRE DE MANERA QUE LA CLAVE  $K_i$  DEPENDA DE LA POSICIÓN (CLAVE DE VUELTA) Y DE LOS SÍMBOLOS

Y CIFRADOS ANTERIORES

$$c_i : A \times K \rightarrow A$$

Δ PARTIR DE UN CIFRADO EN BLOQUE  
PODEMOS HACER UN SENCILLO CIFRADO EN FLUJO

- PARA UN MENSAJE LARGO  $a \in A^*$

- PARA UN CRIPTOSISTEMA EN BLOQUE  $c_k : A^n \rightarrow A^n$

TROCEAMOS EL MENSAJE EN BLOQUES DE TAMAÑO  $n$   
CIFRAMOS CADA BLOQUE Y LOS CONCATENAMOS

ASÍ HACEMOS UN SENCILLO CIFRADO EN FLUJO  
Sobre el alfabeto  $A^n$

¿COMO REPRESENTAMOS EL ALFABETO?

## CRYPTOGRAFÍA CLÁSICA

- ALFABETO LATINO SIN ESPACIOS, COMAS, ...  
NI ACENTOS, NI Ñ, ...

26 CARACTERES

$$A = \{a, b, \dots, z\} \longleftrightarrow \{0, 1, \dots, 25\}$$

$$\begin{array}{ll} a \mapsto 0 & y \mapsto 24 \\ b \mapsto 1 & z \mapsto 25 \end{array}$$

TRAJAMOS EN  $\mathbb{Z}/26\mathbb{Z}$

Y EN GENERAL, SI TENEMOS HASTA  
 N SIMBOLOS TRABAJAMOS EN  $\mathbb{Z}/N\mathbb{Z}$   
 IDENTIFICANDO ESOS SIMBOLOS CON ELEMENTOS  
 DE  $\mathbb{Z}/N\mathbb{Z}$

EJ: CÓDIGO ASCII - 256 SIMBOLOS

PODEMOS TRABAJAR CON

$$\mathbb{Z}_{256} \text{ ó } F_{256}$$

$$(i_1, \dots, i_8) \in (\mathbb{Z}_2)^8$$

$$F_q \neq \mathbb{Z}_q$$

$\uparrow$   
 CUERPO       $\uparrow$   
 NO CUERPO

## CÓDIGOS DE SUBSTITUCIÓN

SE SUBSTITUYE EL ALFABETO  $A$  DEL MENSAJE EN CLARO  
POR UN SEGUNDO ALFABETO  $B$  DEL MISMO TAMAÑO  
ASÍ TENEMOS UNA BIYECCIÓN

$$f: A \rightarrow B$$

USUALMENTE  $B$  ES EL MISMO ALFABETO  $A$  PERO  
PERMUTADO (CAMBIADO EL ORDEN)

CLAVE CIFRADO: UNA PERMUTACIÓN DETERMINADA DE  $A$   
CLAVE DESCIFRADO: LA PERMUTACIÓN INVERSA

EJ: CÓDIGO DE CÉSAR (JULIO CESAR)

SE DESPLAZA CADA LETRA DEL ABECEDARIO  $k$

POSICIONES. EN EL CASO DE JULIO CESAR,  
 $K=3$ .

$$\text{CIFRSDO: } C \equiv m + k \pmod{N}$$

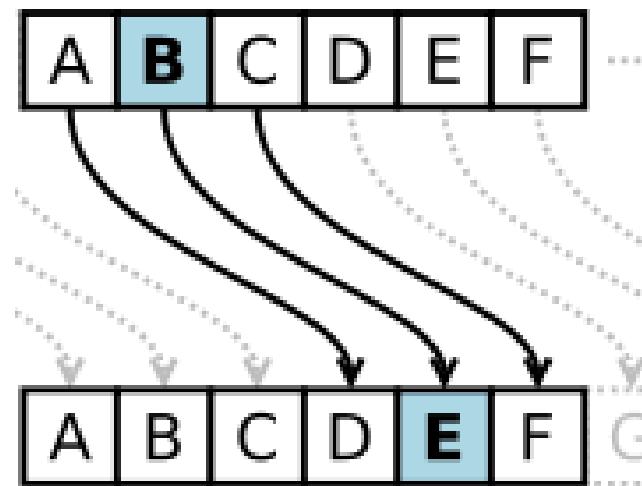
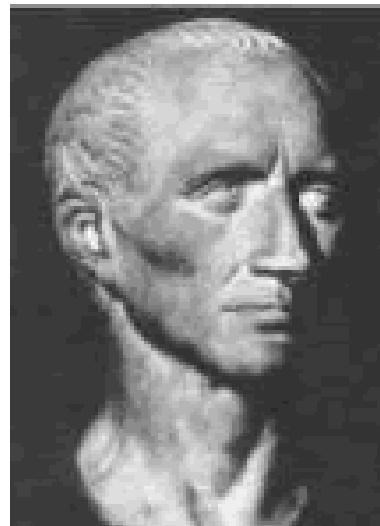
**DESCIFRADO:**  $m \equiv c - k \pmod{N}$

EJ: SIGUIENTE TRANSPARENCIA

SEGURIDAD: NULA. TAMAÑO MUY PEQUEÑO DE CLAVES

Roma....

El cifrado de César:



A  
B

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

Texto: VINI VIDI VINCI

Texto cifrado: YLPL YLGL YLPFL

**SUSTITUCIÓN:** El alfabeto se cambia en otro alfabeto, normalmente el mismo en otro orden. En el caso de César desplazado 3 unidades.

En general se tomará una reordenación cualquiera:

A      | 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

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

PERMUTACIÓN  
BIYECCIÓN

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

Texto: VINI VIDI VINCI

Texto cifrado: ZSXS ZSÑS ZSXRM

HAY MUCHAS CLAVES: n!

PERO HAY OTRO PROBLEMA ...

ANÁLISIS DE FRECUENCIAS: (BAGDAD, SIGLO IX)

ATAQUE PARA CUALQUIER CÓDIGO DE SUBSTITUCIÓN

CADA LETRA TIENE UNA FRECUENCIA DE USO DISTINTA, POR EJEMPLO LA LETRA e ES LA MÁS USADA EN ESPAÑOL E INGLÉS.

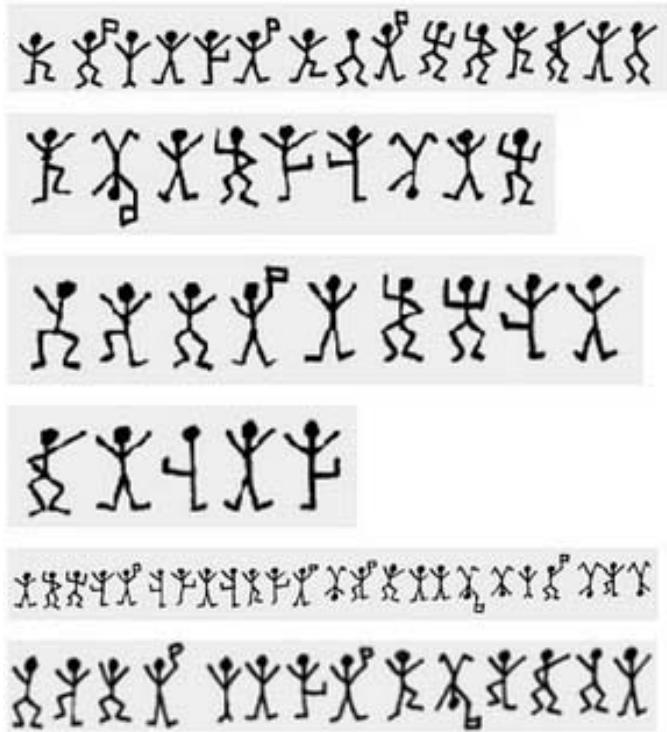
ASÍ QUE CONOCIENDO UNA SUFFICIENTE CANTIDAD DE TEXTO CIFRADO, PODEMOS DESCIFRARLO.

PARA DIFICULTAR ESTE ATAQUE:

- POLISUBSTITUCIONES: EN LUGAR DE SUBSTITUIR LETRA A LETRA DEL MENSAJE (MONOSUBSTITUCIONES), SE PUEDEN SUBSTITUIR BLOQUES DE LETRAS

SEGURIDAD: SE DIFICULTA EL ANÁLISIS DE FRECUENCIAS PERO SE PUEDE ATACAR DE LA MISMA MADERA

No importa tomar alfabetos extraños....

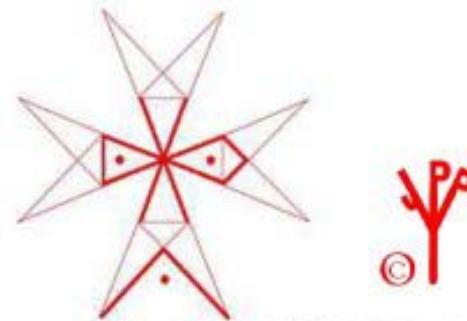


Conan Doyle: *Los bailarines (El regreso de Sherlock Holmes)*

## Criptografía Templaria

V	A	<	F	◊	L	Λ	Q	▷	V
<	B	△	G	◇	M	▷	R	•	X
Λ	C	▽	H	✗	N	▽	S	•	Y
▷	D	◊	I	∨	O	◁	T	•	W
▷	E	◇	K	<	P	△	U	•	Z

*El Alfabeto que los Círculos internos de la Orden utilizaban. Derivado de la Cruz de las Ocho Beatitudes*



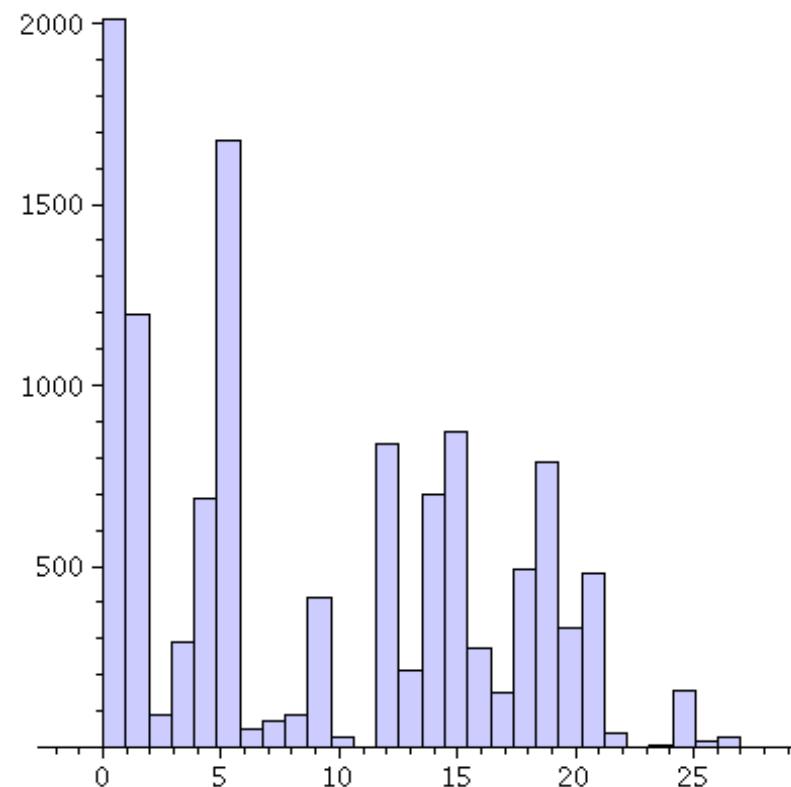
*Los signos son extraídos de la regla Oficial del Temple Conservados en Roma, Dijon y París*

El análisis de frecuencias funciona de la misma forma.

La “huella” de frecuencias de un idioma es muy característica....

## Frecuencias del castellano

ES	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	
2012	1196	92	292	687	1676	52	73	89	415	30	1	837	212	701	29	869	276	153	494	788	331	480	39	1	6	154	15	
ES	E	A	O	L	S	N	D	R	U	I	T	C	P	M	Y	Q	B	H	G	F	V	J	Ñ	Z	X	K	W	
		1196	869							415	331					153	92							29	15			1



- CÓDIGOS HOMÓFONOS : SE TOMA UN ALFABETO  $\mathcal{B}$  CON CARDINAL (TAMÁÑO) MAYOR QUE  $\mathcal{A}$ .

$$\begin{array}{l} \varphi: \mathcal{A} \rightarrow \mathcal{B} \quad \text{"UNO A VARIOS"} \\ x \mapsto \varphi(x) \\ y \mapsto \varphi(y) \end{array}$$

$\varphi(x) \cap \varphi(y) = \emptyset$

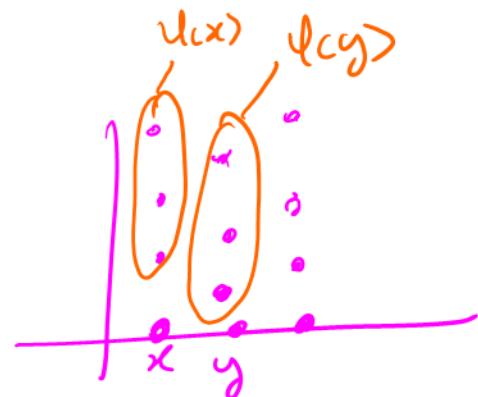
↑

PARA QUE NO HAYA AMBIGÜEDAD  
EN EL CIFRADO

ASÍ PODEMOS ENMASCARAR LA FRECUENCIA DE LAS LETRAS  
POR EJEMPLO ASIGNAMOS A UNA LETRA CON ALTA  
FRECUENCIA VARIOS IMÁGENES.

$$e \mapsto \{1, 5, 15, 33, 43\}$$

$$w \mapsto \{?y\}$$



## - SUBSTITUCIONES POLIALFABÉTICAS:

LA IMAGEN DE CADA LETRA DEPENDE DE SU POSICIÓN DENTRO DEL MENSAJE A CIFRAR.  
NORMALMENTE CON LA AYUDA DE UNA PALABRA CLAVE.

EJ: CÓDIGO DE AGUSTO (NO DOCUMENTADO)

CLAVE: UNA PALABRA O FRASE QUE LOS COMUNICANTES ESCOGEN

EN EL CASO DE AGUSTO, ERA EL PRINCIPIO DE LA ILIADA

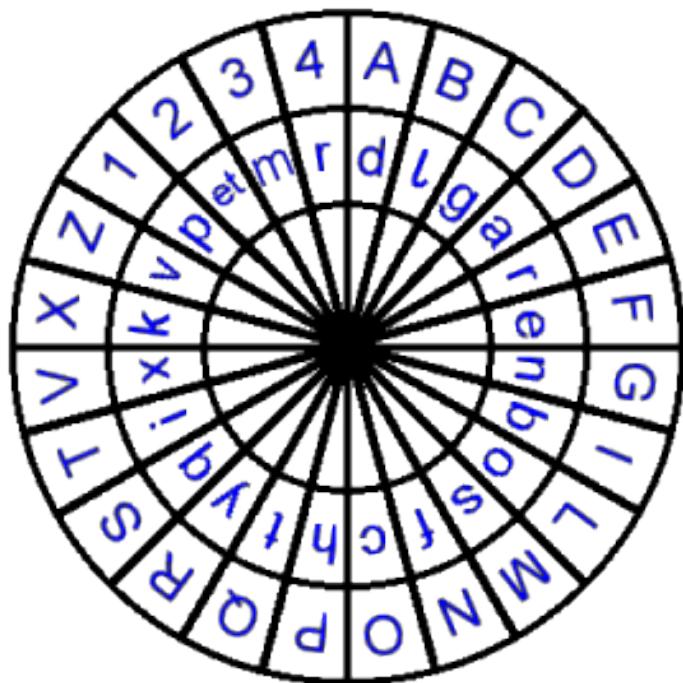
CLAVE:  $k_1 \dots k_n \dots$

MENSAJE:  $m_1 m_2 \dots m_n$

CIFRADO: SUMAR MODULARMENTE CADA LETRA

EJ:  $(k_1 + m_1 \bmod N), (k_2 + m_2 \bmod N), \dots$

Cifrados de sustitución **polialfabética**: La idea es utilizar varias sustituciones que se van alternando. El disco de Alberti es el primer ejemplo documentado de uso.



Clave: CIFRA

Mensaje: HOLA

CLAVE	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	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	A	B
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
F	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	D	E
R	R	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
A	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: ~~JPWR~~  
Jw PR

Un mensaje más largo: LACRIPTOGRAFIAYANOESUNARTESINOUNACIENCIA

- 1) Lo sepáramos en bloques de 5 (tantas letras como tiene la clave):

C	I	F	R	A
L	A	C	R	I
P	T	O	G	R
A	F	I	A	Y
A	N	O	E	S
U	N	A	R	T
E	S	I	N	O
U	N	A	C	I
E	N	C	I	A

2) Cada columna se cifra con la sustitución que marca la clave: la primera con C, la segunda con I, ...

CLAVE	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	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	A	B
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
F	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	D	E
R	R	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
A	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	F	R	A
L	N	A	I	C
P	R	T	B	H
A	C	F	N	R
A	C	N	U	J
U	W	N	U	T
E	G	S	M	G
U	W	N	U	C
E	G	N	U	H

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

Cifrado: **NIHJIRBTXRCNNRYCUTVSWUFJTGMNROWUFTIGUHZA**

El criptoanálisis se consigue en el S. XIX por **Kasiski y Babbage**

LAS IRREGULARIDADES DEL LENGUAJE SE FORMALIZAN  
Y CUANTIFICAN EN TEORÍA DE LA INFORMACIÓN : RE-  
DUNDANCIA DEL LENGUAJE

UN LENGUAJE SIN REDUNDANCIA SERÍA AQUEL EN EL  
QUE TODAS LAS COMBINACIONES DE LETRAS SON VÁLIDAS  
Y TIENEN LA MISMA FRECUENCIA DE APARICIÓN  
ESTE LENGUAJE SERÍA INMUNE AL ANÁLISIS DE FRECUEN-  
CIAS. DE HECHO SERÍA INMUNE AL CRPTOANÁLISIS  
PORQUE NO SE SABRÍA SI SE HABÍA TENIDO ÉXITO AL  
DESCIFRAR UN MENSAJE .

La antigua Grecia....

El escitalo lacedemonio:



Consiste en “desordenar” el mensaje original con una pauta (clave).

# CÓDIGOS DE TRANSPOSICIÓN

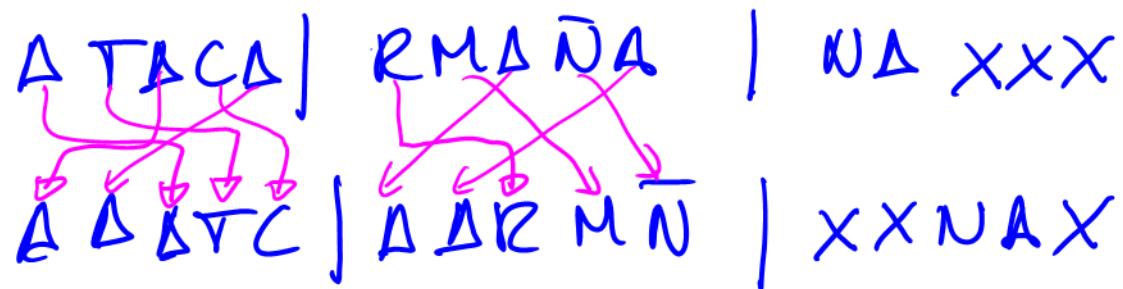
SE CIFRA TRANSPONIENDO (PERMUTANDO) LAS LETRAS DEL MENSAJE EN CLARO.

EL MENSAJE SE DIVIDE EN BLOQUES DE TAMAÑO  $n$  Y CADA UNO SE CIFRA DE FORMA INDEPENDIENTE, REORDENANDO LAS LETRAS QUE LO FORMAN, DE ACUERDO A UNA PERMUTACIÓN QUE ES LA CLAVE.  
(ES UN CIFRADO EN BLOQUE)

EJ:  $n=5$

CLAVE  $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 5 & 2 \end{pmatrix} \downarrow$

$M = ATACARMANADA$



SEGURIDAD: SE CONSERVA LA FRECUENCIA DE LAS LETRAS → ANÁLISIS DE FRECUENCIAS

PERO SE DESTRUYEN LAS ESTRUCTURAS GRAMATICALES.

# CÓDIGOS LINEALES O MATEMÁTICOS (1929)

MENSAJES: BLOQUES LONGITUD  $n$  (PREFIJADA)

IDENTIFICAMOS LETRAS CON NÚMEROS  $\mathbb{Z}/N\mathbb{Z}$

MENSAJE  $\in (\mathbb{Z}/N\mathbb{Z})^n$

CLAVE: MATRIZ  $A$  INVERTIBLE TAMAÑO  $n \times n$

$$(\text{mcd}(\det(A), N) = 1)$$

CLAVE DESCIFRADO:  $A^{-1}$

CIFRADO:  $\vec{c} = \vec{m} \vec{A}$

DESCIFRADO:  $\vec{c} A^{-1}$

EJ:  $N=27$   $n=3$

$$\Delta = \begin{pmatrix} 2 & 8 & 15 \\ 15 & 25 & 3 \\ 1 & 16 & 2 \end{pmatrix}$$

$$\vec{m} = DOS = (3, 15, 19)$$

$$\vec{c} = (3, 15, 19) \Delta = (6, 18, 11) = GRL$$

VARIANTE: CIFRADO AFIN

CLAVE: { MATRIZ  $\Delta$  nxn INVERTIBLE  
 $\vec{b} \in (\mathbb{Z}/N\mathbb{Z})^n$

CIFRADO:  $\vec{c} = \vec{m}\Delta + \vec{b}$

DESCIFRADO:  $\vec{c}\Delta^{-1} - \vec{b}\Delta^{-1}$

$$\begin{aligned} \vec{c}\Delta^{-1} - \vec{b}\Delta^{-1} &= (\vec{m}\Delta + \vec{b})\Delta^{-1} - \vec{b}\Delta^{-1} \\ &= \vec{m}\Delta\Delta^{-1} + \vec{b}\Delta^{-1} - \vec{b}\Delta^{-1} \\ &= \vec{m}\text{Id} = \vec{m} \end{aligned}$$

## SEGURIDAD:

PARECEN MUY SEGUROS, ENMASCARAMOS LA ESTRUCTURA DEL LENGUAJE AL MULTIPLICAR POR LA MATRIZ Y NO ES VISIBLE UN ATAQUE DE FRECUENCIAS  
ADEMÁS EL NÚMERO DE CLAVES (LLAVES) POSIBLES ES MUY GRANDE

PROBLEMA: VULNERABLES A ATAQUES DE TEXTO CLARO CONOCIDO

A PUEDE COLUCLARSE RESOLVIENDO UN SISTEMA DE ECUACIONES LINEALES SI CONOCEMOS

$(\vec{c}_1, \vec{m}_1), \dots, (\vec{c}_n, \vec{m}_n)$  LINEALMENTE INDEPENDIENTES

$$\left\{ \vec{c}_i = m_i A \quad i=1, \dots, n^2 \right.$$

## CIFRADO DE VIGENÈRE (1853)

SE FIJA UNA PALABRA  $K_1, \dots, K_s$  (CLAVE)

EL MENSAJE EN CLARO  $m_0, m_1, \dots, m_n, \dots$  SE REPARTIZO EN BLOQUES DE LONGITUD  $\Delta$

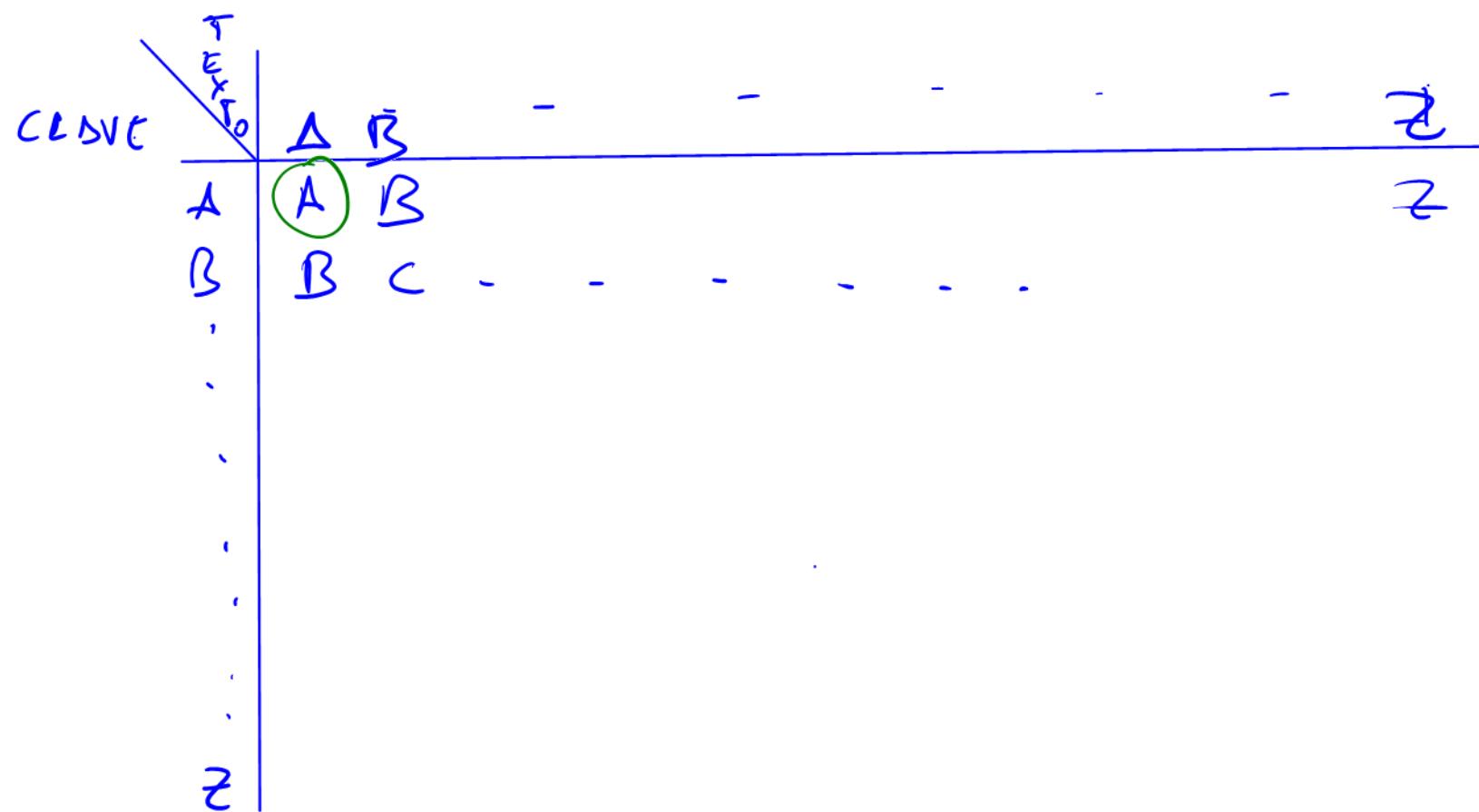
EL CARÁCTER  $i$  DE CADA BLOQUE SE CIFRA CON LA CLAVE DE CÉSAR  $K_i$

$$m_{\Delta t+i} \rightarrow m_{\Delta t+i} + K_i$$

EL CIFRADO Y DESCIFRADO SE PUEDE HACER FÁCILMENTE CON UN DISCO O UNA TABLA

$$BCB = K_1 K_2 K_3$$

HOLASI  $\rightarrow [HOL | ASI] \rightarrow [HOL + BCB] \rightarrow [ASI + BCB] \rightarrow [QM | BUJ] \rightarrow [QMBUJ]$



## CRIPTOANÁLISIS (KASINSKI / BABSTAGE 1859)

PARA TEXTOS LARGOS EN COMPARACIÓN CON EL TAMAÑO  
DE LA CLAVE. SEPARAMOS EL TEXTO EN BLOQUES DE  
TAMAÑO  $\lambda$  Y HACEMOS ANÁLISIS DE FRECUENCIAS

SE ESTIMA  $\lambda$  MEDIANTE CORRELACIÓN ENTRE LAS  $\lambda \times \lambda$ -  
BLOQUES DE FRECUENCIAS DE LOS SUBTEXTOS CIFRADOS  
CON LA TABLA DE FRECUENCIAS DEL ALFABETO  
FRECUENCIA  $k\lambda + i$ ,  $k=1, 2, \dots$  DEBE SER IGUAL A  
LA DEL ALFABETO

TAMBIÉN SE BUSCAN 2, 3, ..., LETRAS REPETIDAS EN  
EL TEXTO: NOS DA UN CANDIDATO PARA  $\lambda$

# CUADERNO DE USO ÚNICO

VERSIÓN MODERNA DEL CIFRADO DE VIGENÈRE: UN CUADERNO CON MUCHAS CLAVES ALEATORIAS DE TAMAÑO SUFFICIENTEMENTE GRANDE Y QUE SE USAN SÓLO UNA VEZ.

ES MUY COMPLEJO GENERAR, DISTRIBUIR Y ALMACENAR LAS CLAVES. POR LO QUE ESTE MÉTODO SÓLO SE USA PARA COMUNICACIONES DE ALTO NIVEL

EJ: MÉTODO USADO COMUNICACIONES VIAL TELEFONO ROJO ENTRE PRESIDENTES EEUU Y URSS.

# CIFRADO DE VERNAM

ES EL CASO LÍMITE DEL CIFRADO DE VIGENÈRE.

EMPLEAMOS UN ALFABETO BINARIO

CLAVE: SECUENCIA BINARIA ALEATORIA DE LA MISMA  
LONGITUD QUE EL TEXTO CLARO.

$$M = M_1, \dots, m_n \in \mathbb{F}_2^n$$

$$K = K_1, \dots, k_n \in \mathbb{F}_2^n$$

CIFRADO:

$$C(M) = M \text{ XOR } K = m_1 + k_1, m_2 + k_2, \dots, m_n + k_n$$

DESCIFRADO:

$$C(M) \text{ XOR } K = M$$

EL CIFRADO DE VERNAM ES INCONDICIONALMENTE SEGURO. ES UN CIFRADO PERFECTO, BAJO LA HIPÓTESIS DE QUE LA CLAVE ES ALEATORIA Y SE USA UNA ÚNICA VEZ.

INCONVENIENTE: NO ES PRÁCTICO. SE NECESITA UNA PREPARACIÓN PREVIA PARA GENERAR LA CLAVE Y COMPARTIRLA.

TRANSMITIR LA CLAVE DE FORMA SEGURA ES IGUAL DE COSTOSO QUE TRANSMITIR EL MENSAJE

CUALQUIER CIFRADO CON SEGURIDAD PERFECTA ES ESENCIALMENTE EL CIFRADO DE VERNAM PROBADO POR CLAUDE SHANNON.

# CIFRADO EN BLOQUE MODERNO

LOS MÉTODOS DE CIFRADO EN BLOQUE QUE SE USAN HOY EN DÍA SON BASTANTE MÁS COMPLICADOS. CADA BLOQUE SE CIFRA USANDO VARIAS OPERACIONES DE UNA MEZCLA DE CIFRADOS DE SUSTITUCIÓN Y TRASPOSICIÓN.

TAMBIÉN SE INCLUYEN TÉCNICAS DE DIFUSIÓN Y PROPAGACIÓN. UN BIT O UNOS POCOS BITS SE PROPAGAN Y CAMBIA MUCHO EL MENSAJE CIFRADO. ASÍ ES RESISTENTES FRENTE A ATAQUES QUE MODIFICAN EL TEXTO CLARO LIGERAMENTE.

INCLUYEN OPERACIONES NO LINEALES PARA NO SER VULNERABLE A ATAQUES LINEALES CRESOLVER SISTEMAS DE ECUACIONES

## DOS CRIPTOSISTEMAS PRINCIPALES

- DES : DATA ENCRYPTION SYSTEM
- AES : ADVANCED ENCRYPTION SYSTEM

DES FUE EL CRIPTOSISTEMA ESTÁNDAR DE CLAVE PRIVADA, DE 1977 A 2002. PERO EN 1998 SE PUBLICÓ UN ATAQUE POR FUERZA BRUTA USANDO 75.000 ORDENADORES).

ENTONCES:  
SE HIZO UN CONCURSO PARA ESCOGER EL NUEVO CRIPTOSISTEMA ESTÁNDAR DE CLAVE PRIVADA.

AES ES EL ESTÁNDAR DESDE 2002

AHORA VAMOS A VER AES. PARA ELLO VAMOS A USAR MATERIAL DISPONIBLE EN MOODLE COMO UNAS TRANSPARENCIAS DE UNOS COMPAÑEROS, UN ARCHIVO FLASH, VÍDEOS, DOCUMENTACIÓN NIST, ...

POSTERIORMENTE VEREMOS CON DETALLE LA CRIPTOGRAFÍA DE CLAVE PÚBLICA QUE NOS VA A SERVIR PARA INTERCAMBIAR LLAVES Y PODER LUEGO USAR LA CRIPTOGRAFÍA DE CLAVE PRIVADA.