Universidad
Carlos III de Madrid
Grupo SeTI · Dpto. Informática

TEMA 2. CRIPTOGRAFÍA
2.2 MÉTODOS CRIPTOGRÁFICOS CLÁSICOS

Criptografía y seguridad informática
Seguridad en las tecnologías de la información
@ COSEC LAB

Curso 2016-2017

ÍNDICE

MÉTODOS CRIPTOGRÁFICOS CLÁSICOS

- INTRODUCCIÓN

CRIPTOGRAFÍA CLÁSICA (siglo V a. C.)

griego: kryptos = escondido

- se hace uso de una clave y un algoritmo de cifrado
- cifrado simétrico: la misma clave sirve para cifrar y descifrar
- se pretendía garantizar la confidencialidad de los mensajes ocultándolos

MÉTODOS CRIPTOGRÁFICOS CLÁSICOS

INTRODUCCIÓN

Se emplean dos técnicas básicas orientadas a caracteres:

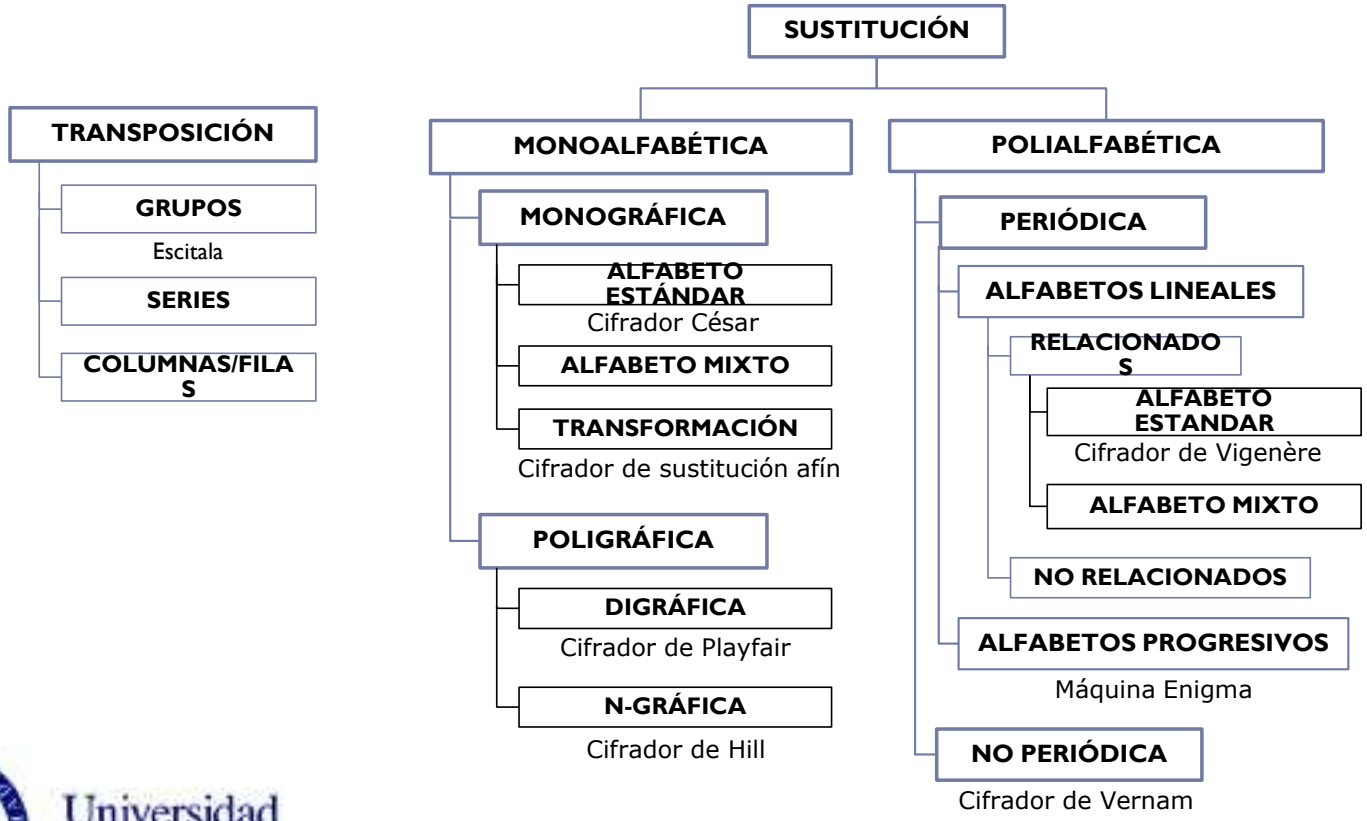
- **Sustitución**: un carácter o letra se modifica o sustituye por otro elemento en la cifra.

- **Transposición o permutación**: los caracteres o letras del mensaje se redistribuyen sin modificarlos, y según unas reglas, dentro del criptograma.

(Muchos siglos después, Shannon lo formaliza matemáticamente).

MÉTODOS CRIPTOGRÁFICOS CLÁSICOS

- CLASIFICACIÓN



ÍNDICE

- 1.1.2 MÉTODOS CRIPTOGRÁFICOS CLÁSICOS
  - INTRODUCCIÓN
  - CLASIFICACIÓN
  - **MÉTODOS DE TRANSPOSICIÓN**
    - **POR GRUPOS**
    - **POR SERIES**
    - **POR COLUMNAS/FILAS**
  - MÉTODOS DE SUSTITUCIÓN
    - SUSTITUCIÓN MONOALFABETO
      - MONOGRÁFICA (SIMPLE)
      - POLIGRÁFICA
    - SUSTITUCIÓN POLIALFABETO
  - CRIPTOANÁLISIS DE CRIPTOGRAFÍA CLÁSICA

MÉTODOS CRIPTOGRÁFICOS CLÁSICOS

- TRANSPOSICIÓN

  Se opera sobre las posiciones, sin alterar el carácter original

  No modifican la frecuencia de aparición de las letras del lenguaje → Análisis de frecuencia

  - EJEMPLOS:
    - TRANSPOSICIÓN DE RIEL
      - escribir mensaje en 2 líneas alternando los caracteres
      - añadir segunda fila al final de la primera

MÉTODOS CRIPTOGRÁFICOS CLÁSICOS

- TRANSPOSICIÓN POR GRUPOS

Permutación Π_M describe orden de un grupo de p letras

Ejemplo:

Π_M=24531

M = `MANOS ARRIB AESTO ESUNA TRACO`

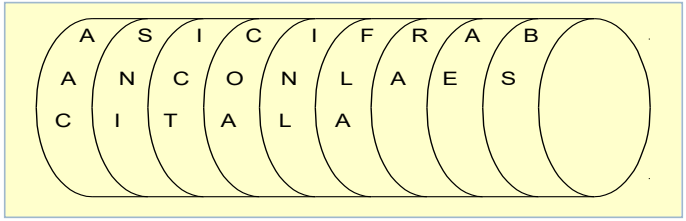
C = `AOSNM RIBRA ETOSA SNAUE RCOAT`

- Cuanto más largo el periodo p, tanto menos vulnerable
- p = longitud de mensaje => transposición por serie

MÉTODOS CRIPTOGRÁFICOS CLÁSICOS

- TRANSPOSICIÓN POR GRUPOS. EJEMPLOS:
  - ESCÍTALA
    - Bastón + cinta de cuero
    - El mensaje se escribe de forma longitudinal
    - El texto en claro se recupera enrollando la cinta en un bastón del mismo diámetro
    - La clave del sistema está en el diámetro del bastón

M = ASI CIFRABAN CON LA ESCITALA



C = AAC SNI ICT COA INL FLA RA AE BS

MÉTODOS CRIPTOGRÁFICOS CLÁSICOS

- TRANSPOSICIÓN POR SERIES

Ordenar mensaje como cadena de submensajes:

$$M' = M_{S1}M_{S2}M_{S3}..., \text{ con } M_{Sx} \text{ funciones o series.}$$

Ejemplo:

M_{S1} = 1,2,3,5,7,11,13,17,19,23 (primos)
M_{S2} = 4,6,8,10,12,14,16,18,20,22,24,26 (pares)
M_{S3} = 9,15,21,25,27 (impares)

M = ERRAR ES HUMANO, PERDONAR DIVINO
C = ERRRSAODNI AEHMNPROADV NUERIO

MÉTODOS CRIPTOGRÁFICOS CLÁSICOS

- TRANSPOSICIÓN POR COLUMNAS/FILAS
- Métodos de reordenación:
  1. disponer los símbolos según un cierto patrón geométrico,
  2. extraerlos posteriormente según una cierta trayectoria.

Patrón bidimensional (matriz).

- Disponer símbolos en filas (columnas) consecutivas y extraer columna a columna (fila a fila) desde la primera a la última.

M = ESTE ES UN EJEMPLO DE TRANSPOSICIÓN COLUMNAR

C = ESEDNICN SUMESCOA TNPTPILR EELROOUX EJOASNMX

E	S	T	E	E
S	U	N	E	J
E	M	P	L	O
D	E	T	R	A
N	S	P	O	S
I	C	I	O	N
C	O	L	U	M
N	A	R	X	X

MÉTODOS CRIPTOGRÁFICOS CLÁSICOS

- EJEMPLO TRANSPOSICIÓN COLUMNAR CON CLAVE

Clave = ESPÍA (orden alfabético: A,E,I,P,S)

M = EJEMPLO DE TRANSPOSICIÓN COLUMNAR CON CLAVE

E	S	P	I	A
E	J	E	M	P
L	O	D	E	T
R	A	N	S	P
O	S	I	C	I
O	N	C	O	L
U	M	N	A	R
C	O	N	C	L
A	V	E	X	X

A	E	I	P	S
P	E	M	E	J
T	L	E	D	O
P	R	S	N	A
I	O	C	I	S
L	O	O	C	N
R	U	A	N	M
L	C	C	N	O
X	A	X	E	V

C = PTPILRLX ELROOUCA MESCOACX EDNICNNE JOASNMOV

ÍNDICE

- 1.1.2 MÉTODOS CRIPTOGRÁFICOS CLÁSICOS
  - INTRODUCCIÓN
  - CLASIFICACIÓN
  - MÉTODOS DE TRANSPOSICIÓN
    - POR GRUPOS
    - POR SERIES
    - POR COLUMNAS/FILAS
  - **MÉTODOS DE SUSTITUCIÓN**
    - **SUSTITUCIÓN MONOALFABETO**
      - **MONOGRÁFICA (SIMPLE)**
      - POLIGRÁFICA
    - SUSTITUCIÓN POLIALFABETO
  - CRIPTOANÁLISIS DE CRIPTOGRAFÍA CLÁSICA

MÉTODOS CRIPTOGRÁFICOS CLÁSICOS

- SUSTITUCIÓN

REPRESENTACIÓN NUMÉRICA DE ALFABETOS

Ejemplos:

- Alfabeto 27 letras: (A, B,..., Z) → (0, 1,...,26)
- Alfabeto 37 letras: (A, B,..., Z, 0, 1, ...9) → (0, 1,...,36)

0	A
1	B
2	C
3	D
4	E
5	F
6	G

7	H
8	I
9	J
10	K
11	L
12	M
13	N

14	Ñ
15	O
16	P
17	Q
18	R
19	S
20	T

21	U
22	V
23	W
24	X
25	Y
26	Z

MÉTODOS CRIPTOGRÁFICOS CLÁSICOS

- SUSTITUCIÓN MONOALFABETO SIMPLE (MONOGRÁFICA)

Sustitución 1 carácter texto-claro por 1 carácter texto-cifrado

- Habría n! posibles cifradores

Parte de los cifradores pueden definirse con una ecuación:

$$E(m_i)=(am_i+b) \text{ mód. } n$$

a : constante de decimación

b : constante de desplazamiento

n : número de letras del alfabeto (27 en español)

Clave = (a,b)

mcd(a,n)=1 (para que exista solución de la ecuación congruencial)

MÉTODOS CRIPTOGRÁFICOS CLÁSICOS

SUSTITUCIÓN MONOGRÁFICA. CASOS PARTICULARES

Cifrador por desplazamiento puro (tipo César, ROT 13, …)

$$E(m_i)=(m_i+b) \text{ mód. } n$$

Ejemplo concreto: Cifrador César

$$E(m_i)=(m_i+3) \text{ mód. } n$$

Cifrador por decimación pura

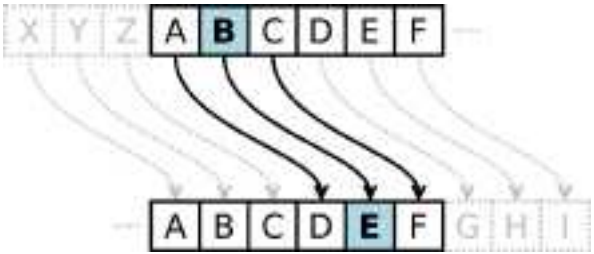
$$E(m_i)=(a \cdot m_i) \text{ mód. } n$$

Cifrador por sustitución afín

$$E(m_i)=(a \cdot m_i+b) \text{ mód. } n$$

MÉTODOS CRIPTOGRÁFICOS CLÁSICOS

- EJEMPLO. CIFRADO CÉSAR



$E_3(x) = (x + 3) \bmod 27$

$D_3(x) = (x - 3) \bmod 27$

M	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	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

M = NUNCA VI NEVAR TANTO

C = PXPFD YL PHYDU WDPWR

ÍNDICE

- 1.1.2 MÉTODOS CRIPTOGRÁFICOS CLÁSICOS
  - INTRODUCCIÓN
  - CLASIFICACIÓN
  - MÉTODOS DE TRANSPOSICIÓN
    - POR GRUPOS
    - POR SERIES
    - POR COLUMNAS/FILAS
  - **MÉTODOS DE SUSTITUCIÓN**
    - **SUSTITUCIÓN MONOALFABETO**
      - MONOGRÁFICA (SIMPLE)
      - **POLIGRÁFICA**
    - SUSTITUCIÓN POLIALFABETO
  - CRIPTOANÁLISIS DE CRIPTOGRAFÍA CLÁSICA

MÉTODOS CRIPTOGRÁFICOS CLÁSICOS

- SUSTITUCIÓN MONOALFABETO POLIGRÁFICA

Sustitución n (n >=2) caracteres texto-claro por n caractereres texto-cifrado

$$M = m_1 m_2 \cdot m_3 m_4 \cdot \ldots \cdot m_{N-1} m_N$$
$$E_k(M) = E_k(m_1 m_2) \cdot E_k(m_3 m_4) \cdot \ldots \cdot E_k(m_{N-1} m_N)$$
$$E_k(M) = c_1 c_2 \cdot c_3 c_4 \cdot \ldots \cdot c_{N-1} c_N$$

Métodos:

- Playfair (Wheatstone)
- Hill

MÉTODOS CRIPTOGRÁFICOS CLÁSICOS

- PLAYFAIR
  - Sustitución digrámica. Digrafos
  - Matriz de 5x5 caracteres (sin J ni Ñ) con la clave comenzando en la primera fila sin caracteres repetidos
  - m_1m_2 misma fila, c_1c_2 → derecha
  - m_1m_2 misma col., c_1c_2 → abajo
  - m_1m_2 con ≠ fila ≠ col., c_1c_2 → esquina opuesta en la misma fila del rectángulo que forman m_1m_2
  - Dígrafos repetidos → deben eliminarse con carácter de relleno
  - Si impares (tras eliminar dígrafos repetidos) → insertar carácter de relleno

Matriz Playfair adaptada al alfabeto castellano, sin 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

Matriz de Playfair adaptada con clave PRIMAVERA

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

RI → IM
BI → HB
ES → CO
BE → CB
FU → NP
OC → SE
OT → QN
AL → DT

MÉTODOS CRIPTOGRÁFICOS CLÁSICOS

- **HILL** Matriz nxn y se multiplica por un vector que es la cadena original.
  - Cifra "n" caracteres a un tiempo (ejemplo: "pan" → "dyj")
  - Utiliza equaciones lineales simples
    - Transformaciones matriciales lineales nxn
    - K_E (nxn) debe tener inversa en el cuerpo de cifra Z_N
    - Caracteres de relleno si texto no múltiplo de "n"
  - Ejemplo de 'cifrador de bloque'

Si $|K_E| \neq 0$ y $mcd(|K_E|, N)=1$

$$K_E^{-1} = |K|^{-1} \cdot (Adj(K))^T \bmod N$$

$$C=K_E * M \text{ (mód. N)}$$

$$M=K_D * C \text{ (mód. N)}$$

$$K_D= K_E^{-1} \text{ (mód. N)}$$

$$\begin{pmatrix} c_1 \\ c_2 \\ \dots \\ c_n \end{pmatrix} = \begin{pmatrix} k_{1,1} & k_{1,2} & \dots & k_{1,n} \\ k_{2,1} & k_{2,2} & \dots & k_{2,n} \\ \dots & \dots & \dots & \dots \\ k_{n,1} & k_{n,2} & \dots & k_{n,n} \end{pmatrix} \times \begin{pmatrix} m_1 \\ m_2 \\ \dots \\ m_n \end{pmatrix}$$

Lo Descrito.. hacer inversa

MÉTODOS CRIPTOGRÁFICOS CLÁSICOS

- HILL. EJEMPLO

M= I CAN'T DO IT

8 2 0 13 19 3 14 8 19

↓

C= EOM TMY SVJ

4 14 12 19 12 14 18 21 9

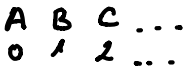
Cadena codificada = Matriz x Cadena ori

$$\begin{pmatrix}4\\14\\12\end{pmatrix} = \begin{pmatrix}9 & 18 & 10\\16 & 21 & 1\\5 & 12 & 23\end{pmatrix} \times \begin{pmatrix}8\\2\\0\end{pmatrix} \text{ (mód. 26)}$$

$$\begin{pmatrix}19\\12\\14\end{pmatrix} = \begin{pmatrix}9 & 18 & 10\\16 & 21 & 1\\5 & 12 & 23\end{pmatrix} \times \begin{pmatrix}13\\19\\3\end{pmatrix} \text{ (mód. 26)}$$

$$\begin{pmatrix}18\\21\\9\end{pmatrix} = \begin{pmatrix}9 & 18 & 10\\16 & 21 & 1\\5 & 12 & 23\end{pmatrix} \times \begin{pmatrix}14\\8\\19\end{pmatrix} \text{ (mód. 26)}$$

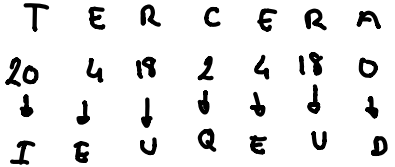
Ejercicios



$E(m) = 7m + 3 \mod 27$

Ejercicios Criptografía Clásica:

1, 5, 6, 7, 8, 9, 10, 11.



ÍNDICE

- 1.1.2 MÉTODOS CRIPTOGRÁFICOS CLÁSICOS
  - INTRODUCCIÓN
  - CLASIFICACIÓN
  - MÉTODOS DE TRANSPOSICIÓN
    - POR GRUPOS
    - POR SERIES
    - POR COLUMNAS/FILAS
  - **MÉTODOS DE SUSTITUCIÓN**
    - SUSTITUCIÓN MONOALFABETO
      - MONOGRÁFICA (SIMPLE)
      - POLIGRÁFICA
    - **SUSTITUCIÓN POLIALFABETO**
  - CRIPTOANÁLISIS DE CRIPTOGRAFÍA CLÁSICA

MÉTODOS CRIPTOGRÁFICOS CLÁSICOS

- SUSTITUCIÓN POLIALFABETO PERIODICA

- Blaise de Vigenére (diplomático francés, 1523-1596)
  - 27 alfabetos cifrados
  - 27 Cambios según método César
  - Clave de longitud m

$$E(m_j) = (m_j + k_{(j \text{ mód } m)}) \text{ mód. } 27$$

donde:

k_i = desplazamiento del alfabeto i

m_j = letra texto en claro en posición j

$E(m_j)$ = letra cifrada

MÉTODOS CRIPTOGRÁFICOS CLÁSICOS

Tabla de Vigenére

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

MÉTODOS CRIPTOGRÁFICOS CLÁSICOS

Ejemplo del método Vigenére con clave:

- Se usa la palabra clave para determinar los alfabetos,

  p.ej.: **SOL (k_1=18, k_2=15, k_3=11)**

- Aplicación:

  Se coloca la clave bajo la cadena y la vamos repitiendo

Mensaje:	H	O	L	A	A	M	I	G	O
Clave repetida:	S	O	L	S	O	L	S	O	L
Cifrado:	Z	D	V	S	O	W	A	U	Z

columna → H O L | A A M | I G O

fila → S O L | S O L | S O L

Después buscamos en la fila de S la columna de H

- Utilizando la tabla:

La tabla empieza con la letra clave como A y las sucesivas a S son B, C, D

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

MÉTODOS CRIPTOGRÁFICOS CLÁSICOS

- Vigenère con autoclave

El texto en claro se utiliza como clave además de la clave primaria:

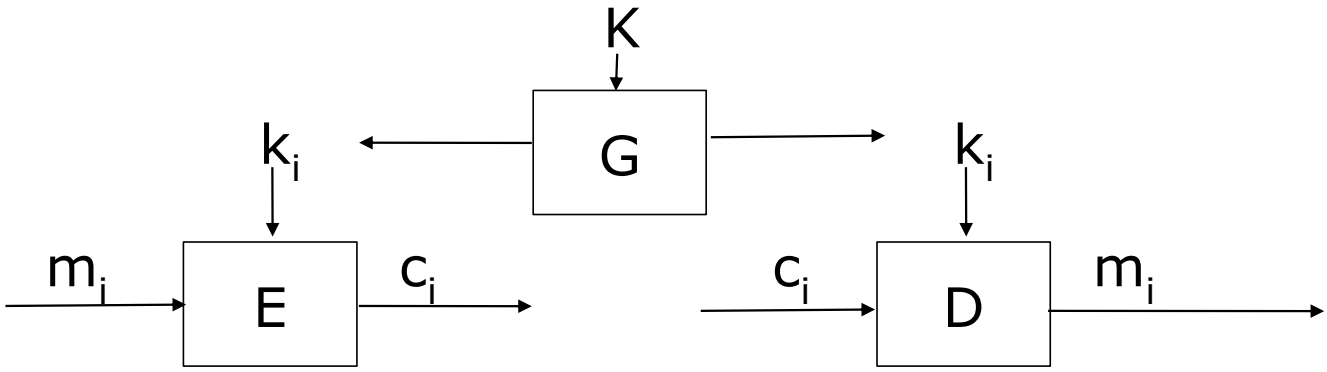
Se escribe la clave y a continuación la propio cadena sin codificar

Clave: SOL

P	L	A	N	T	A	A	T	O	M	I	C	A
S	O	L	P	L	A	N	T	A	A	T	O	M
I	Z	L	C	E	A	N	N	O	M	B	Q	M

MÉTODOS CRIPTOGRÁFICOS CLÁSICOS

- Sustitución polialfabética no periódica: Vernam



$c_i = E(m_i) = (m_i \oplus k_i)$

$m_i = D(c_i) = (c_i \oplus k_i)$

- Secreto perfecto:
  - Longitud_clave igual o mayor que longitud_texto en claro
  - Clave aleatoria
  - Clave de un solo uso

MÉTODOS CRIPTOGRÁFICOS CLÁSICOS

- Sustitución polialfabética no periódica: Vernam
  - Problemas
    - Tamaño de la clave
    - Reutilización
    - Aleatoriedad
  - Ventajas
    - Perfecto

MÉTODOS CRIPTOGRÁFICOS CLÁSICOS

- Máquina Enigma

- Usada por las fuerzas Alemanas desde 1930
- Cifrado/descifrado rotatorio
- Militarmente conocida como Máquina "M"→ Enigma-D
- Funcionamiento:
  - Varios rotores con 26 contactos eléctricos en cada cara del rotor
  - Cada contacto de una cara esta conectado a un contacto diferente de la cara contraria
  - Cada rotor está conectado de forma distinta con sus caras
  - Cada contacto de salida de un rotor se conectaba al de entrada del siguiente
  - Cada vez que se introduce una letra la posición del rotor varía
  - Por cada tecla pulsada se ilumina la tecla equivalente después de ser procesada, tanto en cifrado como descifrado

Ejercicios

Ejercicios Criptografía Clásica:

2, 3, 4

ÍNDICE

- 1.1.2 MÉTODOS CRIPTOGRÁFICOS CLÁSICOS
  - INTRODUCCIÓN
  - CLASIFICACIÓN
  - MÉTODOS DE TRANSPOSICIÓN
    - POR GRUPOS
    - POR SERIES
    - POR COLUMNAS/FILAS
  - MÉTODOS DE SUSTITUCIÓN
    - SUSTITUCIÓN MONOALFABETO
      - MONOGRÁFICA (SIMPLE)
      - POLIGRÁFICA
    - SUSTITUCIÓN POLIALFABETO
  - **CRIPTOANÁLISIS DE CRIPTOGRAFÍA CLÁSICA**

CRIPTOANÁLISIS DE CRIPTOGRAFÍA CLÁSICA

- **Rompiendo el Cifrado de Desplamiento**

Espacio de claves reducido:

fuerza bruta

Probando todas las n dentro de que es mod 27

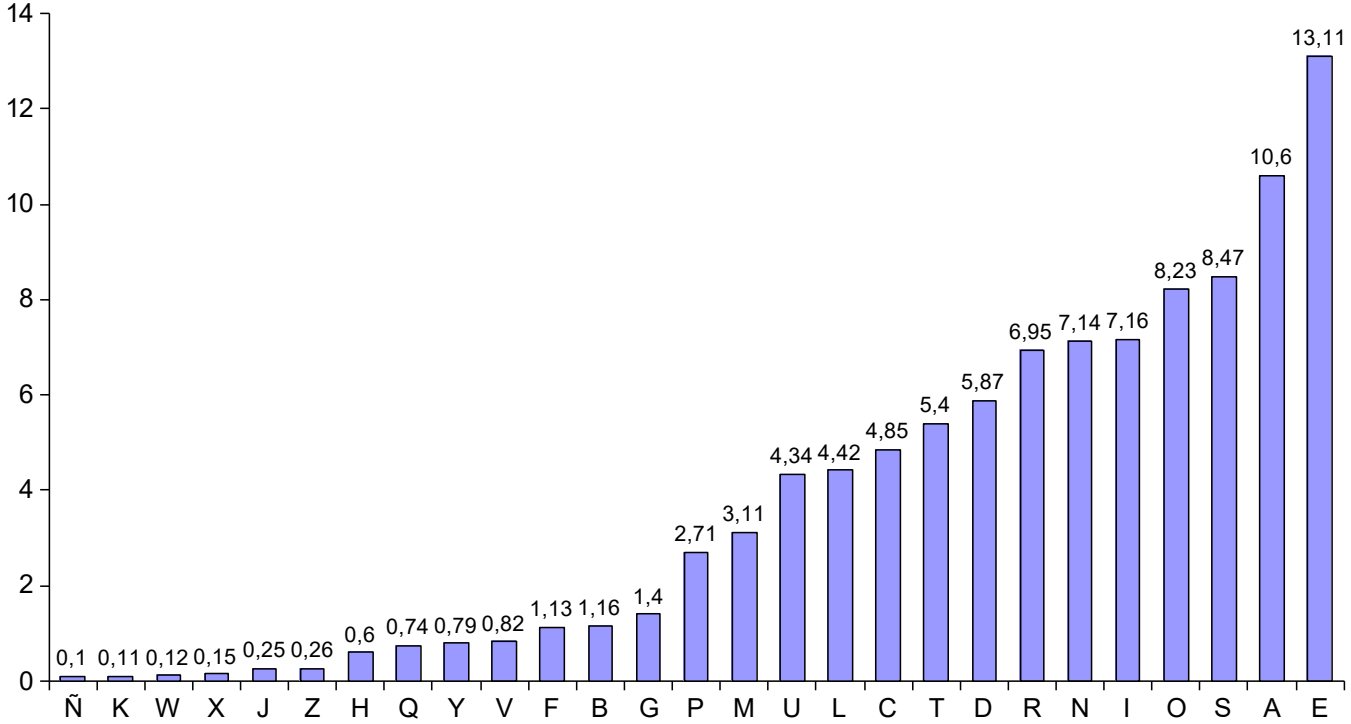
$$E_n(x) = (x + n) \bmod 27$$

$$D_n(x) = (x - n) \bmod 27$$

Desplazamiento	Posible mensaje original
0	Ep exeuyi
1	Do dwdtxh
2	Cn cvcswg
3	Bm bubrvf
4	Al ataque
5	Zk zszptd
6	Yj yryosc
...	
23	Hs hahxbl
24	Gr gzgwak
25	Fq fyfvzj

CRIPTOANÁLISIS DE CRIPTOGRAFÍA CLÁSICA

- Frecuencias de los caracteres en el lenguaje castellano



- **Rompiendo el Cifrado de Sustitución Monoalfabeto**

Caso del cifrador sustitución monoalfabeto **afín**:

$$E(m_i) = (a\, m_i + b) \,mód\, n$$

- Análisis de frecuencias

Texto cifrado:

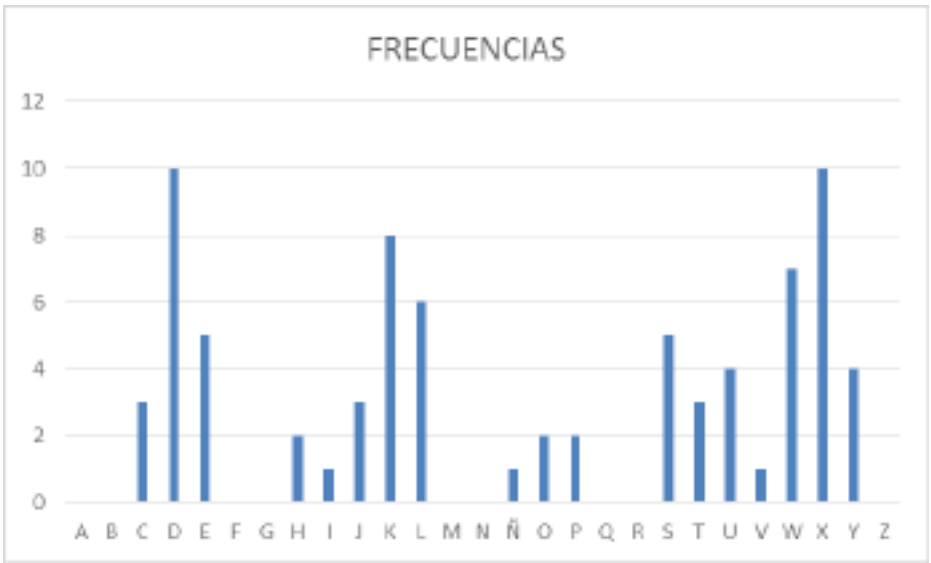
UEYDXTHWYDWXLEXCDXCYDLKXJSKTCWTKXUWLEXJSEOLDP
KXYDLDVKPDUIWUKLXWÑHDSDWXKJSEOKS

CRIPTOANÁLISIS DE CRIPTOGRAFÍA CLÁSICA

- Rompiendo el Cifrado de Sustitución Monoalfabeto

Texto cifrado:
UEYDXTHWYDWXLEXCDXCYDLKXJSKTCWTKXUWLEXJSEOLD
PKXYDLDVKPDUIWUKLXWÑHDSDWXKJSEOKS

0	A	0	
1	B	0	
2	C	10	3,9%
3	D	10	12,99%
4	E	8	6,49%
5	F	0	
6	G	0	
7	H	7	2,6%
8	I	6	1,3%
9	J	5	3,9%
10	K	5	10,39%
11	L	4	7,79%
12	M	0	
13	N	0	
14	Ñ	4	1,3%
15	O	3	2,6%
16	P	3	2,6%
17	Q	0	
18	R	0	
19	S	3	6,49%
20	T	2	3,9%
21	U	2	5,19%
22	V	2	1,3%
23	W	1	9,09%
24	X	1	12,99%
25	Y	1	5,19%
26	Z	0	



CRIPTOANÁLISIS DE CRIPTOGRAFÍA CLÁSICA

- Rompiendo el Cifrado de Sustitución Monoalfabeto (supuesto transformación afín)

Las letras más frecuentes en el texto cifrado son D, X y K.

Supongamos que dos de ellas son el cifrado de dos de las letras más frecuentes en castellano (E, A y S).

Vamos probando suponiendo que coinciden las + frecuentes

Suposición 1: E (4) → D (3), A (0) → X (24)

$3 = a \cdot 4 + b \text{ mód } 27$

$24 = a \cdot 0 + b \text{ mód } 27$

Luego

$b = 24$

$a = (3 - 24) \cdot 4^{-1} \text{ mód } 27 = -21 \cdot 7 \text{ mód } 27 = 6 \cdot 7 = 42 = 15$

Para descifrar, hay que calcular

$a^{-1} \text{ mód } 27 = 15^{-1} \text{ mód } 27 =$ ¡NO EXISTE! pues mcd(15, 27) no es 1

CRIPTOANÁLISIS DE CRIPTOGRAFÍA CLÁSICA

- Rompiendo el Cifrado de Sustitución Monoalfabeto (supuesto transformación afín)

Podemos suponer que el emparejamiento es al revés:

Suposición 2: E (4) → X (24), A (0) → D (3)

$24 = a \cdot 4 + b \bmod 27$

$3 = a \cdot 0 + b \bmod 27$

Luego

$b = 3$

$a = (24 - 3) \cdot 4^{-1} \bmod 27 = 21 \cdot 7 \bmod 27 = 147 = 12$

Para descifrar, hay que calcular

$a^{-1} \bmod 27 = 12^{-1} \bmod 27 =$ ¡NO EXISTE! pues mcd(12, 27) no es 1

CRIPTOANÁLISIS DE CRIPTOGRAFÍA CLÁSICA

- Rompiendo el Cifrado de Sustitución Monoalfabeto (supuesto transformación afín)

Podríamos seguir suponiendo que A (0) → X (24) pero buscar otra pareja de letras para plantear la otra ecuación. Por ejemplo, A (0) → X (24), S (19) → K (10).

Suposición 3: A (0) → X (24), S (19) → K (10)

$10 = a \cdot 19 + b \text{ mód } 27$

$24 = a \cdot 0 + b \text{ mód } 27$

Luego

$b = 24$

$a = (10 - 3) \cdot 19^{-1} \text{ mód } 27 = 7 \cdot 10 \text{ mód } 27 = 70 = 16$

Para descifrar, hay que calcular

$a^{-1} \text{ mód } 27 = 16^{-1} \text{ mód } 27 = -5 = 22$

CRIPTOANÁLISIS DE CRIPTOGRAFÍA CLÁSICA

- Rompiendo el Cifrado de Sustitución Monoalfabeto

Para descifrar, hay que aplicar $m_i = (c_i - b) \cdot a^{-1}$ mód 27

(carácter cifrado – 24) * 22 mód 27 = carácter claro

Obtenemos que el texto cifrado siguiente:

UEYDXTHWYDWXLEXCDXCYDLKXJSKTCWTKXUWLEXJSEOLDPKXYDLDVKPDUIWUKLXWÑHDSDWXKJSEOKS

Se descifra al siguiente texto en claro:

OSVXATEFVXFALSACXACVXLPAUYPTCFTPAOFLSAUYSRLXNPAVXLXKPNXOZFOPLAFWEXYXFAPUYSRPY

Que no tiene ningún sentido…

Debemos seguir probando parejas

CRIPTOANÁLISIS DE CRIPTOGRAFÍA CLÁSICA

- Rompiendo el Cifrado de Sustitución Monoalfabeto (supuesto transformación afín)

Podríamos probar muchas opciones entre las posibles (solo considerando las tres más frecuentes en texto en claro y texto cifrado):

	Claro	Cifrado
Sup. 1	E, A	D, X
Sup. 2	E, A	X, D
	E, A	D, K
	E, A	K, D
	E, A	X, K
	E, A	K, X

	Claro	Cifrado
	A, S	D, X
	A, S	X, D
	A, S	D, K
	A, S	K, D
Sup. 3	A, S	X, K
	A, S	K, X

Claro	Cifrado
E, S	D, X
E, S	X, D
E, S	D, K
E, S	K, D
E, S	X, K
E, S	K, X

CRIPTOANÁLISIS DE CRIPTOGRAFÍA CLÁSICA

- Rompiendo el Cifrado de Sustitución Monoalfabeto (supuesto transformación afín)

Por acortar, vamos a probar con la "buena"

Suposición 4: A (0) → K (10), S (19) → X (24)

$24 = a \cdot 19 + b \text{ mód } 27$

$10 = a \cdot 0 + b \text{ mód } 27$

Luego

$b = 10$

$a = (24 - 10) \cdot 19^{-1} \text{ mód } 27 = 14 \cdot 10 \text{ mód } 27 = 140 = 5$

Para descifrar, hay que calcular

$a^{-1} \text{ mód } 27 = 5^{-1} \text{ mód } 27 = 11$

CRIPTOANÁLISIS DE CRIPTOGRAFÍA CLÁSICA

- Rompiendo el Cifrado de Sustitución Monoalfabeto

Para descifrar, hay que aplicar $m_i = (c_i - b) \cdot a^{-1}$ mód 27

(carácter cifrado – 10) * 11 mód 27 = carácter claro

Obtenemos que el texto cifrado siguiente:

UEYDXTHWYDWXLEXCDXCYDLKXJSKTCWTKXUWLEXJSEOLDPKXYDLDVKPDUIWUKLXWÑHDSDWXKJSEOKS

Se descifra al siguiente texto en claro:

NO DESCUIDEIS LOS TEST DE LAS PRACTICAS NI LOS PROBLEMAS DEL EXAMEN FINAL SI QUEREIS APROBAR

Que ahora sí que tiene sentido

CRIPTOANÁLISIS DE CRIPTOGRAFÍA CLÁSICA

- Cifradores sustitución monoalfabeto
  - La frecuencia de los caracteres del texto en claro se transmite al texto cifrado
  - Necesario contar con texto cifrado de longitud significativa

    evitar lipogramas (se omite una letra o varias): *La Disparition* de Georges Perec traducido como *A Void* o *El secuestro* en español
    Le Train de Nulle Part, 2004 de Michel Dansel, no usa ni un solo verbo.
  - Si es desplazamiento puro: hay 1 incógnita (*b*) {a=1}

    Carácter de + frecuencia en alfabeto texto en claro (E ó A) ←→carácter de + frecuencia en texto cifrado
  - Si es transformación afín: hay 2 incógnitas (*a* y *b*)

    2 c. con + frec. aparición ←→c.+ frec. en texto cifrado
  - Si es asignación arbitraria: Hay tantas incógnitas como letras del alfabeto

CRIPTOANÁLISIS DE CRIPTOGRAFÍA CLÁSICA

- **Rompiendo el cifrador de sustitución polialfabeto periódica: Vigènere**

¿Puede romperse?

El método de KASISKI

Ejemplo:

Mensaje	thes unan dthe mani nthe moon
Clave	KING KING KING KING KING KING
Cifra	DPRY EVNT NBUK WIAO XBUK WWBT

8 saltos

Grupos recurrentes y seles tamaño

→ Hay una distancia de 8 entre ambas repeticiones

→ Es posible que sea porque "hay un número entero de claves entre ambas"

→ La distancia es múltiplo de la longitud de la clave

→ == la longitud de la clave divide la distancia

CRIPTOANÁLISIS DE CRIPTOGRAFÍA CLÁSICA

- El método de KASISKI

  Pasos:

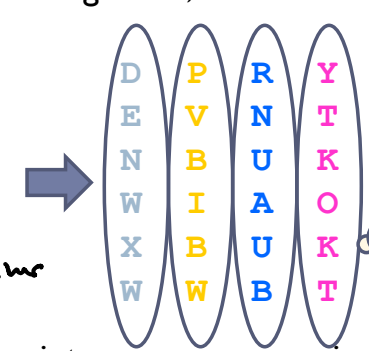
  - Buscar repeticiones de cadenas de caracteres en el criptograma. (ejem: BUK)
  - Medir la distancia entre las mismas
  - **L = longitud de la clave = DIVISOR MÁS COMÚN ENTRE TODAS LAS DISTANCIAS**

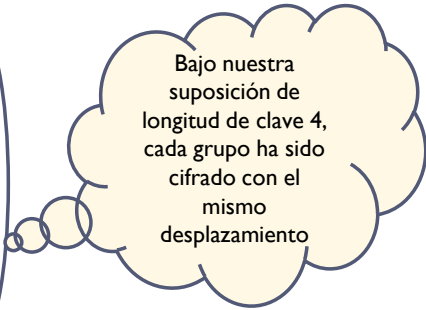
    (si simplificamos y asumimos que todas las repeticiones en el texto cifrado se deben a coincidencias de fragmentos de texto en claro con el mismo fragmento de la clave, la longitud de la clave sería el m.c.d.(conjunto de distancias entre cadenas repetidas), pero no tiene porqué ser verdad siempre)
  - Dividir el criptograma en subcriptogramas de longitud L, cifrados con la misma letra de la clave:

    Imaginemos que en el ejemplo suponemos que la longitud de la clave es 4 (que lo es):

    DPRY EVNT NBUK WIAO XBUK WWBT

    Las separas por supuesto tamaño clave y haces estudio estadístico de cada uno

  - Realizamos análisis de frecuencia en cada subcriptograma para averiguar el desplazamiento

CRIPTOANÁLISIS DE CRIPTOGRAFÍA CLÁSICA

- Método de KASISKI. Ejemplo detallado

```
PBVRQ 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
OÑTGR RYVLP WJIFW XOTGG RPQRR JSKET XRNBL ZETGG NEMUO TXJAT
ORVJH RSFHV NUEJI BCHAS EHEUE UOTIE FFGYA TGGMP IKTBW UEÑEN
IEEU.
```

- Paso 1, buscar repeticiones:
  - 3 cadenas de **GGMP** → separadas por 256 y 104 caracteres
  - 2 cadenas de **YEDS** → separadas por 72 caracteres
  - 2 cadenas de **HASE** → separadas por 156 caracteres
  - 2 cadenas de **VSUE** → separadas por 32 caracteres
- Paso 2: m.c.d.=4

CRIPTOANÁLISIS DE CRIPTOGRAFÍA CLÁSICA

- Método de KASISKI. Ejemplo detallado
  - Paso 3: subcriptogramas

C1 = PQAAEPDMRÑEEDCNUSRIECNIONSAAETLUOLAUIEULMNIIEAAOOLUMNA
RSOMRSISERNAISIRTMDTOORLIORRENENOAVSNIAEOFAMTEI

C2 = BVDÑTSBPPPDÑPPPBFDPQBUFNUEZCDFBÑMBEÑSFNPBBÑBÑNMKDPFQF
SJFTBPUNJMBNGDUNUFPFSSÑRPFTPJTBTETTJFUBSUTFTPBÑE

C3 = VISSSIGSWWSDCQWZNMWVOEQMVIYESPHEEXEEEWMQRPMVISTMSWO
MOEWQWJWEQEGDISSETEGOOSETYWWGQSXLGMXOHHECEEIGGIWEE

C4 = RCKDJEGLRYDRRMKVVTUVVDLWRKEYEHGSHVPLVHCPRVTVDJJDEIZVHSR
CVGVXRUGGLJVEGEGRGTQGVJXGRKRZGUJRRVJHHUEYGKUNU

CRIPTOANÁLISIS DE CRIPTOGRAFÍA CLÁSICA

- Método de KASISKI. Ejemplo detallado
  - Paso 4: análisis de frecuencias

Se busca las letras equivalentes a E,A,O y S (las más frecuentes en castellano) :

Posibilidades para $k_{I:}$

A : m (mód. 27)
E : m+4 (mód. 27)
O : m+15 (mód. 27) S : m+19 (mód. 27)

Frecuencias observadas:

	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_1	11	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_2	0	14	1	6	4	12	1	0	0	4	1	0	3	6	8	6	14	2	1	6	9	7	1	0	0	0	1
C_3	0	0	1	2	18	0	7	3	7	1	0	1	7	1	0	0	2	6	1	12	3	0	3	12	3	2	1
C_4	0	0	3	5	7	0	12	6	1	7	5	4	1	1	0	6	2	1	13	2	3	7	14	0	2	3	2

CRIPTOANÁLISIS DE CRIPTOGRAFÍA CLÁSICA

- Método de KASISKI. Ejemplo detallado

  Apariciones encontradas en el orden de distancias:

  C_1: A
  C_2: B
  C_3: E
  C_4: R

  Clave puede ser: ABER

- Paso 5, comprobación:

Cifra	PBVRQ VICAD SKAÑS DETSJ PSIED BGGMP SLRPW
Clave	ABERA BERAB ERABE RABER ABERA BERAB ERABE
Mensaje	PARAQ UELAC OSANO MESOR PREND ACOMO OTROS

CRIPTOANÁLISIS DE CRIPTOGRAFÍA CLÁSICA

- Cifradores sustitución polialfabeto periódica
  - Determinar el número de alfabetos utilizados
    (e.d. longitud de la clave o periodo)
  - Separar el texto en partes cifradas con el mismo alfabeto
    (y criptoanalizar como Vigènere)
  - Método Kasiski para descubrir el periodo:
    - Buscar grupos de caracteres repetidos en el texto cifrado
    - Pueden corresponder a grupos comunes en el lenguaje del texto en claro (castellano: -as, -es, -ción, co-, in-, con, de, -ando, -ada, -ido, -ado, -mente)
    - Periodo ¿=? m.c.d. (diferencias relativas en posición dentro del texto cifrado para un mismo grupo)

CRIPTOANÁLISIS DE CRIPTOGRAFÍA CLÁSICA

- RECUERDA
  - Criptoanálisis cifradores sustitución monoalfabeto
    - Redundancia del lenguaje
    - Análisis de frecuencias.
      - Transformación afín
      - Si asignación arbitraria, búsqueda de emparejamientos uno a uno según frecuencias
  - Criptoanálisis cifradores sustitución polialfabeto periódica
    - Determinar el número de alfabetos utilizados (e.d. longitud de la clave o periodo)
    - Separar el texto en partes cifradas con el mismo alfabeto (y criptoanalizar como Vigènere)
    - Método Kasiski para descubrir el periodo:
    - Buscar grupos de caracteres repetidos en el texto cifrado
    - Pueden corresponder a grupos comunes en el lenguaje del texto en claro (castellano: -as, -es, -ción, co-, in-, con, de, -ando, -ada, -ido, -ado, -mente)
    - Periodo ¿=? m.c.d. (diferencias relativas en posición dentro del texto cifrado para un mismo grupo)

CRIPTOANÁLISIS DE CRIPTOGRAFÍA CLÁSICA

- Índice de Coincidencia (IC)
  - El Índice de Coincidencia (IC) es una medida estadística sobre un texto.

    El IC fué inventado por William Friedman y presentado en The Index of Coincidence and its Applications in Cryptography (1920)

  - El IC es la probabilidad de que dos letras (seleccionadas aleatoriamente) de un texto sean la misma

Imagine un sombrero con las 27 letras del alfabeto.

→ La probabilidad de sacar una A es 1/27.

Imagine dos sombreros.

→ La probabilidad de sacar dos As simultáneamente es (1/27)*(1/27)

La probabilidad de sacar dos letras cualesquiera iguales es

→ 27*(1/27)*(1/27) = (1/27) = 0.037

Luego el IC de un conjunto de letras distribuido aleatoriamente (uniformemente) es 0.037

CRIPTOANÁLISIS DE CRIPTOGRAFÍA CLÁSICA

- Índice de Coincidencia (IC)

Suponga que llenamos un sombrero con 100 letras. Y que introducimos cada letra tantas veces como su frecuencia en Español (es decir, 13 Es, 10 As, 8 S, etc.).

La probabilidad de sacar dos letras iguales sería

$$(^{13}/_{100})*(^{12}/_{99}) + (^{10}/_{100})(^{9}/_{99}) + (^{8}/_{100})(^{7}/_{99}) + \ldots = 0.0775 \quad \leftarrow \text{IC del Español}$$

Cada lenguaje tiene un IC:

Español:	0.0775	Inglés:	0.0667
Ruso:	0.0529	Alemán:	0.0762

- Cálculo del IC

$$\frac{\sum(f_i * (f_i - 1))}{N(N-1)}$$

para $0 \geq i \geq 26$,

f_i es la frecuencia (n° de apariciones) de la letra i-ésima del alfabeto, en el texto analizado

y N es el n° de letras del texto analizado

CRIPTOANÁLISIS DE CRIPTOGRAFÍA CLÁSICA

- IC. EJEMPLO DE CÁLCULO

  - El IC del texto "EL INDICE DE COINCIDENCIA" es :

    a(1*0)+ c(4*3)+ d(3*2)+ e(4*3)+ i(5*4)+ l(1*0)+ n(3*2)+ o(1*0) = 56

    dividido por N*(N-1) = 22*21 = 462

    lo que da un IC de 56/462 = 0.121

  - El IC del texto "BMQVSZFPJTCSSWGWVJLIO" es :

    b(1*0)+ c(1*0)+ f(1*0)+ g(1*0)+ i(1*0)+ j(2*1)+ l(1*0)+ m(1*0)+ o(1*0) + p(1*0)+ q(1*0)+ s(3*2)+ t(1*0)+ v(2*1)+ w(2*1)+ z(1*0) = 12

    dividido por N*(N-1) = 21*20 = 420

    que da un IC de 12/420 = 0.0286

CRIPTOANÁLISIS DE CRIPTOGRAFÍA CLÁSICA

- ÍNDICE DE COINCIDENCIA
  - ¿PARA QUE SIRVE EL IC?
    - Distinguir texto cifrado de texto en claro
    - Encontrar la longitud de la clave de cifrado de Vigènere
  - ¡¡Un cifrado de sustitución monoalfabeto no altera el IC de un texto!!
    - IC('MITIATIENEBIGOTE') = 0.1
    - IC('PLWLDWLHQHELJRWH') = 0.1

CRIPTOANÁLISIS DE CRIPTOGRAFÍA CLÁSICA

- IC Y VIGÈNERE

  - Vigènere = varias sustituciones simples tipo desplazamiento puro:

MITIATIENEBIGOTE

LIOLIOLIOLIOLIOL

XQHTIHTMBPJWRWHP

CRIPTOANÁLISIS DE CRIPTOGRAFÍA CLÁSICA

- IC Y VIGÈNERE

  - Vigènere = varias sustituciones simples tipo desplazamiento puro:

MITIATIENEBIGOTE

LIOLIOLIOLIOLIOL

XQHTIHTMBPJWRWHP

IC(XQHTIHTMBPJWRWHP) = 0.05

1 en 1

CRIPTOANÁLISIS DE CRIPTOGRAFÍA CLÁSICA

- IC Y VIGÈNERE
  - Vigènere = varias sustituciones simples tipo desplazamiento puro:

MITIATIENEBIGOTE
LIOLIOLIOLIOLIOL
XQHTIHTMBPJWRWHP

2 en 2 → IC(XHITBJRH) = 0.035
Al revés IC(QTHMPWWP) = 0.071

CRIPTOANÁLISIS DE CRIPTOGRAFÍA CLÁSICA

- IC Y VIGÈNERE
  - Vigènere = varias sustituciones simples tipo desplazamiento puro:

MITIATIENEBIGOTE
LIOLIOLIOLIOLIOL
XQHTIHTMBPJWRWHP

3 en 3

IC(XTTPRP) = 0.133
IC(QIMJW) = 0
IC(HHBWH) = 0.3

CRIPTOANÁLISIS DE CRIPTOGRAFÍA CLÁSICA

- IC Y VIGÈNERE
  - Texto cifrado:

RIPTCICXVRTFCWFDRKTOAFGNOSUFLZPJGSWRONHRTFQZGXGRZCCUXLFEUWZOHCGTDGYJLHTHKKCTMVLQDHHSQ
XNQLBXHISSHMGLGRLKISAIUZWBJUVBHYPLGEUPVZAIEVFGYEACTMNVGHCOWGDHRVFFOGUWBIFVEJYOPTPGKSWPMG
HZDMRHRXFNHGEYTVCSCQJCBIULJTYUJFXNQSCHMKTDHIPKSKYTKOSGGJFTUEVBUFKJHDUUPEJYRVFBCUOITPQZOBUT
PZAIULGRLKIWGYNVGHCOWGDHULBUCPSSHXGJWPKWLQDHOVHXPQKSAURYCMCOHZAYIHRPXGSOEYNPQJFCKSAIU
ZWBJUVBHMGLBILGCWHNQHAPNVNFDYPPBVXQURTLGCSAIXHFXIUZSRLGACHHQZCAIUVPGYNHDTFKJIAUUPBDMQIF
TUNNICIUKSAIUTWHNGYWDMSBSWUPLLXMVPRDUNVZPLIVRTNQKOAUJPGIITPOSYNHQPLKJOIOTHMSYEPRXWQTDPLV
PFAUEVBIIFVGJMVLRTMCTOCNGZRTFQZGXGRZCCMRBSSYUZSGWNHJPXGYFXGQJCBIAVCHCOWZTGGUHTPGYZDMQJ
OHCQUOAGGUHTJGYCCIEVBDTEVOCUFPSFOGVRXYCSCHMKTDHIPZFTWWLFSUPLZRURPHJFQKSAWWTDAYCUCHXGS
WHUFVBSYWUZDKWPHDKWLXJLCXITYUTWRBCLZYUERGDHNLQDGRVBTOPHQPHEPCCJWLGHCFLGEOGZRTNCUHD
MCUCHMGJCCZKYAPKWLGXZWLAXWJHSADCJYHIPLZFOGSSELGZHDFCCCOUGZSEYTZCCULLFTWWLFSUPACSIUSCHA
CNGRUFHEJYEYSTGQZEJYRVFUCPZOQLGTCHYPXITJCYHTXGLGIUFVGJHKKCHMGLBROGUHGUUWFXHIMWTFFWITMCO
CGUGUZPJGSWRONHGTLGCSAUTHHTHGTCHOPTINVWLBRBKZHTMQIFTYNSCEYTVFTWWLFSYPXITYUBBRBKZHTKWL
GXJQYGTLRLZXWWSOKYTLADMCSUDKWLBDMGWITXCVEJYPVVPSCTCHPKZHDYPASAYXPGXIPCSGYOVGSYUUISIUWC
QLGTOGAGJCCNGZHDATVSCCPNGTUESOGUTVBSIUYIBITLGFOGTOSIPUOPJCYSRYTPOTHNHGTLKLMTFVLAPXGSOEYNP
QJFCNFDYPPBVYZWZXWQHZVOKLBAYRYSVOPACPOPVRTFQZSHWTPHDLGZRTKWLGTNTHHPLKHZPJGSWRONHMSYD
YCBUEVBIYUACQUTADTLFLFPMWCWGAKUWSUFHAQIUYIBITLGHIPMOAMQZGDVTLGJWCWWIONVTPPQYWIIOHHIXK
QCBYIBGIUOBQWIGSRTZTHBZATPATMEBOAYULGT

Longitud: 1416 caracteres

Suposición: en Español

Probamos longitudes de clave: de 1 a 10

CRIPTOANÁLISIS DE CRIPTOGRAFÍA CLÁSICA

- IC Y VIGÈNERE
  - Probamos longitudes de clave: de 1 a 10

IC Español: 0.0775

Tiene el IC más parecido. Averiguamos long. clave.

Después con Kasiski cogrupos de 5

CLAVE DE 1 CARACTERES: 1:0,0426

CLAVE DE 2 CARACTERES: 1:0,0443, 2:0,0416

CLAVE DE 3 CARACTERES: 1:0,0422, 2:0,0421, 3:0,0441

CLAVE DE 4 CARACTERES: 1:0,0427, 2:0,0412, 3:0,0448, 4:0,0422

CLAVE DE 5 CARACTERES: 1:0,0739, 2:0,074, 3:0,0746, 4:0,0763, 5:0,0722

CLAVE DE 6 CARACTERES: 1:0,0419, 2:0,0396, 3:0,0455, 4:0,0422, 5:0,0454, 6:0,0415

CLAVE DE 7 CARACTERES: 1:0,0404, 2:0,0434, 3:0,0423, 4:0,0426, 5:0,0389, 6:0,0438, 7:0,0458

CLAVE DE 8 CARACTERES: 1:0,0398, 2:0,0412, 3:0,0458, 4:0,0424, 5:0,0429, 6:0,0401. 7:0,0444, 8:0,0404

CLAVE DE 9 CARACTERES: 1:0,0442, 2:0,0388, 3:0,041, 4:0,043, 5:0,0452, 6:0,0437, 7:0,0381, 8:0,0409, 9:0,0425

CLAVE DE 10 CARACTERES: 1:0,0739, 2:0,0705, 3:0,0767, 4:0,0662, 5:0,0735, 6:0,076, 7:0,0791, 8:0,0686, 9:0,0862, 10:0,0687

CRIPTOANÁLISIS DE CRIPTOGRAFÍA CLÁSICA

- IC Y VIGÈNERE

  Clave: "PUCHO"

  - Texto descifrado:

CONMOTIVODELAPROXIMALLEGADADELAPELICULADELOSSIMPSONAVERPAUSASIEMPREHETENIDOESTECO
NFLCITOENINGLESSEESCRIBELOSSIMPSONSENESPANOLLOCORRECTOESLOSSIMPSONPORQUENIMODOQUEMIFAMILIA
SEALOSPADILLASPEROODIOCOMOSEVEESCRITOLOSSIMPSONDEVERDADMECREACONFLICTOASIQUEPORMISHUEVOS
AMARILLOSESCRIBIRELOSSIMPSONSENFINLESDECIAQUECONMOTIVODELAPROXIMALLEGADADELAPELICULADELOSSI
MPSONSSEENTREVISTOAMATTGROENINGDONDEREVELOVARIOSSECRETOSNOSOLOSOBRELAPELICULASINOSOBREAL
GUNOSDELOSMISTERIOSQUEHANEXISTIDOALOLARGODETODALAHISTORIADELACARICATURAYDECIDICOMPARTIRL
ACONTODOSUSTEDESAMANTESDELOSSIMPSONSPUEDESSERCLAVADERRIMOCOMOYOOSIMPLEMENTEVERLOSOCASI
ONALMENTEPERONOCONOZCOANADIEQUEODIEALOSSIMPSONSRECUERDANELCAPITULODELCUMPLEANOSDELISA
DONDEUNLOQUITOQUEJURAQUEESMICHAELJACKSONLECOMPONEUNACANCIONPUESSIDESPUESDETANTOSANOSS
ECONFIRMAQUESIFUEMICHAELJACKSONELQUELEPRESTOLAVOZAESEPERSONAJERECUERDANTODOSLOSGAGSCADA
QUECREEMOSQUEPORFINSABREMOSENQUEPARTEDEESTADOSUNIDOSSEENCUENTRASPRINGFIELDPUESAHORAENLA
PELICULASEREVELARATENEMOSUNMUYBUENCHISTESOBREELLOPERORECUERDENQUEESUNCHISTEQUESIPORSERPELI
CULAVEREMOSALGOQUENOSEPUEDAOQUENOHAYAMOSVISTOENTELEVISIONVEREMOSDESNUDOSPOBREMARGECO
NTESTOGROENINGSEACLARARONDOSRUMORESQUEMADONNAAPARECERIAENLASERIEYELTEMADELAPELICULAGRO
ENINGEXPLICOALGUIENLEPREGUNTOAUNODELOSESCRITORESDEQUESETRATARIALAPELICULAYDEBROMACONTEST
OBARTPERDERASUVIRGINIDADAMBOSRUMORESSONFALSOSSOBRESUCAPITULOFAVORITOMATTDIJOMEGUSTAMUCH
OELDEFRANKGRIMESCUALESESE