



Universidad
Carlos III de Madrid

COSEC LAB · Dpto. Informática

Universidad Carlos III de Madrid

Criptografía Clásica

CSI
Curso 2016/2017

Almudena Alcaide Raya

Ejercicios Criptografía Clásica.

(Obs: Considérese el alfabeto en castellano en mayúsculas de 27 caracteres).

$$27 \cdot 3^2 \quad \phi(3^2) = 3^2 \cdot 2 = 18 \quad 7^{-1} = 7^{17} \pmod{27} = 7^{16} \cdot 7 \pmod{27} = 7 \cdot 16 \pmod{27} = 4 \pmod{27}$$

✓ 1. Dada la función de cifrado $E(m) = 7m + 3 \pmod{27}$ se pide: A 0 / B 1 / ... / Z 26

a. Valores de las constantes de decimación y desplazamiento.

b. Cifrar el mensaje "TERCERA" 8/4/21/17/4/21/3 I E U Q E U D

c. Descifrar el mensaje "DID ÑOE"

$$D(m) = (m - 3) 7^{-1} \pmod{27} = 4m - 12 \pmod{27}$$

49 4 13 16 5	3 → 0 A	14 → 17 Q	
38 3 14 15 4	8 → 20 T	15 → 21 U	ATAQVE
	3 → 0 A	4 → 4 E	

2. Dada la clave "LUCI" cifrar el siguiente mensaje mediante el método de Vigenere. M= "CAMINERO".

3. Dada la clave "PLUS" descifrar el siguiente mensaje sabiendo que fue cifrado mediante el método de Vigenere. C= "LSAW COMW".

4. Dada la clave "ALA" descifrar el siguiente mensaje sabiendo que fue cifrado mediante el método de Vigenere con Autoclave. C= "EDVI KVQG".

5. Dada la clave "MARTES" cifrar el siguiente mensaje mediante el método de Playfair. M= "FALSO PUENTE".

6. Dada la clave "MARTES" descifrar el siguiente mensaje sabiendo que fue cifrado mediante el método de Playfair. C= "FOMUMB ZFTERZ".

7. Dada la matriz clave $K = \begin{bmatrix} 3 & 2 \\ 4 & 6 \end{bmatrix}$ se pide:

a. Valorar si la matriz reúne las condiciones para utilizarse como clave en un método de sustitución polígrafa de Hill.

b. Cifrar el mensaje M= "RECORDAR" mediante el método de Hill.

8. Dada la matriz clave $K = \begin{bmatrix} 7 & 6 \\ 3 & 11 \end{bmatrix}$

Se pide descifrar el mensaje C= "J8D6 L4N3" sabiendo que el alfabeto utilizado es {A,...,Z} + {0,...,9}.

9. Habiendo utilizando la siguiente permutación KP= (642135) se pide descifrar el mensaje C= "OOEMTDIACSLSEEOCSE"

6 4 2 1 3 5 | 6 4 2 1 3 5

MÉTODOS SCIASI COSEEE = MÉTODOS CLÁSICOS

2) CAMI NERO
LUCI LUCI

CAMINERO \Rightarrow NUNPYZTW

NUNP XYTW

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

3) ZSAW COMW \Rightarrow VIGENERE
PLUS PLUS
VIGE NERE

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

4) EDUI KUVQ G

Mixando tabla alfabetica como esta pero la clave a la propia cadena

Le va escribiendo la cadena descifrada como clave.

ALAE SVER
ESVERANO

ES VERANO

5) MARTES

α α → ↓ α α
FALSO PUENTEX
BE GF PQ ZF QH RZ

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

→ / Opuesto vertical
Espejo → es

B E G F P Q Z F Q M R Z

Revisa

α el opuesto en la vertical
en el cuadro que forman la ds
A R T E
B C D F

6) MARTE

FOMUMB ZFTERZ \Rightarrow BUENA SUERTE X
BU VERT EX
ENAS EX

→ / opuesto vertical
Espejo
Endiagonal es endiagonal.
M A R T E
S B C D F
G H I J K L
N O P Q U
V W X Y Z

7) $k = \begin{pmatrix} 3 & 2 \\ 4 & 6 \end{pmatrix}$ Invertible $|k| \neq 0 = \det(k)$

RE CO RD AR = 10JQGJJA
184 215 183 018
10 JQ GS JA

$$\begin{pmatrix} C_1 \\ C_2 \end{pmatrix} = \begin{pmatrix} 3 & 2 \\ 4 & 6 \end{pmatrix} \begin{pmatrix} 18 \\ 4 \end{pmatrix} = \begin{pmatrix} \quad \\ \quad \end{pmatrix} \mod 27 \quad \begin{pmatrix} C_3 \\ C_4 \end{pmatrix} = \begin{pmatrix} 3 & 2 \\ 4 & 6 \end{pmatrix} \begin{pmatrix} 2 \\ 15 \end{pmatrix} = \begin{pmatrix} 6+30 \\ 8+90 \end{pmatrix} \mod 27$$

$$\begin{pmatrix} C_5 \\ C_6 \end{pmatrix} = \begin{pmatrix} 18 \\ 3 \end{pmatrix} = \begin{pmatrix} \quad \\ \quad \end{pmatrix} \mod 27 \quad \begin{pmatrix} C_7 \\ C_8 \end{pmatrix} = \begin{pmatrix} 0 \\ 18 \end{pmatrix} = \begin{pmatrix} \quad \\ \quad \end{pmatrix} \mod 27$$

$$8) \quad k = \begin{pmatrix} 7 & 6 \\ 3 & 11 \end{pmatrix} \quad |k| = 59 \neq 0$$

Descifrar = J8 D6 L4 N3
AT LA 2F A6

37 = 27 letras + 10 números
a-9 0-9

$$k^{-1} = \frac{1}{\det(k)} \quad k^T = \frac{1}{59} \begin{pmatrix} 11 & -6 \\ -3 & 7 \end{pmatrix} \pmod{37} = 59^{-1} \begin{pmatrix} 11 & -6 \\ -3 & 7 \end{pmatrix} \pmod{37} = 32 \begin{pmatrix} 11 & -6 \\ -3 & 7 \end{pmatrix} \pmod{37} \quad k^{-1}$$

$$\begin{pmatrix} 7 & 6 \\ 3 & 11 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \cdot \\ \cdot \end{pmatrix}$$

$$M = 32 \begin{pmatrix} 11 & -6 \\ -3 & 7 \end{pmatrix} \begin{pmatrix} 9 \\ 35 \end{pmatrix} \pmod{37} = \begin{pmatrix} \cdot \\ \cdot \end{pmatrix} = \begin{matrix} A \\ T \end{matrix} \begin{pmatrix} 0 \\ 20 \end{pmatrix}$$

~~$$59^{-1} = 59^{36} \pmod{37}$$~~

$$59^{-1} = 32 \pmod{37}$$

$$M = 32 \begin{pmatrix} 11 & -6 \\ -3 & 7 \end{pmatrix} \begin{pmatrix} 3 \\ 33 \end{pmatrix} \pmod{37} = \begin{pmatrix} \cdot \\ \cdot \end{pmatrix} = \begin{matrix} L \\ A \end{matrix}$$

$$M = 32 \begin{pmatrix} 11 & -6 \\ -3 & 7 \end{pmatrix} \begin{pmatrix} 11 \\ 34 \end{pmatrix} \pmod{37} = \begin{pmatrix} \cdot \\ \cdot \end{pmatrix} = \begin{matrix} 29 \\ 8 \end{matrix}$$

$$M = 32 \begin{pmatrix} 11 & -6 \\ -3 & 7 \end{pmatrix} \begin{pmatrix} 13 \\ 30 \end{pmatrix} \pmod{37} = \begin{pmatrix} \cdot \\ \cdot \end{pmatrix} \pmod{37} = \begin{matrix} 0 \\ 31 \end{matrix} \begin{matrix} A \\ 6 \end{matrix}$$

10. Habiendo utilizado una transposición con 5 filas de recorrido en zig-zag descifre el siguiente criptograma: C="PISOML AROPTS LEEOS"

S C E O = S C E O E R T

11. Cifre mediante una transposición columnar de 4 columnas el siguiente texto M="FIESTA NACIONAL".

10)

P		I		S
O	M	L		A
R	O	P		T
S	L	E	E	

PORSOLOMIL PESETAS

Zig-zag

1	→	9	→	17
2	→	8	→	16
3	→	7	→	15
4	→	6	→	14
5	→	13		

11)

F		T		C		A		
I		A		I		L		
E		N		O		X		
S		A		N		X		

= FTCAIAILENOX SANX