



“Criptografía clásica”

Ejercicios propuestos

Ejercicio 1 :

Dada la función de cifrado $E(m)=7m+3 \text{ Mod.}27$ se pide

- a) Valores de las constantes de decimación y desplazamiento
- b) Cifrar el mensaje “TERCERA”
- c) Descifrar el mensaje “DID ÑOE”

Solución:

- a) Constante de decimación = 7; constante de desplazamiento =3
- b)

$$E("T") = E(20) = 20 \cdot 7 + 3 \pmod{27} = 8 = "I"$$

$$E("E") = E(4) = 4 \cdot 7 + 3 \pmod{27} = 31 \pmod{27} = 4 = "E"$$

Así se procedería con todas las letras hasta obtener el texto: “IEUQ EUD”

- c) Lo primero que hay que hacer es obtener la ecuación de descifrado:

$7^{-1} \pmod{27} = 4$. Por lo tanto, la expresión para el descifrado es

$$D(c) = 4(c - 3) \pmod{27} = 4c - 12 \pmod{27} = 4c + 15 \pmod{27}$$

$$D("D") = E(3) = 4 \cdot 3 + 15 \pmod{27} = 0 = "A"$$

$$D("I") = E(8) = 4 \cdot 8 + 15 \pmod{27} = 20 = "T"$$

Así se procedería con todas las letras hasta obtener el texto: “ATAQUE”

Ejercicio 2:

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

Solución:

NUÑPXYTW

Ejercicio 3:

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

Solución:

VIGENERE

Ejercicio 4:

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

Solución:

Al ser Vigenere con autoclave no es posible descifrar de forma directa, sino que es necesario ir descifrando poco a poco:

EDVI KVQG
ALA

ESV

EDVI KVQG
ALAE SV

ESVE RA

EDVI KVQG
ALAE SVER

ESVE RANO

Ejercicio 5:

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

Solución:

BE GF PQ ZF QM RZ

Considere que la matriz utilizada es:

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

Ejercicio 6:

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

Solución:

BUENA SUERTE X

La matriz es equivalente a la del ejercicio anterior.

Ejercicio 7:

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

- Valorar si la matriz reúne las condiciones para utilizarse como clave ne un método de sustitución polígrafa de Hill.
- Cifrar el mensaje M="RECORDAR" mediante el método de Hill.

Solución:

- $\det(K)=10 \neq 0$ y $\text{mcd}(\det(K), 27) =1$, la matriz es una clave válida.
- C="IOJQ GJJA"

El mensaje a cifrar se convierta a decimal y en pares de letras se multiplica por la matriz K indicada.

Ejercicio 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 $\{A,...,Z\}+\{0,...,9\}$.

Solución:

- "ATLA 2FA6"

Tenga en cuenta que para el descifrado se necesita calcular $M = C \times K^{-1}$, de modo que es necesario calcular la matriz inversa de K. Puede hacer uso de la fórmula $K^{-1} = |K|^{-1} \times (\text{adj}(K))^T \text{ mod } 37$

Ejercicio 9:

Habiendo utilizando la siguiente permutación $K_P = (642135)$ se pide descifrar el mensaje $C = \text{"OOEMTD IACSLS EEOCSE"}$

Solución:

OOEMTD IACSLS EEOCSE

1 234 5 6 123456 123456 → Hay que ordenar en función de la permutación indicada

$M = \text{"METODOS CLASICOS"}$

Ejercicio 10:

Cifre mediante una transposición columnar de 4 columnas el siguiente texto $M = \text{"FIESTA NACIONAL"}$

Solución:

$C = \text{"FTCAI AILENO XSANX"}$

La transposición sería:

F I E S

T A N A

C I O N

A L X X

El cifrado se corresponde con la concatenación de las columnas.