



Evaluación de conocimientos del primer parcial.

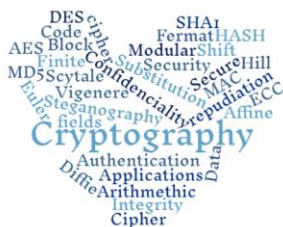
1. Clasifica el cifrador Atbash _____
2. Suponga que $\text{MCD}(a, n) = d$ con $d > 1$ entonces $a^{-1} \bmod n$ no existe, explique porque.
3. Find $\phi(9438) =$ _____
4. $111 \bmod 17 =$ _____ $-111 \bmod 17 =$ _____ $1/111 \bmod 17 =$ _____ $-1/111 \bmod 17 =$ _____
5. Cálcula: $17^{-1} \bmod 101$ utilizando el Algoritmo Extendido de Euclides.
6. The following ciphertext was encrypted by Affine Cipher VMBAON. The plaintext ends with ar. Decrypt the message. Show the Dk
7. The ciphertext XNQV was encrypted using the affine function $15p + 13$. Find the plaintext. Show the Dk
8. The ciphertext FRVSEUIW was encrypted using Vigenere cipher with the key *mars*. Find the plaintext Show the decryption key
9. Eve captures Bob's Hill cipher machine, which uses a 2×2 matrix $M \bmod 26$. She tries to find the key, she knows that the plaintext *dont* encrypts to *ELNI*. Find matrix K?
10. Using block cipher with CBC mode. Show that if an error occurs in the transmission of a block C_i , but all the others blocks are transmitted correctly. Show in a diagram which decrypted blocks affects?
11. Betito recibió la siguiente imagen bmp de 24 bits cifrada. Sabe que Alicia utilizó Hill $m=3$ cuya llave
11.- IV 26, 13, 9

$k = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 11 & 9 & 8 \end{pmatrix}$ y con el modo de operación CBC.

C1			C2		
40	171	36	236	184	95
C3			C4		
47	97	212	194	9	97

Ayuda a Betito a encontrar **P2** (al finalizar utiliza un generador de colores RGB para ilustrarlo).

M. en C. Nidia A. Cortez Duarte





Evaluación de conocimientos del primer parcial.

Sanchez Mendez Edmundo Josue

1. Clasifica el criptador Atbash.

2. Suponga que $\text{MCD}(a, n) = d$ con $d > 1$ entonces $a^x \text{ mod } n$ no existe, explique porque

R: Para que exista $a^x \text{ mod } n$ es necesario que a y n sean coprimos o primos relativos, lo cual se da por $\text{gcd}(a, n) = 1$ y además sabemos que si $\text{MCD}(a, n) = 1 \Rightarrow \text{gcd}(a, n) = 1$ es posible.

\therefore Como $\text{MCD}(a, n) = d$ y $d > 1$, $\Rightarrow a^x \text{ mod } n$ no existe.

3. Find $\phi(9438) = 2640$

$$\begin{array}{r|l} 9438 & 2 \\ 4719 & 3 \\ 1573 & 11 \\ 143 & 11 \\ 13 & 13 \\ 1 & \end{array}$$

$$\begin{aligned} \phi(9438) &= 2 \cdot 3 \cdot 11^2 \cdot 13 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) \left(1 - \frac{1}{11}\right) \left(1 - \frac{1}{13}\right) \\ &= 2 \cdot 3 \cdot 11^2 \cdot 13 \left(\frac{2-1}{2}\right) \left(\frac{3-1}{3}\right) \left(\frac{11-1}{11}\right) \left(\frac{13-1}{13}\right) \\ &= 11(2-1)(3-1)(11-1)(13-1) = \\ &= 11(1)(2)(10)(12) = 2640 \end{aligned}$$

4. $111 \text{ mod } 17 = 9$

$$\begin{array}{r} 6 \\ 17 \overline{) 111} \\ \underline{102} \\ 9 \end{array}$$

$$-111 \text{ mod } 17 = -9 \text{ mod } 17 = 8$$

$$1/111 \text{ mod } 17 = 1 \cdot 111^{-1} \text{ mod } 17 = 1 \cdot 9^{-1} \text{ mod } 17 = 2$$

$$111^{-1} \text{ mod } 17 = 9^{-1} \text{ mod } 17$$

$$17 = 9(1) + 8 \quad 8 = 17 - 9(1)$$

$$9 = 8(1) + 1 \quad 1 = 9 - 8(1)$$

$$8 = 1(8) + 0 \quad 1 = 9 - 17 + 9$$

$$1 = 9(2) + 17(-1)$$

Norma



Evaluación de conocimientos del primer parcial.

$$1 = 9(2) + 17$$

$$9 \bmod 17 = 2$$

$$-1/11 \bmod 17 = -1 \cdot 11^{-1} \bmod 17 = 16 \cdot 9^{-1} \bmod 17 = 16 \cdot 2 \bmod 17 = 32 \bmod 17$$

$$-1 \bmod 17 = 16$$

$$32 \bmod 17 = 15$$

$$-1/11 \bmod 17 = 15$$

$$6. VMBAON = C_n = 21 \ 12 \ 1 \ 0 \ 14 \ 13$$

$$a \ r \ g \ f \ t \ s = 0 \ 17 \ 6 \ 5 \ 19 \ 18$$

$$21 = \alpha \cdot 0 + \beta \bmod 26 \Rightarrow 21 = \beta \bmod 26 \Rightarrow \beta = 21$$

$$12 = \alpha \cdot 17 + \beta \bmod 26$$

$$12 = 17\alpha + 21 \bmod 26$$

$$(12 - 21) \bmod 26 = 17\alpha \bmod 26$$

$$-9 \bmod 26 = 17\alpha \bmod 26$$

$$17 = 17\alpha \bmod 26$$

$$1 = \alpha \bmod 26 \quad \alpha = 1$$

$$5^{-1} \bmod 26 = 1$$

$$26 = 1(25) + 1 \quad 1 = 1(25) + 26$$

$$1 = 1 \cdot 1$$

$$-25 \bmod 26 = 1$$

$$P_n = \alpha^{-1} [C_n + (\beta)] \bmod 26 = C_n + 5 \bmod 26$$

$$a = 1[21 + 5] \bmod 26 = 26 \bmod 26 = 0 \checkmark$$

$$r = 1[12 + 5] \bmod 26 = 17 \bmod 26 = 17 \checkmark$$

$$1 + 5 \bmod 26 = 6 \quad 0 + 5 \bmod 26 = 5$$

$$\begin{array}{l} \alpha = 1 \\ \alpha^{-1} = 1 \\ \beta = 21 \\ -\beta = 5 \end{array}$$



Evaluación de conocimientos del primer parcial.

$$14 + 5 \bmod 26 = 19$$

$$13 + 5 \bmod 26 = 18$$

$$D_K = \arg f_{13}$$

$$7 = C_K = X \cdot N \cdot Q \cdot V = 23 \ 13 \ 16 \ 21$$

$$C_N = 15p + 13 \ 18 \ 0 \ 21 \ 8$$

$$\alpha = 15 \quad \alpha^{-1} = 7$$

$$\beta = 13 \quad -\beta = 13$$

$$15^{-1} \bmod 26 = 7$$

$$26 = 15(1) + 11$$

$$15 = 11(1) + 4$$

$$11 = 4(2) + 3$$

$$4 = 3(1) + 1$$

$$3 = 1(3) + 0$$

$$1 = 15(3) - 4(26 - 11)$$

$$1 = 15(3) - 26(4) + 15(4)$$

$$1 = 15(7) + 26(-4)$$

$$15^{-1} \bmod 26 = 7$$

$$11 = 26 - 15(1)$$

$$4 = 15 - 11(1)$$

$$3 = 11 - 4(2)$$

$$1 = 4 - 3(1)$$

$$1 = 4 - 11 + 4(2)$$

$$1 = 4(3) - 11$$

$$1 = 3(15 - 11(1)) - 11$$

$$1 = 15(3) - 11(3) - 11$$

$$1 = 15(3) - 11(4)$$

$$P_N = 7[C_N + 13] \bmod 26$$

$$P_1 = 7(23 + 13) \bmod 26 = 252 \bmod 26 = 18$$

$$P_2 = 7(13 + 13) \bmod 26 = 182 \bmod 26 = 0$$

$$P_3 = 7(16 + 13) \bmod 26 = 203 \bmod 26 = 21$$

$$P_4 = 7(21 + 13) \bmod 26 = 238 \bmod 26 = 4$$

$$D_K = \text{save}$$



Evaluación de conocimientos del primer parcial.

8. FRVSEUW

K = mars

FRVSEUW = 5 17 21 18 4 20 8 22

K = marsmars = 12 0 17 18 12 0 17 18

~~-K = 14 0 9 8~~ = 14 0 9 8 14 0 9 8

$$P_1 = 5 + 14 \bmod 26 = 19 = t$$

$$P_2 = 17 + 0 = 17 = r$$

$$P_3 = 21 + 9 = 30 \bmod 26 = 4 = e$$

$$P_4 = 18 + 8 = 26 \bmod 26 = 0 = a$$

$$P_5 = 4 + 14 = 18 = s$$

$$P_6 = 20 + 0 = 20 = u$$

$$P_7 = 8 + 9 = 17 = r$$

$$P_8 = 22 + 8 = 30 \bmod 26 = 4 = e$$

Plaintext = ~~treasure~~

$$P = C_n + (-K) \bmod 26$$

9. dont

ELWI

$$K = \begin{pmatrix} 10 & 19 \\ 13 & 23 \end{pmatrix}$$

$$\begin{pmatrix} E & L \\ W & I \end{pmatrix} = \begin{pmatrix} d & 0 \\ n & 6 \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} \bmod 26$$

$$\begin{pmatrix} 4 & 11 \\ 13 & 8 \end{pmatrix} = \begin{pmatrix} 3 & 14 \\ 13 & 19 \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$



Evaluación de conocimientos del primer parcial.

$$1) 3a + 14c = 4$$

$$2) 13a + 14c = 13$$

$$(14 \cdot 13 - 3 \cdot 14)c = 13 \cdot 4 - 13 \cdot 3$$

$$125c = 13$$

$$c = 13 \cdot 125^{-1} \bmod 26 = 13 \cdot 5 \bmod 26 = 65 \bmod 26 = 13$$

$$125^{-1} \bmod 26 = 21^{-1} \bmod 26 = 5$$

$$26 = 21(1) + 5 \quad 5 = 26 - 21(1)$$

$$21 = 5(4) + 1 \quad 1 = 21 - 5(4)$$

$$5 = 1(5) + 0 \quad 1 = 21 - 4(26) + 21(4)$$

$$1 = 21(5) - 4(26)$$

$$21^{-1} \bmod 26 = 5$$

$$3a = 4 - 14 \cdot 13$$

$$a = -178 \cdot 3^{-1} \bmod 26 = 4 \cdot 4 \bmod 26 = 36 \bmod 26 = 10$$

$$-178 \bmod 26 = -22 \bmod 26 = 4$$

$$3^{-1} \bmod 26 = 9$$

$$26 = 3(8) + 2 \quad 2 = 26 - 3(8)$$

$$3 = 2(1) + 1 \quad 1 = 3 - 2(1)$$

$$2 = 1(2) + 0 \quad 1 = 3 - 26 + 3(8)$$

$$1 = 3(4) - 26$$

$$1) 4b + 11d = 11$$

$$2) 13b + 14d = 8$$

$$(13 \cdot 11 - 4 \cdot 14)d = 11 \cdot 13 - 8 \cdot 4$$

$$67d = 111$$

$$d = 111 \cdot 67^{-1}$$



Evaluación de conocimientos del primer parcial.

$$d = 111 \cdot 67^{-1} \bmod 26 = 7 \cdot 7 \bmod 26 = 49 \bmod 26 = 23$$

$$111 \bmod 26 = 7$$

$$67^{-1} \bmod 26 = 15^{-1} \bmod 26 = 7$$

$$d = 23$$

$$26 = 15(1) + 11 \quad 11 = 26 - 15(1)$$

$$15 = 11(1) + 4 \quad 4 = 15 - 11(1) \checkmark$$

$$11 = 4(2) + 3 \quad 3 = 11 - 4(2) \checkmark$$

$$4 = 3(1) + 1 \quad 1 = 4 - 3(1) \checkmark$$

$$3 = 1(3) + 0 \quad 1 = 4 - 11 + 4(2)$$

$$1 = 4(3) - 11$$

$$1 = 15(3) - 11(3) + 1$$

$$1 = 15(3) - 11(4)$$

$$1 = 15(3) - 26(4) + 15(4)$$

$$1 = 15(7) + 26(-4)$$

$$13b + 14 \cdot 23 = 8$$

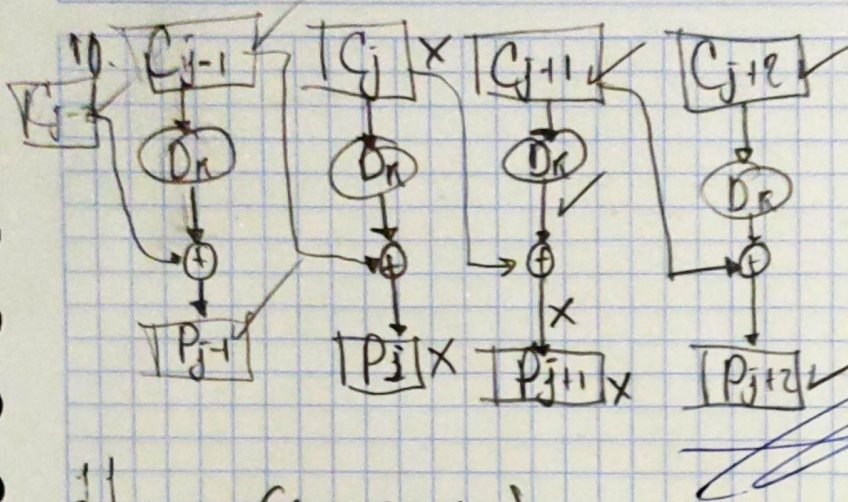
$$13b = 1 - 124$$

$$b = -33 \bmod 26 = -7 \bmod 26$$

$$b = 19$$



Evaluación de conocimientos del primer parcial.



$$K^{-1} = \begin{pmatrix} 96 & 167 & 1 \\ 74 & 179 & 254 \\ 177 & 81 & 1 \end{pmatrix}$$

$$P_2 \Rightarrow P_L \text{ y } C_2$$

$$(236, 184, 95) \begin{pmatrix} 96 & 167 & 1 \\ 74 & 179 & 254 \\ 177 & 81 & 1 \end{pmatrix} = (53687, 80643, 47067) \bmod 256$$

$$(95 \quad 171 \quad 214)$$

xor

$$\begin{array}{r} 40 \quad 171 \quad 36 \\ \hline 119 \quad 0 \quad 255 \end{array}$$

$$P_2 = (119 \quad 0 \quad 255)$$

$$\begin{array}{r} 1011111 \\ 0101000 \\ \hline 1110111 \end{array}$$

$$\begin{array}{r} 11011011 \\ 00100100 \\ \hline 11111111 \end{array}$$



Evaluación de conocimientos del primer parcial.

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 11 & 9 & 8 \end{pmatrix}^{-1} \Rightarrow \begin{pmatrix} 1 & 2 & 3 & 1 & 0 & 0 \\ 4 & 5 & 6 & 0 & 1 & 0 \\ 11 & 9 & 8 & 0 & 0 & 1 \end{pmatrix} \begin{matrix} \\ F_2 - 4F_1 \\ F_3 - 11F_1 \end{matrix}$$

$$\begin{pmatrix} 1 & 2 & 3 & 1 & 0 & 0 \\ 0 & -3 & -6 & -4 & 1 & 0 \\ 0 & -13 & -25 & -11 & 0 & 1 \end{pmatrix} \Leftrightarrow -\frac{F_2}{3} \begin{pmatrix} 1 & 2 & 3 & 1 & 0 & 0 \\ 0 & 1 & 2 & 4/3 & 1/3 & 0 \\ 0 & -13 & -25 & -11 & 0 & 1 \end{pmatrix} \begin{matrix} F_1 - 2F_2 \\ \\ F_3 + 13F_2 \end{matrix}$$

$$\begin{pmatrix} 1 & 0 & -1 & 5/3 & 2/3 & 0 \\ 0 & 1 & 2 & 4/3 & 1/3 & 0 \\ 0 & 0 & 1 & 19/3 & -13/3 & 1 \end{pmatrix} \begin{matrix} F_1 + F_3 \\ F_2 - 2F_3 \\ \end{matrix} \begin{pmatrix} 1 & 0 & 0 & 14/3 & -1/3 & 1 \\ 0 & 1 & 0 & -34/3 & 25/3 & -2 \\ 0 & 0 & 1 & 19/3 & -13/3 & 1 \end{pmatrix}$$

$$K^{-1} = \begin{pmatrix} 14/3 & -1/3 & 1 \\ -34/3 & 25/3 & -2 \\ 19/3 & -13/3 & 1 \end{pmatrix} \mod 256 = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix}$$

⑨ $14 \cdot 3^{-1} \mod 256 = 14 \cdot 171 \mod 256 = 2394 \mod 256 = 90$

$$3^{-1} \mod 256 = 171$$

$$256 = 3(85) + 1 \quad 1 = 256 - 3(85)$$

$$3 = 1(3) + 0 \quad 1 = 256 + 3(-85)$$

$$3^{-1} \mod 256 = -85 \mod 256$$

$$3^{-1} \mod 256 = 171$$

Comprobación

$$3 \cdot 171 \mod 256 = 1$$

$a = 90$

Duarte



Evaluación de conocimientos del primer parcial.

$$\textcircled{b} \cdot 11 \cdot 3^{-1} \bmod 256 = 245 \cdot 171 \bmod 256 = 41895 \bmod 256 = 167$$
$$-3^{-1} \bmod 256 = 171$$
$$-11 \bmod 256 = 245$$

$$b = 167$$

$$\textcircled{c} 1 \bmod 256 = 1$$

$$c = 1$$
 Usando resultados anteriores =

$$\textcircled{d} -34 \cdot 3^{-1} \bmod 256 = 222 \cdot 171 = 37962 \bmod 256 = 74$$
$$-34 \bmod 256 = 222$$

$$d = 74$$

$$\textcircled{e} 75 \cdot 3^{-1} \bmod 256 = 75 \cdot 171 \bmod 256 = 4245 \bmod 256 = 179$$
$$e = 179$$

$$\textcircled{f} -2 \bmod 256 = 254$$

$$f = 254$$

$$\textcircled{g} 19 \cdot 3^{-1} \bmod 256 = 19 \cdot 171 = 3249 \bmod 256 = 177$$

$$g = 177$$

$$\textcircled{h} -13 \cdot 3^{-1} \bmod 256 = 243 \cdot 171 \bmod 256 = 41553 \bmod 256 = 81$$
$$-13 \bmod 256 = 243$$

$$h = 81$$

$$c = 1$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 11 & 9 & 8 \end{pmatrix} \bmod 256 = \begin{pmatrix} 90 & 167 & 1 \\ 74 & 179 & 254 \\ 177 & 81 & 1 \end{pmatrix}$$