ALEJANDRO SANTORUM VARELA 44090946-S

$\boxed{1.}$ SONAFQCHMWPTVEVY

$$\shortparallel$$

$$(18\ 14\ 13\ 0\ 5\ 16\ 2\ 7\ 14\ 22\ 15\ 19\ 21\ 4\ 21\ 24)$$

$$\Rightarrow M_c = \begin{pmatrix} 18 & 13 & 5 & 2 & 14 & 15 & 21 & 21 \\ 14 & 0 & 16 & 7 & 22 & 19 & 4 & 24 \end{pmatrix}$$

Sabemos que: $A \begin{pmatrix} T & H \\ H & E \end{pmatrix} = \begin{pmatrix} K & X \\ H & W \end{pmatrix} \Rightarrow$

$$\Rightarrow A \begin{pmatrix} 19 & 7 \\ 7 & 4 \end{pmatrix} = \begin{pmatrix} 10 & 23 \\ 7 & 22 \end{pmatrix} \Rightarrow A = \begin{pmatrix} 10 & 23 \\ 7 & 22 \end{pmatrix} \begin{pmatrix} 19 & 7 \\ 7 & 4 \end{pmatrix}^{-1}$$

Como $\det \begin{pmatrix} 19 & 7 \\ 7 & 4 \end{pmatrix} = 27 \equiv 1 \pmod{26}$ y $mcd(1, 26) = 1$

entonces es invertible mod. 26.

$$\Rightarrow \begin{pmatrix} 19 & 7 \\ 7 & 4 \end{pmatrix}^{-1} = \begin{pmatrix} 4 & 19 \\ 19 & 19 \end{pmatrix} \Rightarrow A = \begin{pmatrix} 10 & 23 \\ 7 & 22 \end{pmatrix} \begin{pmatrix} 4 & 19 \\ 19 & 19 \end{pmatrix} = \begin{pmatrix} 9 & 3 \\ 4 & 5 \end{pmatrix}$$

$$\Rightarrow B = A^{-1} = \begin{pmatrix} 23 & 7 \\ 18 & 5 \end{pmatrix}$$ (matriz de descifrado)

$$M_p = B \cdot M_c = \begin{pmatrix} 18 & 13 & 19 & 17 & 8 & 10 & 17 & 1 \\ 4 & 0 & 14 & 19 & 24 & 1 & 8 & 4 \end{pmatrix}$$

$\Rightarrow$ mensaje: $\boxed{\text{SENATORTOOKBRIBE}}$

$\boxed{2.}$ ZRIXXYVBMNPO

27 letras : $\{A, B, C, \dots, Y, Z, -\}$

$$B\begin{pmatrix} P & R \\ K & Z \end{pmatrix} = \begin{pmatrix} E & S \\ - & - \end{pmatrix} \Longrightarrow B\begin{pmatrix} 15 & 17 \\ 10 & 25 \end{pmatrix} = \begin{pmatrix} 4 & 18 \\ 26 & 26 \end{pmatrix}$$

$$\Rightarrow B = \begin{pmatrix} 4 & 18 \\ 26 & 26 \end{pmatrix}\begin{pmatrix} 15 & 17 \\ 10 & 25 \end{pmatrix}^{-1}$$

La matriz $\begin{pmatrix} 15 & 17 \\ 10 & 25 \end{pmatrix}$ es invertible ya que $\det\begin{pmatrix} 15 & 17 \\ 10 & 25 \end{pmatrix} = 16 \pmod{27}$

y $\mathrm{mcd}(16, 27) = 1$.

$$\begin{pmatrix} 15 & 17 \\ 10 & 25 \end{pmatrix}^{-1} = \begin{pmatrix} 10 & 4 \\ 23 & 6 \end{pmatrix} \Longrightarrow B = \begin{pmatrix} 4 & 18 \\ 26 & 26 \end{pmatrix}\begin{pmatrix} 10 & 4 \\ 23 & 6 \end{pmatrix} = \underbrace{\begin{pmatrix} 22 & 16 \\ 21 & 17 \end{pmatrix}}_{\text{matriz de descifrado}}$$

Como $M_c = \begin{pmatrix} Z & I & X & V & M & P \\ R & X & Y & B & N & O \end{pmatrix} \simeq \begin{pmatrix} 25 & 8 & 23 & 21 & 12 & 15 \\ 17 & 23 & 24 & 1 & 13 & 14 \end{pmatrix}$

$$\Rightarrow M_p = B \circ M_c = \begin{pmatrix} 12 & 4 & 26 & 19 & 13 & 14 \\ 4 & 19 & 0 & 26 & 14 & 13 \end{pmatrix}$$

$\Rightarrow$ mensaje : $\boxed{\text{MEET-AT-NOON}}$

$\boxed{3.}$

¡IWGVIEX!ZRADRYD

$\{A, B, C, \ldots, Y, Z, -, ?, !\}$ 29 símbolos

Firma: MARIA

a)

$$B\begin{pmatrix} D & Y \\ R & D \end{pmatrix} = \begin{pmatrix} A & I \\ R & A \end{pmatrix} \Longrightarrow B\begin{pmatrix} 3 & 24 \\ 17 & 3 \end{pmatrix} = \begin{pmatrix} 0 & 8 \\ 17 & 0 \end{pmatrix} \Rightarrow$$

$$\Rightarrow B = \begin{pmatrix} 0 & 8 \\ 17 & 0 \end{pmatrix}\begin{pmatrix} 3 & 24 \\ 17 & 3 \end{pmatrix}^{-1}$$

Como $\det\begin{pmatrix} 3 & 24 \\ 17 & 3 \end{pmatrix} = 7 \pmod{29}$ y $\text{mcd}(7, 29) = 1$, es invertible.

$$\begin{pmatrix} 3 & 24 \\ 17 & 3 \end{pmatrix}^{-1} = \begin{pmatrix} 17 & 9 \\ 10 & 17 \end{pmatrix} \Longrightarrow B = \begin{pmatrix} 0 & 8 \\ 17 & 0 \end{pmatrix}\begin{pmatrix} 17 & 9 \\ 10 & 17 \end{pmatrix} = \underbrace{\begin{pmatrix} 22 & 20 \\ 28 & 8 \end{pmatrix}}_{\text{matriz de descifrado}}$$

Sabemos que $M_c \approx \begin{pmatrix} 28 & 22 & 21 & 4 & 28 & 17 & 3 & 24 \\ 8 & 6 & 8 & 23 & 25 & 0 & 17 & 3 \end{pmatrix}$

$$\Rightarrow M_p = B \circ M_c = \begin{pmatrix} 22 & 24 & 13 & 26 & 14 & 26 & 0 & 8 \\ 7 & 26 & 14 & 6 & 27 & 12 & 17 & 0 \end{pmatrix}$$

$\Rightarrow$ mensaje $= \boxed{\text{WHY-NO-GO?-MARIA}}$

b) $M_p = \text{DAMN-FOG!-JO} \approx \begin{pmatrix} 3 & 12 & 26 & 14 & 28 & 9 \\ 0 & 13 & 5 & 6 & 26 & 14 \end{pmatrix}$

$A = B^{-1} = \begin{pmatrix} 3 & 7 \\ 4 & 1 \end{pmatrix}$ matriz de cifrado

$$\Rightarrow M_c = A.M_p = \begin{pmatrix} 9 & 11 & 26 & 26 & 5 & 9 \\ 12 & 3 & 22 & 4 & 22 & 21 \end{pmatrix}$$

$\Rightarrow$ mensaje $= \boxed{\text{JMLD-W-EFWJV}}$

i) $A\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} a \\ b \end{pmatrix}$

$A\begin{pmatrix} b \\ c \end{pmatrix} = \begin{pmatrix} a \\ c \end{pmatrix}$

Sabemos que $A\begin{pmatrix} a & b \\ b & c \end{pmatrix} = \begin{pmatrix} a & a \\ b & c \end{pmatrix} \Rightarrow$

$\Rightarrow A\begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 1 & 2 \end{pmatrix}$

$\Rightarrow A = \begin{pmatrix} 0 & 0 \\ 1 & 2 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix}^{-1} \pmod{26}$

Tenemos que calcular $\begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix}^{-1} \pmod{26}$

$\det\begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix} = -1 \pmod{26} = 25 \pmod{26}$

$\text{mcd}(25, 26) = 1 \Rightarrow$ la matriz es invertible

$\begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix}^{-1} (\text{mod. } 26) = \begin{pmatrix} 24 & 1 \\ 1 & 0 \end{pmatrix}$

$\Rightarrow A = \begin{pmatrix} 0 & 0 \\ 1 & 2 \end{pmatrix}\begin{pmatrix} 24 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$ $\quad \det A = 0$

Como A no es invertible $\Rightarrow$ NO existe un criptosisteme que satisfaga las condiciones.

ii)

$$A\begin{pmatrix} a & d \\ b & d \end{pmatrix} = \begin{pmatrix} a & f \\ b & d \end{pmatrix} \Rightarrow A\begin{pmatrix} 0 & 3 \\ 1 & 3 \end{pmatrix} = \begin{pmatrix} 0 & 5 \\ 1 & 3 \end{pmatrix}$$

$$\Rightarrow A = \begin{pmatrix} 0 & 5 \\ 1 & 3 \end{pmatrix}\begin{pmatrix} 0 & 3 \\ 1 & 3 \end{pmatrix}^{-1} \pmod{26}$$

$$\det\begin{pmatrix} 0 & 3 \\ 1 & 3 \end{pmatrix} = -3 = 23$$

Como $\operatorname{mcd}(23,26) = 1 \Rightarrow$ invertible

$$\begin{pmatrix} 0 & 3 \\ 1 & 3 \end{pmatrix}^{-1} \pmod{26} = \begin{pmatrix} 25 & 1 \\ 9 & 0 \end{pmatrix} \pmod{26}$$

$$\Rightarrow A = \begin{pmatrix} 0 & 5 \\ 1 & 3 \end{pmatrix}\begin{pmatrix} 25 & 1 \\ 9 & 0 \end{pmatrix} \pmod{26} = \begin{pmatrix} 19 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\det\begin{pmatrix} 19 & 0 \\ 0 & 1 \end{pmatrix} = 19 \Rightarrow \operatorname{mcd}(19,26) = 1 \Rightarrow \text{invertible}$$

$\boxed{A^{-1} = \begin{pmatrix} 11 & 0 \\ 0 & 1 \end{pmatrix}} \Rightarrow$ sí existe un criptosistema