Temă:

$$A = \begin{pmatrix} 3 & 7 \\ 11 & 5 \end{pmatrix}$$

alfabet 29

(A - Z _ ? .)

Decriptare

CSAXDPJSEFCAUYUYC

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \Rightarrow A^t = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \Rightarrow A^* = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \Rightarrow$$

$$\Rightarrow A^{-1} = (\det A)^{-1} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

$$\det A = 3 \cdot 5 - 7 \cdot 11 = 15 - 77 = -62 \Rightarrow -2 \pmod{30}$$

~~$(\det A)^{-1} = (-62)^{-1} =$~~

$$(\det A)^{-1} = (-2)^{-1} = 28^{-1}$$

$$28 \cdot x \equiv 1 \mod 30$$

$(28,30) = 2 \neq 1 \Rightarrow$ 28 nu are invers în modulo 30

deoarece nu este prim în 30

matricea A nu este inversabilă în mod 30 deci nu se poate decripta mesajul cu această matrice în mod 30
nu există matricea de decriptare A^{-1}

---

fără ! = 28

$$A = \begin{pmatrix} 3 & 7 \\ 11 & 5 \end{pmatrix}$$

$\det A = 3 \cdot 5 - 7 \cdot 11 = 15 - 77 = -62 \Rightarrow -4 \pmod{29}$

$(\det A)^{-1} = (-4)^{-1} = 25^{-1}$

$25 \cdot x \equiv 1 \pmod{29}$

$(29, 25) = 1$

$29 = 25 \cdot 1 + 4$

$25 = 4 \cdot 6 + 1$

$4 = 1 \cdot 4$

$x_{29} = (1,0) \quad x_{25} = (0,1)$

$x_4 = x_{29} - x_{25}$

$(1,0) - (0,1) = (1,-1)$

$x_1 = x_{25} - 6 \cdot x_4$

$(0,1) - 6 \cdot (1,-1) = (0,1) - (6,-6) = (-6,7)$

$25 \cdot 7 \equiv 1 \pmod{29}$

$A^{-1} = 7 \cdot \begin{pmatrix} 5 & -7 \\ -11 & 3 \end{pmatrix} \bmod 29 = \begin{pmatrix} 35 & -49 \\ -77 & 21 \end{pmatrix} \bmod 29 =$

$$= \begin{pmatrix} 6 & -20 \\ -19 & 21 \end{pmatrix} \not\equiv \not\equiv \not\equiv \pmod{29} \equiv$$

$$= \begin{pmatrix} 6 & 9 \\ 10 & 21 \end{pmatrix}$$

$$\begin{pmatrix} 6 & 9 \\ 10 & 21 \end{pmatrix} \begin{pmatrix} C & A & D & J & E & C & U & U & C \\ S & X & P & S & F & A & Y & Y & \end{pmatrix}$$

$$\begin{pmatrix} 6 & 9 \\ 10 & 21 \end{pmatrix} \begin{pmatrix} 2 & 0 & 3 & 9 & 4 & 2 & 20 & 20 & 2 \\ 18 & 23 & 15 & 18 & 5 & 0 & 24 & 24 & 26 \end{pmatrix}$$

$$= \begin{pmatrix} 6 \cdot 2 + 9 \cdot 18 & 6 \cdot 0 + 9 \cdot 23 & 6 \cdot 3 + 9 \cdot 15 & 6 \cdot 9 + 9 \cdot 18 \\ 10 \cdot 2 + 21 \cdot 18 & 10 \cdot 0 + 21 \cdot 23 & 10 \cdot 3 + 21 \cdot 15 & 10 \cdot 9 + 21 \cdot 18 \end{pmatrix}$$

$$6 \cdot 4 + 9 \cdot 5 \qquad 6 \cdot 2 + 9 \cdot 0 \qquad 6 \cdot 20 + 9 \cdot 24 \qquad \not\equiv \not\equiv$$
$$10 \cdot 4 + 21 \cdot 5 \qquad 10 \cdot 2 + 21 \cdot 0 \qquad 10 \cdot 20 + 21 \cdot 24$$

$$\begin{matrix} 6 \cdot 20 + 9 \cdot 24 & 6 \cdot 2 + 9 \cdot 26 \\ 10 \cdot 20 + 21 \cdot 24 & 10 \cdot 2 + 21 \cdot 26 \end{matrix} \Bigg) =$$

$$= \begin{pmatrix} 174 & 207 & 153 & 216 & 69 & 12 & 336 & 336 & 246 \\ 398 & 483 & 345 & 468 & 165 & 20 & 704 & 704 & 566 \end{pmatrix}$$

$$\xrightarrow{\text{mod}(29)} \begin{pmatrix} 0 & 4 & 8 & 13 & 11 & 12 & 17 & 17 & 14 \\ 21 & 19 & 26 & 4 & 0 & 20 & 8 & 8 & 15 \end{pmatrix}$$

$$= \begin{pmatrix} A & E & I & H & L & M & R & R & O \\ V & T & & E & A & V & I & I & P \end{pmatrix}$$

AVETI NELAMURIRIOP