Lema 5 - Criptă

23) Interceptăți mesajul: SONAFQCHMWPTVEVY

$KH = TH \to A \cdot TH = KH \pmod{26}$
$XW = HE \to A \cdot HE = XW \pmod{26}$ $= \begin{cases} Ax_1 = y_1 \\ Ax_2 = y_2 \end{cases}$

$KH = (10, 7)$ $XW = (23, 22)$
$TH = (19, 7)$ $HE = (7, 4)$

$A \cdot \begin{pmatrix} 19 \\ 7 \end{pmatrix} = \begin{pmatrix} 10 \\ 7 \end{pmatrix}$ $= A \cdot \begin{pmatrix} 19 & 7 \\ 7 & 4 \end{pmatrix} = \begin{pmatrix} 10 & 23 \\ 7 & 22 \end{pmatrix}$

$A \cdot \begin{pmatrix} 7 \\ 4 \end{pmatrix} = \begin{pmatrix} 23 \\ 22 \end{pmatrix}$

$\Rightarrow A = \begin{pmatrix} 10 & 23 \\ 7 & 22 \end{pmatrix} \cdot \begin{pmatrix} 19 & 7 \\ 7 & 4 \end{pmatrix}^{-1}$ notăm această matrice cu B

B^{-1}: $\det B = \begin{vmatrix} 19 & 7 \\ 7 & 4 \end{vmatrix} = 27 \pmod{26} = 1$

$B^t = \begin{pmatrix} 19 & 7 \\ 7 & 4 \end{pmatrix}$, $B^* = \begin{pmatrix} 4 & -7 \\ -7 & 19 \end{pmatrix} \pmod{26} = \begin{pmatrix} 4 & 19 \\ 19 & 19 \end{pmatrix}$

$B^{-1} = (\det B)^{-1} \cdot B^* = \begin{pmatrix} 4 & 19 \\ 19 & 19 \end{pmatrix}$

$\Rightarrow A = \begin{pmatrix} 10 & 23 \\ 7 & 22 \end{pmatrix} \cdot \begin{pmatrix} 4 & 19 \\ 19 & 19 \end{pmatrix} = \begin{pmatrix} 10 \cdot 4 + 23 \cdot 19 & 10 \cdot 19 + 23 \cdot 19 \\ 7 \cdot 4 + 22 \cdot 19 & 7 \cdot 19 + 22 \cdot 19 \end{pmatrix}$

$= \begin{pmatrix} 447 & 627 \\ 446 & 551 \end{pmatrix} \pmod{26} = \begin{pmatrix} 9 & 3 \\ 4 & 5 \end{pmatrix}$

A^{-1}: o) $\det A = \begin{vmatrix} 9 & 3 \\ 4 & 5 \end{vmatrix} = 9 \cdot 5 - 3 \cdot 4 = 33 = 7$

$A^t = \begin{pmatrix} 9 & 4 \\ 3 & 5 \end{pmatrix}$ $A^* = \begin{pmatrix} 5 & -3 \\ -4 & 9 \end{pmatrix}$

$A^{-1} = (\det A)^{-1} \cdot \begin{pmatrix} 5 & -3 \\ -4 & 9 \end{pmatrix} = 15 \cdot \begin{pmatrix} 5 & -3 \\ -4 & 9 \end{pmatrix} \pmod{26}$

$= 15 \begin{pmatrix} 5 & 23 \\ 22 & 9 \end{pmatrix} = \begin{pmatrix} 75 & 345 \\ 330 & 135 \end{pmatrix} = \begin{pmatrix} 23 & 7 \\ 18 & 5 \end{pmatrix}$

$7^{-1} \pmod{26} = 7x + 26y = (7, 26)$

$26 = 7 \cdot 3 + 5$ $\quad 5 = 2 \cdot 2 + 1 \Rightarrow 1 = 5 - 2 \cdot 2 = 5 - 2(7 \cdot 5) = 3 \cdot 5 - 2 \cdot 7$

$7 = 5 \cdot 1 + 2$ $\quad = 3 \cdot (26 - 7 \cdot 3) - 2 \cdot 7 = 3 \cdot 26 - 11 \cdot 7 \Rightarrow x = -11$

$-11 = 15 \pmod{26}$

$A^{-1} = \begin{pmatrix} 23 & 7 \\ 18 & 5 \end{pmatrix}$ KM

$SO = (18, 14)$

$SO \cdot A^{-1} = \begin{pmatrix} 18 \\ 14 \end{pmatrix} \begin{pmatrix} 23 & 7 \\ 18 & 5 \end{pmatrix} = \begin{pmatrix} 18\cdot 23 + 18\cdot 18 \\ 14\cdot 7 + 14\cdot 5 \end{pmatrix} = \begin{pmatrix} 738 \\ 168 \end{pmatrix} = \begin{pmatrix} 10 \\ 12 \end{pmatrix}$

$\cdot \begin{pmatrix} 23 & 7 \\ 18 & 5 \end{pmatrix} \begin{pmatrix} 18 \\ 14 \end{pmatrix} = \begin{pmatrix} 23\cdot 18 + 7\cdot 14 \\ 18\cdot 18 + 5\cdot 14 \end{pmatrix} = \begin{pmatrix} 512 \\ 394 \end{pmatrix} = \begin{pmatrix} 18 \\ 4 \end{pmatrix} \begin{matrix} S \\ E \end{matrix}$

$A^{-1} \cdot NA = \begin{pmatrix} 23 & 7 \\ 18 & 5 \end{pmatrix} \begin{pmatrix} 13 \\ 0 \end{pmatrix} = \begin{pmatrix} 23\cdot 13 \\ 18\cdot 13 \end{pmatrix} = \begin{pmatrix} 299 \\ 234 \end{pmatrix} = \begin{pmatrix} 13 \\ 0 \end{pmatrix} \begin{matrix} N \\ A \end{matrix}$

$A^{-1} \cdot FQ = \begin{pmatrix} 23 & 7 \\ 18 & 5 \end{pmatrix} \begin{pmatrix} 5 \\ 16 \end{pmatrix} = \begin{pmatrix} 23\cdot 5 + 7\cdot 16 \\ 18\cdot 5 + 5\cdot 16 \end{pmatrix} = \begin{pmatrix} 227 \\ 170 \end{pmatrix} = \begin{pmatrix} 19 \\ 14 \end{pmatrix} \begin{matrix} T \\ O \end{matrix}$

$A^{-1} \cdot CH = \begin{pmatrix} 23 & 7 \\ 18 & 5 \end{pmatrix} \begin{pmatrix} 2 \\ 7 \end{pmatrix} = \begin{pmatrix} 23\cdot 2 + 7\cdot 7 \\ 18\cdot 2 + 5\cdot 7 \end{pmatrix} = \begin{pmatrix} 95 \\ 71 \end{pmatrix} = \begin{pmatrix} 17 \\ 19 \end{pmatrix} \begin{matrix} R \\ T \end{matrix}$

$A^{-1} \cdot MW = \begin{pmatrix} 23 & 7 \\ 18 & 5 \end{pmatrix} \begin{pmatrix} 12 \\ 22 \end{pmatrix} = \begin{pmatrix} 23\cdot 12 + 7\cdot 22 \\ 18\cdot 12 + 5\cdot 22 \end{pmatrix} = \begin{pmatrix} 14 \\ 14 \end{pmatrix} \begin{matrix} O \\ O \end{matrix}$

$A^{-1} \cdot PT = \begin{pmatrix} 23 & 7 \\ 18 & 5 \end{pmatrix} \begin{pmatrix} 15 \\ 19 \end{pmatrix} = \begin{pmatrix} 23\cdot 15 + 7\cdot 19 \\ 18\cdot 15 + 5\cdot 19 \end{pmatrix} = \begin{pmatrix} 478 \\ 365 \end{pmatrix} = \begin{pmatrix} 10 \\ 1 \end{pmatrix} \begin{matrix} K \\ B \end{matrix}$

$A^{-1} \cdot VE = \begin{pmatrix} 23 & 7 \\ 18 & 5 \end{pmatrix} \begin{pmatrix} 21 \\ 4 \end{pmatrix} = \begin{pmatrix} 23\cdot 21 + 7\cdot 4 \\ 18\cdot 21 + 5\cdot 4 \end{pmatrix} = \begin{pmatrix} 511 \\ 398 \end{pmatrix} = \begin{pmatrix} 17 \\ 8 \end{pmatrix} \begin{matrix} R \\ I \end{matrix}$

$A^{-1} \cdot VY = \begin{pmatrix} 23 & 7 \\ 18 & 5 \end{pmatrix} \begin{pmatrix} 21 \\ 24 \end{pmatrix} = \begin{pmatrix} 23\cdot 21 + 7\cdot 24 \\ 18\cdot 21 + 5\cdot 24 \end{pmatrix} = \begin{pmatrix} 651 \\ 498 \end{pmatrix} = \begin{pmatrix} 1 \\ 4 \end{pmatrix} \begin{matrix} B \\ E \end{matrix}$

Mesajul decriptat: SENATORTOOKBRIBE