Nichita Bogdan Valentin

M531

TEMA 4

23. Interceptați mesajul **SONAFQCHMWPTVEVY** obținut prin criptare afină pe blocuri, folosind o matrice de criptare $A \in \mathcal{M}2\times2\ (\mathbb{Z}26)$ și un alfabet de 26 caractere (A-Z). Cele mai frecvente blocuri ale mesajului cifrat sunt KH si XW si ele corespund lui TH si respectiv HE. Determinați matricea de decriptare și citiți mesajul.

KH -> TH => $[10, 7]^t = A \cdot [19, 7]^t$

XW -> HE => $[23, 22]^t = A \cdot [7, 4]^t$

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

$$\begin{cases} 19a + 7b \equiv 10 \ mod\ 26 \\ 19c + 7d \equiv 7 \ mod\ 26 \end{cases}$$

$$\begin{cases} 7a + 4b \equiv 23 \ mod\ 26 \\ 7c + 4d \equiv 22 \ mod\ 26 \end{cases}$$

$$7a + 4b \equiv 23 \ mod\ 26 |^7 => 49a + 28b \equiv 161 \ mod\ 26$$

$$19a + 7b \equiv 10 \ mod\ 26 |^4 => 76a + 28b \equiv 40 \ mod\ 26$$

$$\begin{cases} 76a + 28b \equiv 40 \ mod\ 26 \\ 49a + 28b \equiv 161 \ mod\ 26 \end{cases}$$

$$27a \equiv -121 \ mod\ 26 => a \equiv 9 \ mod\ 26$$

$$171 + 7b \equiv 23 \ mod\ 26 => 15 + 7b \equiv 10 \ mod\ 26 => \ 7b \equiv -5 \ mod\ 26 =>$$

$$b \equiv -75 \ mod\ 26 \equiv 3 \ mod\ 26$$

$$7c + 4d \equiv 22 \ mod\ 26 |^7 => 49a + 28b \equiv 154 \ mod\ 26$$

$$19c + 7d \equiv 7 \ mod\ 26 |^4 => 76a + 28b \equiv 28 \ mod\ 26$$

$$\begin{cases} 76c + 28d \equiv 28 \ mod\ 26 \\ 49c + 28d \equiv 154 \ mod\ 26 \end{cases}$$

$27c \equiv -126 \, mod \, 26 => c \equiv 4 \, mod \, 26$

$76 + 7d \equiv 7 \, mod \, 26 => -2 + 7d \equiv 7 \, mod \, 26 => \ 7d \equiv 9 \, mod \, 26 => \ d \equiv 5 \, mod \, 26$

$A = \begin{bmatrix} 9 & 3 \\ 4 & 5 \end{bmatrix}$

$\det(A) = 7 \bmod 26$

$A^{-1} = 15 \cdot \begin{bmatrix} 5 & -3 \\ -4 & 9 \end{bmatrix} = \begin{bmatrix} 23 & 7 \\ 18 & 5 \end{bmatrix} \, mod \, 26$

$A^{-1} \cdot \mathrm{SO} = \mathrm{SE\ NA\ FQ\ CH\ MW\ PT\ VE\ VY}$

$A^{-1} \cdot \mathrm{NA} = \mathrm{NA}$

$A^{-1} \cdot \mathrm{FQ} = \mathrm{TO}$

$A^{-1} \cdot \mathrm{CH} = \mathrm{RT}$

$A^{-1} \cdot \mathrm{MW} = \mathrm{OO}$

$A^{-1} \cdot \mathrm{PT} = \mathrm{KB}$

$A^{-1} \cdot \mathrm{VE} = \mathrm{RI}$

$A^{-1} \cdot \mathrm{VY} = \mathrm{BE}$

SENATOR TOOK BRIBE