Tema 5

20.

$$A = \begin{pmatrix} 3 & 7 & 1 \\ 13 & 11 & 12 \\ 1 & 2 & 3 \end{pmatrix} \qquad B = \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} \qquad 26 \text{ caractere}$$

Pentru a decripta textul vom folosi decriptarea afină, trebuie să găsim matricea inversă a matricii de criptare A

$X = A^{-1} \cdot (Y - B) \bmod 26$. Y - matricea cu textul de criptat

X - matricea cu textul decriptat

Vom împărți textul în 3 caractere "blacuri" și vom aplica formula.

Blocul "RSN"

P_I : Y - matrice 3 pe 1

P_{II} : Aflăm X

P_{III} : Convertim X

$$A^{-1} = \frac{1}{\det(A)} \cdot \text{adj}(A)$$ ⟵ adjuncta

Blocurile sunt: RSN
CEW
VXP
NKB
JZP
VUJ

Pasul I: $A=0 \quad B=1 \quad C=2 \quad D=3 \ldots Z=25$

- convertim in numere: $R=17$, $S=18$, $N=13$

Pasul II: $Y=\begin{pmatrix}17\\18\\13\end{pmatrix}$

Pasul III: $X = A^{-1} \cdot (Y-B) \bmod 26$

$$Y-B=\begin{pmatrix}17\\18\\13\end{pmatrix}-\begin{pmatrix}1\\2\\3\end{pmatrix}=\begin{pmatrix}16\\16\\10\end{pmatrix}$$

$$A^{-1}=\begin{pmatrix}-11 & 5 & 2\\17 & -8 & -3\\-5 & 2 & 1\end{pmatrix} \qquad X=\begin{pmatrix}-11 & 5 & 2\\17 & -8 & -3\\-5 & 2 & 1\end{pmatrix}\cdot\begin{pmatrix}16\\16\\10\end{pmatrix}$$

$$X=\begin{pmatrix}(-11\cdot16+5\cdot16+2\cdot10)\\(17\cdot16-8\cdot16-3\cdot10)\\(-5\cdot16+2\cdot16+1\cdot10)\end{pmatrix} \Rightarrow X=\begin{pmatrix}240-80+20\\272-128-30\\-80+32+10\end{pmatrix}$$

$$X=\begin{pmatrix}180\\114\\-38\end{pmatrix} \bmod 26 \Rightarrow X=\begin{pmatrix}180 \bmod 26\\114 \bmod 26\\-38 \bmod 26\end{pmatrix} \Rightarrow X=\begin{pmatrix}4\\10\\12\end{pmatrix}$$

$\Rightarrow$ "CON"

- $C=2 \quad E=4 \quad W=22$

Pas II: $Y=\begin{pmatrix}2\\4\\22\end{pmatrix}$

Pas III: $X = A^{-1} \cdot (Y-B) \bmod 26 \qquad Y=\begin{pmatrix}2\\4\\22\end{pmatrix}$

$$Y - B = \begin{pmatrix} 2 \\ 4 \\ 22 \end{pmatrix} - \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} = \begin{pmatrix} 1 \\ 2 \\ 19 \end{pmatrix}$$

$$X = \begin{pmatrix} -11 & 5 & 2 \\ 17 & -8 & -3 \\ -5 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 2 \\ 19 \end{pmatrix} = \begin{pmatrix} 5+10+38 \\ 17-16-57 \\ -5+4+19 \end{pmatrix} \Rightarrow X = \begin{pmatrix} 53 \\ -56 \\ 18 \end{pmatrix}$$

$$X \bmod 26 = \begin{pmatrix} 53 \bmod 26 \\ -56 \bmod 26 \\ 18 \bmod 26 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 18 \end{pmatrix} \Rightarrow \text{"GRA"}$$

- $V = 21 \quad X = 23 \quad P = 15$

$$Y = \begin{pmatrix} 21 \\ 23 \\ 15 \end{pmatrix} \qquad Y - B = \begin{pmatrix} 21 \\ 23 \\ 15 \end{pmatrix} - \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} = \begin{pmatrix} 20 \\ 21 \\ 12 \end{pmatrix}$$

$$X = \begin{pmatrix} -11 & 5 & 2 \\ 17 & -8 & -3 \\ -5 & 2 & 1 \end{pmatrix} \cdot \begin{pmatrix} 20 \\ 21 \\ 12 \end{pmatrix} \Rightarrow X = \begin{pmatrix} -220+105+24 \\ 340-168-36 \\ -100+42+12 \end{pmatrix}$$

$$\Rightarrow X = \begin{pmatrix} -91 \\ 136 \\ -46 \end{pmatrix} \bmod 26 = \begin{pmatrix} -91 \bmod 26 \\ 136 \bmod 26 \\ -46 \bmod 26 \end{pmatrix} = \begin{pmatrix} 13 \\ 12 \\ 6 \end{pmatrix}$$

$\Rightarrow$ "TIO"

- $N = 13 \quad K = 10 \quad B = 1$

$$Y = \begin{pmatrix} 13 \\ 10 \\ 1 \end{pmatrix} \qquad Y - B = \begin{pmatrix} 13 \\ 10 \\ 1 \end{pmatrix} - \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} = \begin{pmatrix} 12 \\ 8 \\ -2 \end{pmatrix}$$

$$\Rightarrow X = \begin{pmatrix} -11 \cdot 12 + 5 \cdot 8 + 2(-2) \\ 17 \cdot 12 - 8 \cdot 8 - 3 \cdot (-2) \\ -5 \cdot 12 + 2 \cdot 8 + 1 \cdot (-2) \end{pmatrix}$$

$$X = \begin{pmatrix} -132+40-4 \\ 204-64+6 \\ -60+16-2 \end{pmatrix} \Rightarrow X = \begin{pmatrix} -96 \\ 146 \\ -46 \end{pmatrix}$$

$$X \bmod 26 = \begin{pmatrix} 6 \\ 12 \\ 6 \end{pmatrix} = \text{"YOU"}$$

Blocul "JZP" —> "ARE"

Blocul "VUJ" —> "FUN"

Traducerea: CONGRATULATION YOU ARE FUN