09.04.24

Cifrul TN 7 _ 312

UN IBC

UNIBCUNIBCUNIBCUNI

If you want to encrypt this

DSG

CRIPTOSISTEM UNIAR PE DIGRAFURI VECTORIALE PESTE ALFABETUL A =

Criptosistem în care textul e împărțit în perechi (ordonate) de litere care sunt interpretate ca elemente din $\mathbb{Z}_n^2$ (unde $n = |A|$), și în care funcția de criptare e de tipul

$$c : \mathbb{Z}_n^2 \to \mathbb{Z}_n^2, \quad c(x) = M \cdot x$$

unde M e o matrice inversabilă din $M_2(\mathbb{Z}_n)$

(obs: Aplicația de decriptare e tot ea de același format

Notând cu matricea de decriptare, $D = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}_{28})$, informația din enunț se concretizează în:

$$D\begin{pmatrix} 8 \\ 5 \end{pmatrix} = \begin{pmatrix} 19 \\ 7 \end{pmatrix} \Leftrightarrow \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 8 \\ 5 \end{pmatrix} = \begin{pmatrix} 19 \\ 7 \end{pmatrix}$$

$$D\begin{pmatrix} 17 \\ 16 \end{pmatrix} = \begin{pmatrix} 7 \\ 4 \end{pmatrix} \Leftrightarrow \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 17 \\ 16 \end{pmatrix} = \begin{pmatrix} 7 \\ 4 \end{pmatrix} \quad (1)$$

a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12

n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

.	!
26	27

$$(1) \Leftrightarrow \begin{cases} 8a + 5b = 19 \\ 17a + 16b = 7 \\ 8c + 5d = 7 \\ 17c + 16d = 4 \end{cases}$$

$$\begin{vmatrix} 8 & 5 \\ -11 & -12 \end{vmatrix} = -96 + 55 = -41 = 15$$

$$a = -13 \begin{vmatrix} -8 & 5 \\ 7 & -12 \end{vmatrix} = -13 \mid 73 = -13 \cdot (-11) = 3$$

$$\frac{28}{15} = 1 + \frac{13}{15} = 1 + \frac{1}{1 + \frac{2}{13}} =$$

$$= 1 + \frac{1}{1 + \frac{1}{6 + \frac{1}{2}}}$$

$$1 + \frac{1}{1 + \frac{1}{6}} = \frac{13}{7}.$$

$b = -13 \begin{vmatrix} 8 & -9 \\ -11 & 7 \end{vmatrix} = -13(-43) = -13 \cdot 13 = -169 = -1$

$c = -13 \begin{vmatrix} 7 & 5 \\ 4 & -12 \end{vmatrix} = -13 \cdot 8 = -104 = 8.$

$d = -13 \begin{vmatrix} 8 & 7 \\ -11 & 4 \end{vmatrix} = -13(4+7) = 39 = 11.$

17
8
136
187
323

136
176
312

Deci $D = \begin{pmatrix} 3 & -1 \\ 8 & 11 \end{pmatrix}$.

Acum descifrăm mesajul!

$$\begin{pmatrix} 3 & -1 \\ 8 & 11 \end{pmatrix} \cdot \begin{pmatrix} 2 & 6 & 1 & 11 & 6 & 8 & 9 \\ 10 & 26 & 0 & 2 & 24 & 13 & 0 \end{pmatrix} =$$

$$= \begin{pmatrix} 24 & 20 & 3 & 3 & 22 & 11 & 27 \\ 14 & 26 & 8 & 26 & 4 & 11 & 16 \end{pmatrix},$$

deci mesajul Natal e

you_did_well!