1341b

Wednesday, 5 November, 2025 9:51

Cifruri simple (Caesar, afin, Hill)

Coduri
- flux (stream cipher): același cheie pt tot mesajul
- pe blocuri (block cipher)
  - fără padding: ultimul bloc mai scurt
  - cu padding: toate blocurile au aceeași lungime (ex. salted hashes)

A	B	C	D	E	F	G	H	I	J	K	L
0	1	2	3	4	5	6	7	8	9	10	11

M	N	O	P	Q	R	S	T	U	V	W	X
12	13	14	15	16	17	18	19	20	21	22	23

Y	Z
24	25

Ar trebui să lucrez în $\mathbb{Z}_{26} = \{0, 1, \dots, 25\}$, dar de ex., nr pare nu au invers în $\mathbb{Z}_{26}$ ($\nexists 2^{-1}, 4^{-1}, 6^{-1}, 8^{-1}, \dots$)

Adaug ␣ . !
26 27 28

$\Rightarrow$ lucrez în $\mathbb{Z}_{29}$

29 prim $\Rightarrow U(\mathbb{Z}_{29}) = \mathbb{Z}_{29} - \{0\}$.

Cifrul Caesar

- varianta flux

Ecuația de criptare: cod = mesaj + cheie

Ecuația de decriptare: mesaj = cod − cheie

în $\mathbb{Z}_{29}$

Ex: mesaj: MESAJ

Ex: mesaj: MESAJ

cheie: 19

Criptarea: [M,E,S,A,J] → [12,4,18,0,9] $\xrightarrow[+19]{+\text{cheie}}$ [31,23,37,19,28]

$\xrightarrow[\text{mod }29]{}$ [2,23,8,19,28] → CXIT!

Decriptarea: [C,X,I,T,!] → [2,23,8,19,28] $\xrightarrow[-19]{-\text{cheie}}$

→ [-17,4,-11,0,9] $\xrightarrow[\text{mod }29]{}$ [12,4,18,0,9] → MESAJ

Pe blocuri: cu padding random

Ex: mesaj: ASTAZI

Blocuri de lungime 3 ⇒ AST: cheie1 = 15, AZI: cheie2 = 20

Blocuri de lung 4

ASTA

ZIPS

padding random

[A,S,T] → [0,18,19] $\xrightarrow[+15]{+\text{cheie1}}$ [15,33,34] $\xrightarrow{\text{mod }29}$ [15,4,5] → PEF

[A,Z,I] → [0,25,8] $\xrightarrow[+20]{+\text{cheie2}}$ [20,45,28] $\xrightarrow[\text{mod }29]{}$ [20,16,28] → UQ!

ASTAZI → PEFUQ!

Cifrul afin

Varianta flux: Ec. de criptare: Cod = mesaj · cheie 1 + cheie 2

Ec. de decriptare: Mesaj = (Cod − cheie2) · cheie1^{-1}

Ex: mesaj: MESAJ

cheie1 = 10; cheie2 = 17

[M,E,S,A,J] → [12,4,18,0,9] $\xrightarrow[\cdot 10,+17]{\cdot \text{cheie1},+\text{cheie2}}$ [137,57,197,17,107]

→ [21,28,23,17,20] → V!XRIL

$\xrightarrow{\text{mod } 29} [21, 28, 23, 17, 20] \rightarrow V!XRU$

$137 = 116 + 21 = 21$ (116 = 0)

$57 = 58 - 1 = -1 = 28$

$197 = 137 + 60 = 137 + 58 + 2 = 21 + 0 + 2 = 23$

$107 = 137 - 30 = 21 - 30 = -9 = 20$

MESAJ → V!XRU.

<u>Decriptare</u>: $[V, !, X, R, U] \rightarrow [21, 28, 23, 17, 20] \xrightarrow{-17,\ \cdot 10^{-1} = 3}$

$[12, 33, 18, 0, 9] \rightarrow [12, 4, 18, 0, 9] \rightarrow$ MESAJ

<u>Cifrul Hill</u>

Matrice de criptare $\in \mathcal{M}_3(\mathbb{Z}_{29})$

Ec. de criptare: $\begin{pmatrix} C \\ O \\ D \end{pmatrix} = \begin{pmatrix} M \\ A \\ T. \end{pmatrix} \cdot \begin{pmatrix} M \\ S \\ J. \end{pmatrix}$

Ec. de decriptare: $\begin{pmatrix} M \\ S \\ J. \end{pmatrix} = \begin{pmatrix} M \\ A \\ T. \end{pmatrix}^{-1} \cdot \begin{pmatrix} C \\ O \\ D \end{pmatrix}$

Ex. mesaj: $\begin{pmatrix} Y \\ E \\ S \end{pmatrix} = \begin{pmatrix} 24 \\ 4 \\ 18 \end{pmatrix}$ mat. $= \begin{pmatrix} -1 & 0 & -1 \\ 2 & -1 & -1 \\ 1 & 0 & -1 \end{pmatrix}$

$\det(\text{mat.}) = -1 - 1 = -2 = 27 \in U(\mathbb{Z}_{29})$

$(\det(\text{mat.}))^{-1} = 27^{-1} = 14$

<u>Criptare:</u> $\underset{\text{mat}}{\begin{pmatrix} -1 & 0 & -1 \\ 2 & -1 & -1 \\ 1 & 0 & -1 \end{pmatrix}} \cdot \underset{\text{msj.}}{\begin{pmatrix} 24 \\ 4 \\ 18 \end{pmatrix}} = \begin{pmatrix} -42 \\ 26 \\ 6 \end{pmatrix} \text{ mod } 29 = \begin{pmatrix} 16 \\ 26 \\ 6 \end{pmatrix}$ Q Ш G

$$\begin{pmatrix} 2 & -1 & -1 \\ 1 & 0 & -1 \end{pmatrix} \cdot \begin{pmatrix} 4 \\ 18 \end{pmatrix} = \begin{pmatrix} 26 \\ 6 \end{pmatrix} \mod 29 = \begin{pmatrix} 26 \\ 6 \end{pmatrix} \begin{matrix} L \\ G \end{matrix}$$

$$-42 = -29 - 13 = -13 = 16$$

Descriptare: $mat^t = \begin{pmatrix} -1 & 2 & 1 \\ 0 & -1 & 0 \\ -1 & -1 & -1 \end{pmatrix} \longrightarrow mat^* = \begin{pmatrix} 1 & 0 & -1 \\ 1 & 2 & -3 \\ 1 & 0 & 1 \end{pmatrix}$

$$mat^{-1} = (\det(mat))^{-1} \cdot mat^* = 14 \cdot \begin{pmatrix} 1 & 0 & -1 \\ 1 & 2 & -3 \\ 1 & 0 & 1 \end{pmatrix}$$

$$14 \cdot \begin{pmatrix} 1 & 0 & -1 \\ 1 & 2 & -3 \\ 1 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 16 \\ 26 \\ 6 \end{pmatrix} = \begin{pmatrix} 24 \\ 4 \\ 18 \end{pmatrix}$$