1342b

Aritmetică modulară (în $\mathbb{Z}_n$)

$\mathbb{Z}_n = \{0, 1, 2, \dots, n-1\}$

$(\mathbb{Z}_n, +, \cdot)$ inel comutativ

$\rightarrow (\mathbb{Z}_n, +)$ grup comutativ

$\rightarrow (\mathbb{Z}_n^*, \cdot)$ monoid comutativ

$U(\mathbb{Z}_n) = \{x \in \mathbb{Z}_n \mid x \text{ este inv. față de } \cdot\}$

$U(\mathbb{Z}_n) \neq \mathbb{Z}_n$

Ex: $\mathbb{Z}_7 = \{0, 1, 2, \dots, 6\}$

-3 = opusul lui $3 = x$ pt care $x + 3 = 0$

$-3 = 4$

3^{-1} = inversul lui $3 = y$ pt care $3 \cdot y = 1$

$3^{-1} = 5$ pt că $3 \cdot 5 = 15 = 1$.

Teoremă: $U(\mathbb{Z}_n) = \{x \in \mathbb{Z}_n \mid \text{cmmdc}(x, n) = 1\}$

Obs: $(U(\mathbb{Z}_n), \cdot)$ grupul unităților

Z_{10} $U(Z_{10}) = \{1, 3, 7, 9\}$

4^{-1} nu există

$3^{-1} = 7$ pt că $3 \cdot 7 = 21 = 1 \mod 10$

Z_{26} Z_{29}

A	B	C	D	...	Z	↳	.	?
0	1	2	3		25	26	27	28

$5x + 2 = 1$ în Z_7

$5x = -1 \quad | \cdot 5^{-1} = 3$

$5^{-1} \cdot 5 \cdot x = (-1) \cdot 5^{-1}$

$x = (-1) \cdot 3 = -3 = 4$

$3x^2 + x - 2 = 0$ în Z_{11}

$\Delta = 1 - 4 \cdot (-2) \cdot 3 = 1 + 24 = 25 = 3$

$\sqrt{a} = b \Leftrightarrow a = b^2$

$\sqrt{3}$ în $Z_{11} = \{5, 6\} = \{5, -5\}$

$$x_{1,2} = \left(-1 \pm \sqrt{\Delta}\right) \cdot 6^{-1}$$

$\sqrt{3} = 5 \Rightarrow x_1 = (-1+5) \cdot 6^{-1} = 4 \cdot 2 = 8$

$x_2 = (-1-5) \cdot 6^{-1} = -6 \cdot 2 = -12$

$= -11 - 1 = -1 = 10$

$\Rightarrow x \in \{8, 10\}$

Logaritmul discret

$$\log_a b = c \Rightarrow a^c = b$$

$\log_2 3 \in \mathbb{Z}_5 = x \Leftrightarrow 2^x = 3 \in \mathbb{Z}_5$

$2^0 = 1;\ 2^1 = 2;\ 2^2 = 4;\ 2^3 = 8 = 3$

$\Rightarrow \log_2 3 = 3 \in \mathbb{Z}_5$

D-H: $\log_{7131}{}_{\underset{x}{\shortparallel}}\ 5247 \in \mathbb{Z}_{21733}$

$\Rightarrow 7131^x = 5247 \bmod 21733$

Teorema lui Lagrange

$(G, \cdot)$ grup, $\#G = n$

$\forall g \in G, \; g^n = e.$

---

g^{52} în $\mathbb{Z}_{11}$

$g^{52} = (g^2)^{26} = (81)^{26} = 4^{26} = (4^2)^{13}$

$= 5^{13} = (5^2)^6 \cdot 5 = 3^6 \cdot 5 = (3^3)^2 \cdot 5$

$= 5^2 \cdot 5 = 3 \cdot 5 = 4.$

$A \in \mathcal{M}_n(\mathbb{Z}_t) \quad A^{-1} = (\det A)^{-1} \cdot A^*$ există

$\Leftrightarrow (\det A)^{-1}$ există $\Leftrightarrow \text{cmmdc}(\det A, t) = 1.$

Cifruri bazate pe $\mathbb{Z}_n$

$\mathbb{Z}_{29}$

A	B	C	D	...	Z	␣	.	?
0					25	26	27	28

Cifruri

1) flux (stream): aceeași cheie pt tot mesajul

2) pe blocuri (block): 1 cheie / bloc

a) cu padding: toate blocurile au aceeași lungime

b) fără padding, $\leq$ 1 bloc mai scurt

$c = m + K \text{ în } \mathbb{Z}_{29}$

Caesar

Flux: Ec. de criptare: Cod = Mesaj + Cheie

Ec. de decriptare: Mesaj = Cod - Cheie

Ex: Mesaj: LUNI ; Cheia = 35

$[L,U,N,I] \to [11,20,13,8] \xrightarrow[+35]{+K} [46,55,48,43] \xrightarrow{\%29} [17,26,19,14]$

$\to [R, \text{␣}, T, O]$: R␣TO

Decriptarea:

$[R, L, T, O] \rightarrow [17, 26, 19, 14] \xrightarrow[-35]{-k}$

$[-18, -9, -16, -21] \xrightarrow{\%29} [11, 20, 13, 8]$

$\rightarrow$ LUNI.

Pe blocuri: fără padding:

Mesaj: NOIEMBRIE

Bloc: 5 $\Rightarrow$ b1: NOIEM k1: 10

b2: BRIE k2: 15

$[N, O, I, E, M] \rightarrow [13, 14, 8, 4, 12] \xrightarrow{+10}$

$\rightarrow [23, 24, 18, 14, 22] \rightarrow$ XYSOW

$[B, R, I, E] \rightarrow [1, 17, 8, 4] \xrightarrow{+15} [16, 32, 23, 19]$

$\xrightarrow{\%29} [16, 3, 23, 19] \rightarrow$ QDXT

NOIEMBRIE $\rightarrow$ XYSOW QDXT

Cu padding :

Mesaj : NOIEMBRIE

Bloc : 5 => NOIEM K1 : 10

BRIEM K2 : 15

NOIEM → XYSOW

BRIEM → QDXT.

12+15=27

NOIEMBRIEM → XYSOWQDXT.

Afin : Ec. de criptare : Cod = Mesaj · K1 + K2

$c = mk_1 + k_2$

Ec. de decriptare : mesaj = (Cod − K2) · K1⁻¹

$m = (c - k_2)\, k_1^{-1}$

Ex : Mesaj : LUNI

K1 = 5 ; K2 = 11

Flux.

[L, U, N, I] → [11, 20, 13, 8] $\xrightarrow{\cdot 5 + 11}$ [66, 111, 76, 51] $\xrightarrow{:29}$ [8, 24, 18, 22]

[i, Y, S, W]

LUNI → iYSW.

Deciptare: 5^{-1} în $Z_{29} = 6$

$[8, 24, 18, 22] \xrightarrow{\cdot 6} [11, 20, 13, 8] \rightarrow$ LUNI.

Hill

Ec. deciptare: $\begin{pmatrix} C \\ O \\ D \end{pmatrix} = MC \cdot \begin{pmatrix} M \\ S \\ J \end{pmatrix}$

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

Ex: Mesaj: Joi $\rightarrow \begin{pmatrix} J \\ O \\ I \end{pmatrix} \rightarrow \begin{pmatrix} 9 \\ 14 \\ 8 \end{pmatrix}$

MC: $\begin{pmatrix} 1 & -1 & 3 \\ 2 & -2 & 1 \\ 0 & -5 & 2 \end{pmatrix}$

$$\begin{pmatrix} 1 & -1 & 3 \\ 2 & -2 & 1 \\ 0 & -5 & 2 \end{pmatrix} \begin{pmatrix} 9 \\ 14 \\ 8 \end{pmatrix} = \begin{pmatrix} 19 \\ -2 \\ -54 \end{pmatrix} \% 29$$

$$\begin{pmatrix} 19 \\ 27 \\ 4 \end{pmatrix} = T.E$$

$$-54 = -58 + 4 = 4$$
$$\parallel$$
$$0$$

$$\det MC = \begin{vmatrix} 1 & -1 & 3 \\ 2 & -2 & 1 \\ 0 & -5 & 2 \end{vmatrix} = -4 - 30 + 5 + 4 = -25$$

$$= 4$$

$$4^{-1} \in \mathbb{Z}_{29} = 22$$

$$4^{-1} = x \Leftrightarrow 4x = 1 \in \mathbb{Z}_{29}$$

$$1 \in \mathbb{Z}_{29} = \{30, 59, 88, \dots\}$$

$$A^t = \begin{pmatrix} 1 & 2 & 0 \\ -1 & -2 & -5 \\ 3 & 1 & 2 \end{pmatrix} \Rightarrow A^* = \begin{pmatrix} 1 & -13 & 5 \\ -4 & 2 & +5 \\ -10 & +5 & 0 \end{pmatrix}$$

$$\Rightarrow A^{-1} = 4^{-1} \cdot A^* = 22 \cdot \begin{pmatrix} 1 & -13 & 5 \\ -4 & 2 & 5 \\ -10 & 5 & 0 \end{pmatrix}$$

$$22 \cdot \begin{pmatrix} 1 & -13 & 5 \\ -4 & 2 & 5 \\ -10 & 5 & 0 \end{pmatrix} \begin{pmatrix} 19 \\ 27 \\ 4 \end{pmatrix} = \begin{pmatrix} 9 \\ 14 \\ 8 \end{pmatrix} \begin{matrix} J \\ O \\ I \end{matrix}$$

Hill afin

Ec. de criptare: $\begin{pmatrix} C \\ O \\ D \end{pmatrix} = MC_1 \cdot \begin{pmatrix} M \\ S \\ J \end{pmatrix} + MC_2$

Ec. de decriptare: $\begin{pmatrix} M \\ S \\ J \end{pmatrix} = MC_1^{-1} \left(\begin{pmatrix} C \\ O \\ D \end{pmatrix} - MC_2 \right)$