Master

I Ecuații de gradul I în $\mathbb{Z}_n$

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

$\Leftrightarrow$ • $(\mathbb{Z}_n, +)$ grup comutativ (0 = el. neutru, $-a$ = opusul lui a)

• $(\mathbb{Z}_n, \cdot)$ monoid comutativ

1 = el. neutru

Nu orice element este inversabil față de „$\cdot$"

Teoremă $U(\mathbb{Z}_n)$ = mulțimea el. inv. (unități) față de „$\cdot$"

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

Ex: 1) $2x + 5 = 2$ în $\mathbb{Z}_7$

$2x = 2 - 5 = -3 = 4$

$2x = 4 \mid \cdot 2^{-1} = 4$ (pt că $2 \cdot 4 = 8 = 1$ în $\mathbb{Z}_7$)

$\underbrace{4 \cdot 2}_{1} \cdot x = 4 \cdot 4 \Rightarrow x = 4 \cdot 4 = 16 = 2$ în $\mathbb{Z}_7$

Ex2) $5x+3=1$ în $\mathbb{Z}_{11}$

$5x=1-3=-2=9$

$5x=9 \mid \cdot 5^{-1}=9$ (pt că $5\cdot 9=45=1$ în $\mathbb{Z}_{11}$)

$\Rightarrow 9\cdot 5x=9\cdot 9 \Rightarrow x=81=77+4=4$

$\Rightarrow \underline{x=4}$ în $\mathbb{Z}_{11}$

Ex3) $6x+2=3$ în $\mathbb{Z}_{10}=\{0,1,2,3,\dots,9\}$

$6x=3-2=1$

$6x=1 \mid \cdot 6^{-1}$ NU există în $\mathbb{Z}_{10}$ pt că $(6,10)=2\neq 1$

$\Rightarrow 6\notin U(\mathbb{Z}_{10})$

Rezolv (dacă se poate) $6x=1$ prin încercări

x	0	1	2	3	4	5	6	7	8	9
6x	0	6	2	8	4	0	6	2	8	4

în $\mathbb{Z}_{10}$

$\Rightarrow$ Ecuația nu are soluții în $\mathbb{Z}_{10}$.

Aplicație: Cifrul Caesar

A	B	C	D	E	F	G	H	I
0	1	2	3	4	5	6	7	8

J 9 K_{10} L_{11} M_{12} N_{13} O_{14} P_{15} Q_{16} R_{17}

S18 T19 U20 V21 W22 X23 Y24 Z25

Ar trebui să lucrăm în $\mathbb{Z}_{26}$

Dar $U(\mathbb{Z}_{26}) = \{1,3,5,7,9,11,15,17,19,21,23,25\}$

Deci Adaug 26 27 ?28 $\Rightarrow \mathbb{Z}_{29}$

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

Var 1: Caesar flux (stream cipher) = = o cheie pt tot mesajul

Ec-de criptare: Mesaj + Cheie = Cod } în $\mathbb{Z}_{29}$

Ec-de decriptare: Cod − cheie = Mesaj

Ex 1: Mesaj = MARTI

Cheia = 24

$[M,A,R,T,I] \to [12,0,17,19,8] \xrightarrow[\text{mod } 29]{+\text{cheia}}$ (+24)

$\to [36,24,41,43,32] \xrightarrow{\text{mod } 29} [7,24,12,14,3]$

$\to$ HYMOD

MARTI $\xrightarrow[\text{mod } 29]{+\text{cheie}}$ HYMOD

mesaj cod

Decriptare: [H, Y, M, O, D] → [7, 24, 12, 14, 3]

$\xrightarrow[\text{mod } 29]{-24\text{-cheie}}$ [-17, 0, -12, -10, -21] $\xrightarrow{\text{mod } 29}$

[12, 0, 17, 19, 8] → MARTI

Decriptare: HYMOD $\xrightarrow{-\text{cheie}}$ MARTI

Cod Mesaj

Varianta Pe blocuri fără padding =
= o cheie pt fiecare bloc

Fără padding: ≤ 1 bloc mai scurt

Ex: Mesaj: OCTOMBRIE

Bloc: 5 ⇒ bloc1: OCTOM; bloc2: BRIE

cheie1: 7 ; cheie2: 11

[O, C, T, O, M] → [14, 2, 19, 14, 12] $\xrightarrow[\text{mod } 29]{+7\ +\text{cheie1}}$

→ [21, 9, 26, 21, 19] → VJ_VT

[BR, I, E] → [1, 17, 8, 4] $\xrightarrow[\text{mod } 29]{+11}$ [12, 28, 19, 15]

→ M?TP

OCTOMBRIE ⟶ VJ_VTM?TP

Ex.: OCTOMBRIE, bloc: 3

b1: OCT ; K1 = 5

b2: OMB ; K2 = 17

b3: RIE ; K3 = 20

Var 2: Pe blocuri cu padding RANDOM (zgomot) — blocuri egale

Ex: Mesaj: MARTI

Bloc: 3 ⇒ b1: MAR K1: 5

b2: TIE K2: 11

$[M,A,R] \to [12,0,17] \xrightarrow[\text{mod } 29]{+5} [17,5,22] \to$

$\to [R,F,W]$

$[T,I,E] \to [19,8,4] \xrightarrow[\text{mod } 29]{+11} [30,19,15] \xrightarrow{\text{mod } 29}$

$\to [1,19,15] \to [B,T,P]$

MARTIE ⟶ RFWBTP

Cifrul afin

1) Flux: Ec. de criptare:

$$\text{Mesaj} \cdot \text{cheie1} + \text{cheie2} = \text{Cod}$$

Ec. de decriptare:

$$(\text{Cod} - \text{cheie2}) \cdot \text{cheie1}^{-1} = \text{Mesaj}$$

Ex: Mesaj: MARTI

cheie1: 2

cheie2: 5

Cript

$m \cdot K1 + K2 = C$

Decript.

$m = (C - K2) \cdot K1^{-1}$

$$[M, A, R, T, I] \xrightarrow{\substack{\cdot 2 + 5 \\ \cdot K1 + K2 \\ \text{mod } 29}} [12, 0, 17, 19, 8]$$

$$\rightarrow [29, 5, 39, 43, 21] \xrightarrow{\text{mod } 29} [0, 5, 10, 14, 21]$$

$$\rightarrow [A, F, K, O, V]$$

MARTI $\longrightarrow$ AFKOV Afin $\begin{matrix} k1=2 \\ k2=5 \end{matrix}$

Decriptare $2m + 5 = c$ pt fiecare $m \in$ Mesaj, $c \in$ Cod

$\Rightarrow m = (c - 5) \cdot 2^{-1}$ în $\mathbb{Z}_{29}$

$2^{-1} = 15$ pt că $2 \cdot 15 = 30 = 1$ în $\mathbb{Z}_{29}$

$m = (c-5)\cdot 15$, $\forall\, c \in Cod$, $m \in Mesaj$

$[A, F, K, O, V] \longrightarrow [0, 5, 10, 14, 21] \xrightarrow[\text{mod } 29]{-5,\ \cdot 15} [-75, 0, 75, 135, 240] \xrightarrow{\text{mod } 29} [12, 0, 17, 19, 8]$ (M A R T i) OK

$-75 = -58 - 17 = -17 = 12 \bmod 29$

$75 = 58 + 17 = 17 \bmod 29$

$135 = 116 + 19 = 19 \bmod 29$

$240 = 232 + 8 = 8 \bmod 29$

$29\cdot 2 = 58$

$29\cdot 3 = 87$

$29\cdot 4 = 116$

$29\cdot 5 = 145$

$29\cdot 8 = 232$

Varianta: Pe blocuri, fără padding

Pt. fiecare bloc: Criptare $m \cdot K1 + K2 = c$, $\forall\, m \in Mesaj$, $c \in Cod$

Decriptare: $m = (c - K2)K1^{-1}$, $\forall\, m \in Mesaj$, $c \in Cod$.

Fiecare bloc va avea câte 2 chei.

b) Cu padding RANDOM.

La fel, doar se mărește ultimul bloc dacă e cazul.

Inverse matriceale $M_3(Z_n)$

Ex: $A = \begin{pmatrix} 2 & 1 & -1 \\ 0 & 3 & 4 \\ 1 & 1 & -2 \end{pmatrix} \in M_3(Z_7)$

$A^{-1} = ?$ dacă există.

Teoremă $A \in M_n(Z_t)$ este inversabilă $\Leftrightarrow \det A \in U(Z_t)$.

$\det A = -12 + 4 + 3 - 8 = -13 = -7 - 6 = -6 = 1$

$1 \in U(Z_7) \Rightarrow$ există A^{-1} $\quad (-1)^{l+c}$

$A \to A^t = \begin{pmatrix} 2 & 0 & 1 \\ 1 & 3 & 1 \\ -1 & 4 & -2 \end{pmatrix} \to A^* = \begin{pmatrix} -10 & +1 & 7 \\ +4 & -3 & -8 \\ -3 & -1 & 6 \end{pmatrix}$

$A^* = \begin{pmatrix} 4 & 1 & 0 \\ 4 & 4 & 6 \\ 4 & 6 & 6 \end{pmatrix} \in M_3(Z_7)$

$A^{-1} = \underbrace{(\det A)^{-1}}_{1} \cdot A^* = A^*$

Ex: $A = \begin{pmatrix} -1 & 2 & 1 \\ 3 & 1 & 0 \\ 2 & 0 & -1 \end{pmatrix} \in \mathcal{M}_3(\mathbb{Z}_{11})$

$\det A = 1 - 2 + 6 = 5 \in U(\mathbb{Z}_{11}) \Rightarrow \exists A^{-1}$

$(\det A)^{-1} = 5^{-1} \text{ în } \mathbb{Z}_{11} = 9 \quad (\text{pt că } 5 \cdot 9 = 1 \text{ în } \mathbb{Z}_{11})$

$A \to A^t = \begin{pmatrix} -1 & 3 & 2 \\ 2 & 1 & 0 \\ 1 & 0 & -1 \end{pmatrix} \to A^* = \begin{pmatrix} -1 & +2 & -1 \\ +3 & -1 & +3 \\ -2 & +9 & -7 \end{pmatrix}$

$\Rightarrow A^* = \begin{pmatrix} 10 & 2 & 10 \\ 3 & 10 & 3 \\ 9 & 9 & 9 \end{pmatrix} \in \mathcal{M}_3(\mathbb{Z}_{11})$

$A^{-1} = (\det A)^{-1} \cdot A^* = 9 \cdot A^* = \begin{pmatrix} 90 & 18 & 90 \\ 27 & 90 & 27 \\ 81 & 36 & 36 \end{pmatrix}$

$\Rightarrow A^{-1} = \begin{pmatrix} 2 & 7 & 2 \\ 5 & 2 & 5 \\ 9 & 3 & 3 \end{pmatrix} \in \mathcal{M}_3(\mathbb{Z}_{11})$