1342a - Aritmetică modulară (în Z_n)

$Z_n = \{0, 1, 2, \ldots, n-1\}$

$(Z_n, +, \cdot)$ inel comutativ

$\rightarrow (Z_n, +)$ grup comutativ

$\rightarrow (Z_n, \cdot)$ monoid comutativ

Ex: $Z_7 = \{0, 1, 2, 3, 4, 5, 6\}$

$0 = \{0, \pm 7, \pm 14, \pm 21, \pm 28, \ldots\} = \{7k \mid k \in Z\}$

$1 = \{1, 8, 15, 22, 29, \ldots\} = \{7k+1 \mid k \in Z\}$

$-a$ = opusul elementului a

= simetricul față de $+$

$-3 = x \Leftrightarrow x + 3 = 0 \Rightarrow -3 = 4$

a^{-1} = inversul el. a

= simetricul față de $\cdot$.

$3^{-1} = y \Leftrightarrow 3y = 1 \Rightarrow y = 3^{-1} = 5 \Rightarrow 5^{-1} = 3$

$2^{-1} = 4$; $6^{-1} = 6$

$U(\mathbb{Z}_n) = \{ x \in \mathbb{Z}_n \mid \text{există } x^{-1} \}$

↑ grupul unităților $(U(\mathbb{Z}_n), \cdot)$ grup com.

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

Ex: $U(\mathbb{Z}_7) = \mathbb{Z}_7^* = \mathbb{Z}_7 - \{0\}$

$U(\mathbb{Z}_{10}) = \{1, 3, 7, 9\}$

$3^{-1} = 7 \Rightarrow 7^{-1} = 3 \; ; \; 9^{-1} = 9$

Ec. de gradul I

$2x + 5 = 1$ în $\mathbb{Z}_7$

$2x = 1 - 5 = -4 \longrightarrow x = -2 = 5$

$\downarrow$

$2x = 3 \quad | \cdot 2^{-1} \Leftrightarrow \underbrace{2^{-1} \cdot 2}_{1} \cdot x = 2^{-1} \cdot 3$

$1 \cdot x = x = 4 \cdot 3 = 12 = 5$

$2x + 5 = 1$ în $\mathbb{Z}_6$ nu are soluție.

$U(\mathbb{Z}_6) = \{1, 5\} \neq 2$

Ec de gradul al II-lea

$3x^2 - 2x + 4 = 1$ în $\mathbb{Z}_7$

$3x^2 - 2x + 3 = 0$

$\Delta = 4 - 4 \cdot 3 \cdot 3 = 4 - 36 = -32 = -28 - 4 \overset{!!}{=} 0$

$= -4 = 3$

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

$\sqrt{3} = a$ în $\mathbb{Z}_7 \Leftrightarrow a^2 = 3$ în $\mathbb{Z}_7$

$0^2 = 0;\ 1^2 = 1;\ 2^2 = 4;\ 3^2 = 2;\ 4^2 = 2;\ 5^2 = 4;\ 6^2 = 1$

$\Rightarrow \sqrt{3}$ nu există în $\mathbb{Z}_7 \Rightarrow$ ec. nu are sol.

$x^2 - 5x + 6 = 0$ în $\mathbb{Z}_{11}$

$\Delta = 25 - 4 \cdot 6 = 1$

$\sqrt{1} \in \{1, 10\} = \{1, -1\}$

$x_{1,2} = (5 \pm \sqrt{1}) \cdot 2^{-1} = (5 \pm 1) \cdot 6$

$x_1 = 6 \cdot 6 = 3\ ;\ x_2 = 4 \cdot 6 = 2$

$x \in \{2, 3\}$

Logaritmul discret

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

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

$2^0 = 1$; $2^1 = 2$; $2^2 = 4$; $2^3 = 3 \Rightarrow \log_2 3 = 3$ în $\mathbb{Z}_5$

$\log_2 3$ în $\mathbb{Z}_7$ nu există

$2^0 = 1$; $2^1 = 2$; $2^2 = 4$; $2^3 = 1$; $2^4 = 2$; $2^5 = 4$

Teorema lui Lagrange (pt grupuri)

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

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

Obs: $(\mathbb{Z}_p^*, \cdot)$ grup

p nr prim

În plus, $\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$

În $\mathbb{Z}_{11}$, $4^{50} = ?$

$4^{50} = (4^2)^{25} = 16^{25} = 5^{25} = (5^5)^5 = 1^5 = 1.$

$5^5 = 5^2 \cdot 5^2 \cdot 5 = 3 \cdot 3 \cdot 5 = 1$

$3 \cdot 3 = 4$

$A \in \mathcal{M}_n(\mathbb{Z}_t)$

$A^{-1} = (\det A)^{-1} \cdot A^*$ există $\Leftrightarrow$

$\text{cmmdc}(\det A, t) = 1.$

$\Leftrightarrow$, $\det A \in U(\mathbb{Z}_t)$.

Algoritmi criptografici bazați pe Z_n

1. Flux (stream cipher): o cheie pt tot mesj.
2. Pe blocuri (block cipher): o cheie pt 1 bloc
   a) fără padding: ≤1 bloc mai scurt
   b) cu padding: toate blocurile au ac. lungime

Z_{29}					Z_{26}			Z_{29}
A	B	C	D	...	Z	_	.	?
0	1	2	3	...	25	26	27	28

Cifrul Caesar

- Ec. de criptare: Cod = Mesaj + Cheie
  $c = m + K$ în Z_{29}
- Ec. de decriptare: $m = c - K$

Flux: Mesaj: ANDREEA
cheia: 15

[ANDREEA] → [A, N, D, R, E, E, A] →

→ [0, 13, 3, 17, 4, 4, 0] $\xrightarrow[+15]{+K}$

→ [15, 28, 18, 32, 19, 19, 15] $\xrightarrow{\%29}$

[15, 28, 18, 3, 19, 19, 15] → P?SDTTP

Decriptare:

P?SDTTP → [15, 28, 18, 3, 19, 19, 15] $\xrightarrow[-15]{-K}$

→ [0, 13, 3, −12, 4, 4, 0] $\xrightarrow{\%29}$

→ [0, 13, 3, 17, 4, 4, 0] → ANDREEA

Re Slovură: Mesaj: ANDREEA

fără padding Bloc: b = 5 ⇒ ANDRE K1 = 20

EA K2 = 9

[A, N, D, R, E] → [0, 13, 3, 17, 4] $\xrightarrow[+20]{+K1}$

→ [20, 33, 23, 37, 24] $\xrightarrow{\%29}$

→ [20, 4, 23, 8, 24] → UEXIY

[E, A] → [4, 0] $\xrightarrow[+9]{+K2}$ [13, 9] → NJ

UEXIY NJ

Pe blocuri: Mesaj: ANDREEA
cu padding Bloc: b=5 ⇒ 1 ANDRE, K1=20
EATID, K2=9

[A,N,D,R,E] → [0,13,3,17,4] $\xrightarrow[+20]{+K}$

[20,33,23,37,24] $\xrightarrow{\%29}$ [20,4,23,8,24] →

→ UEXiY

[E,A,T,i,D] → [4,0,19,8,3] $\xrightarrow[+9]{+K2}$

[13,9,28,17,12] → NJ?RM

ANDREEATiD → UEXiYNJ?RM

ANDREEA, b=5

ANDRX EEAYT

Cifrul afin

- Ec. de criptare: $c = m \cdot K1 + K2$
- Ec. de decriptare: $(C - K2) \cdot K1^{-1} = m$

Ex: Mesaj: AZi Flux.

K1: 5 ; K2: 12

$[A,Z,i] \to [0,25,8] \xrightarrow[\cdot 5+12]{\cdot K1+K2} [12,137,52]$

$\xrightarrow{\%29} [12,21,23] \to MVX.$

$137 = 145-8 \ \%29 = -8 = 21$

$52 = 58-6 \ \%29 = -6 = 23$

Decriptarea: $C = m \cdot 5 + 12 \Rightarrow m = (C-12) \cdot 5^{-1}$

$5^{-1} \in Z_{29} = 6 \qquad m = (C-12) \cdot 6$

$[M,V,X] \to [12,21,23] \xrightarrow{-12 \cdot 6} [0,54,66]$

$\xrightarrow{\%29} [0,25,8] \to AZi$

Hill:

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

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

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

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

$$\begin{pmatrix} C \\ O \\ D \end{pmatrix} = \begin{pmatrix} -2 & 0 & 1 \\ 1 & -1 & 1 \\ 0 & 2 & -3 \end{pmatrix} \cdot \begin{pmatrix} 9 \\ 14 \\ 8 \end{pmatrix} = \begin{pmatrix} -10 \\ 3 \\ 4 \end{pmatrix} \mid 29$$

$$\begin{pmatrix} 19 \\ 3 \\ 4 \end{pmatrix} = \begin{pmatrix} T \\ D \\ E \end{pmatrix}$$

Decriptare: $\det MC = -6 + 2 + 4 = 0$

$\Rightarrow$ MC nu este inversabilă!

$\Rightarrow$ Mesajul nu se poate decripta

Mesaj: A2i $\rightarrow \begin{pmatrix} 0 \\ 25 \\ 8 \end{pmatrix}$

$$MC = \begin{pmatrix} 0 & 1 & -1 \\ 2 & 0 & 1 \\ -1 & 1 & 1 \end{pmatrix} \quad \det MC = -1 - 2 - 2 = -5 = 24$$

Criptarea: $\begin{pmatrix} c \\ o \\ d \end{pmatrix} = \begin{pmatrix} 0 & 1 & -1 \\ 2 & 0 & 1 \\ -1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 25 \\ 8 \end{pmatrix}$

$= \begin{pmatrix} 17 \\ 8 \\ 33 \end{pmatrix} \% 29 = \begin{pmatrix} 17 \\ 8 \\ 4 \end{pmatrix} = \begin{pmatrix} R \\ i \\ E \end{pmatrix}$

<u>Decriptarea</u>: $MC^{-1} = 24^{-1} \cdot MC^{*}$

24^{-1} în $\mathbb{Z}_{29} = x \Leftrightarrow$ $24x = 1$ în $\mathbb{Z}_{29}$

1 în $\mathbb{Z}_{29} = \{1, 30, 59, 88, 117, 146, 175,$
$204, 233, 262, 291,$
$320, 349, 378, 407, 436,$
$465, 494, 523, 552$

$552 = 24 \cdot 23$

$\Rightarrow x = 23$

$$MC^t = \begin{pmatrix} 0 & 2 & -1 \\ 1 & 0 & 1 \\ -1 & 1 & 1 \end{pmatrix} \rightarrow MC^* = \begin{pmatrix} -1 & -2 & 1 \\ -3 & -1 & -2 \\ 2 & -1 & -2 \end{pmatrix}$$

$$\Rightarrow MC^{-1} = 23 \cdot \begin{pmatrix} -1 & -2 & 1 \\ -3 & -1 & -2 \\ 2 & -1 & -2 \end{pmatrix}$$

$$\begin{pmatrix} M \\ S \\ J \end{pmatrix} = 23 \cdot \begin{pmatrix} -1 & -2 & 1 \\ -3 & -1 & -2 \\ 2 & -1 & -2 \end{pmatrix} \cdot \begin{pmatrix} 17 \\ 8 \\ 4 \end{pmatrix}$$

$$= \begin{pmatrix} 0 \\ 25 \\ 8 \end{pmatrix} = \begin{pmatrix} A \\ Z \\ I \end{pmatrix}$$

Hill afin:

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

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