<u>1343b</u> – Aritmetică modulară (în Z_n)

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

$\rightarrow (Z_n, +)$ grup comutativ

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

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

− a = opusul elem. a
   = simetricul în raport cu „+"

−3 = X pt care $3 + x = 0 \Rightarrow -3 = 4$

a^{-1} = inversul elem. a
   = simetricul față de „·"

$3^{-1} = X$ pt care $3X = 1 \Rightarrow 3^{-1} = 5 \Rightarrow 5^{-1} = 3$

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

$Z_{10} = \{0, 1, \ldots, 9\}$

$3^{-1} = 7$; 5^{-1} nu există   grupul unităților

Def: $U(Z_n) = \{x \in Z_n \mid \text{există } x^{-1}\}$

Tlm: $U(Z_n) = \{x \in Z_n \mid \text{cmmdc}(x, n) = 1\}$

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

$1^{-1} = 1$; $9^{-1} = 9$

$(U(Z_{10}), \cdot)$ grup comutativ.

Ec. de gradul I

- $3x + 2 = 1$ în Z_7

  $3x = 1 - 2 = -1 = 6 \Rightarrow x = 2$

  sau: $3x = -1 \mid \cdot 3^{-1}$

  $\underbrace{3^{-1} \cdot 3} \cdot x = (-1) \cdot 3^{-1}$

  $x = (-1) \cdot 5 = -5 = 2$

- $\boxed{4}x - 1 = 5$ în Z_{10} nu are sol. p⁺ că

  $4 \notin U(Z_{10})$.

- $4x + 1 = 5$ în Z_{10}

  $4x = 4 \boxed{=1} x = 1$ (NU)

Ec. de gradul II

- $2x^2 - 5x + 1 = 3$ în Z_{11}

  $2x^2 - 5x - 2 = 0$

$$\Delta = 25 - 4 \cdot 2 \cdot (-2) = 3 + 5 = 8$$

$$\sqrt{8} = a \Rightarrow a^2 = 8$$

$$0^2 = 0; \ 1^2 = 1; \ 2^2 = 4; \ 3^2 = 9; \ 4^2 = 5; \ 5^2 = 3; \ 6^2 = 3;$$

$$7^2 = 5; \ 8^2 = 9; \ 9^2 = 4; \ 10^2 = 1$$

$$\Rightarrow \sqrt{8} \text{ nu există în } Z_{11} \Rightarrow \text{ ec. nu are sol.}$$

- $x^2 - 5x + 6 = 0$ în Z_{13}

$$\Delta = 25 - 24 = 1 \Rightarrow \sqrt{\Delta} = \{1, 12\} = \{1, -1\}$$

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

$$x_1 = 6 \cdot 7 = 42 = 3 \quad \Big| \Rightarrow x \in \{2, 3\}.$$
$$x_2 = 4 \cdot 7 = 28 = 2 \quad \Big|$$

Logaritmul discret

$$\color{red}{\log_a b = c \Leftrightarrow a^c = b}$$

$$\log_2 3 \text{ în } Z_5 \Rightarrow 2^x = 3 \text{ în } Z_5 \quad \Big| \Rightarrow \log_2 3 = 3$$
$$2^0 = 1; \ 2^1 = 2; \ 2^2 = 4; \ 2^3 = 3 \quad \Big| \quad \text{în } Z_5$$

$\log_2 3$ în $\mathbb{Z}_7 \Rightarrow 2^x = 3$ în $\mathbb{Z}_7$

$\underbrace{2^0 = 1; \ 2^1 = 2; \ 2^2 = 4;}_{} \ \underbrace{2^3 = 1; \ 2^4 = 2; \ 2^5 = 4}_{}$

$\Rightarrow$ nu există.

$\log_a b$ în $\mathbb{Z}_n \Leftrightarrow a^x = b$ în $\mathbb{Z}_n, \ x \in \{0, 1, \ldots, n-1\}$

Teorema lui Lagrange pt grupuri

$(G, \cdot)$ grup, $g \in G \Rightarrow g^n = e.$

Dacă $\#G = n$

$\underline{Obs}$: $\left(\mathbb{Z}_p^*, \cdot \right)$ grup $\quad \underline{\#\mathbb{Z}_p^* = p-1.}$

$\quad\quad p$ nr. prim

$\left(\mathbb{Z}_{23}^*, \cdot \right) \quad \log_5 11$ în $\mathbb{Z}_{23}$

$5^x = 11$ în $\mathbb{Z}_{23} \ , \ x \in \{0, \ldots, 22\}$

4^{100} în $\mathbb{Z}_{11} = ?$

$4^{100} = (4^2)^{50} = (16)^{50} = 5^{50} = (5^2)^{25} = 1^{25} = 1$

$= 3^{25} = (3^5)^5$

$3^5 = \underbrace{3^2 \cdot 3^2 \cdot 3}_{5} = 1$

$A \in M_n(\mathbb{Z}_t)$

$A^{-1} = (\det A)^{-1} \cdot A^*$ există $\iff \det A$ este element

inversabil în $\mathbb{Z}_t \iff \det A \in U(\mathbb{Z}_t) \iff$

$\quad cmmdc(\det A, t) = 1$

Alg. criptografici bazați pe $\mathbb{Z}_n$

1) Flux (stream cipher): aceeași cheie pt tot mesajul

2) Pe blocuri (block cipher): 1 cheie / 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	$\sqcup$	.	?
0	1	2	3	---	25	26	27	28

Caesar

$$c = m + k$$

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

Ec. de decriptare: $m = c - k$

Ex: Flux: Mesaj: A N D R E E A

cheia: 21

$$[A, N, D, R, E, E, A] \rightarrow [0, 13, 3, 17, 4, 4, 0]$$

$$\xrightarrow{+21} [21, 34, 24, 38, 25, 25, 21]$$

$$\xrightarrow{\% 29} [21, 5, 24, 9, 25, 25, 21]$$

$$\rightarrow V F Y J Z Z V$$

Decriptare:

$VFYJZZV \rightarrow [21, 5, 24, 9, 25, 25, 21]$

$\xrightarrow{-21} [0, -16, 3, -12, 4, 4, 0] \xrightarrow{\%29}$

$\rightarrow [0, 13, 3, 17, 4, 4, 0] \rightarrow ANDREEA$

Pe blocuri, fără padding

Mesaj: ANDREEA

Bloc: b=5 $\Rightarrow$ ANDRE   K1:5

EA   K2:12

$[A, N, D, R, E] \rightarrow [0, 13, 3, 17, 4] \xrightarrow[+5]{+K1}$

$\rightarrow [5, 18, 8, 22, 9] \rightarrow FSIWJ$

$[E, A] \rightarrow [4, 0] \xrightarrow[+12]{+K2} [16, 12] \rightarrow QM$

ANDREEA $\rightarrow$ FSIWJQM

Pe blocuri, cu padding

Mesaj: ANDREEA   ANDRE $K_1 = 11$

Bloc: $b = 5$ $\Rightarrow$ EAMDS, $K_2 = 7$

$$[A, N, D, R, E] \rightarrow [0, 13, 3, 17, 4] \xrightarrow{+K_1}$$

$$\rightarrow [11, 24, 14, 28, 15] \rightarrow L Y O ? . P$$

$$[E, A, M, D, S] \rightarrow [4, 0, 12, 3, 18] \xrightarrow[+7]{+K_2}$$

$$[11, 7, 19, 10, 25] \rightarrow L H T K Z$$

ANDREEAMDS $\rightarrow$ LYO?.PLHTKZ

Cifrul afin

Ec. de criptare: $C = m \cdot K_1 + K_2$

Ec. de decriptare: $m = (C - K_2) \cdot K_1^{-1}$

Ex: Mesaj: CAIET   flux

Cheia 1: $K_1 = 5$

Cheia 2: $K_2 = 15$

$$[C, A, I, E, T] \rightarrow [2, 0, 8, 4, 19] \xrightarrow[\cdot 5 + 15]{\cdot K1 + K2}$$

$$\rightarrow [25, 15, 55, 35, 110] \xrightarrow{\% 29}$$

$$\rightarrow [25, 15, 26, 6, 23] \longrightarrow ZP\_GX$$

$$55 = 58 - 3 = -3 = 26$$

$$110 = 116 - 6 = -6 = 23$$

$$CAIET \rightarrow ZP\_GX$$

$\underline{Decriptare}$: $c = m \cdot 5 + 15 \Rightarrow m = (C - 15) \cdot 5^{-1}$

$$5^{-1} \text{ ĭ } Z_{29} = 6$$

$$ZP\_GX \rightarrow [25, 15, 26, 6, 23] \xrightarrow{-15; 6} [60, 0, 66, -54, 48]$$

$$\xrightarrow{\% 29} [2, 0, 8, 4, 19] \rightarrow CAIET.$$

$\overline{Ex.}$ afin pe blocuri; fără padding

Mesaj: CAIET

Bloruri: $b = 3$ $\begin{array}{l} CAI \rightarrow K1 = 2; K2 = 5 \\ ET \rightarrow K3 = 10; K4 = 2 \end{array}$

$$[C, A, I] \rightarrow [2, 0, 8] \xrightarrow{\cdot 2 + 5} [9, 5, 21]$$
$$JFV$$

$\rightarrow [13, 18] \rightarrow NS$

$\dfrac{29}{\underset{203}{7}}$

$192 = 203 - 11 = -11 = 18$
$\underset{0}{\%}$

$CAIET \rightarrow J F V N S.$

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: $\begin{pmatrix} M \\ S \\ J \end{pmatrix} = \begin{pmatrix} J \\ O \\ i \end{pmatrix} = \begin{pmatrix} 9 \\ 14 \\ 8 \end{pmatrix}$

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

$\begin{pmatrix} C \\ O \\ D \end{pmatrix} = \begin{pmatrix} -1 & 0 & 2 \\ 1 & -1 & 1 \\ -2 & -1 & 1 \end{pmatrix} \begin{pmatrix} 9 \\ 14 \\ 8 \end{pmatrix} = \begin{pmatrix} 7 \\ 3 \\ -24 \end{pmatrix} \% 29 \begin{pmatrix} 7 \\ 3 \\ 5 \end{pmatrix} \begin{matrix} H \\ D \\ F \end{matrix}$

$$\det MC = \begin{vmatrix} -1 & 0 & 2 \\ 1 & -1 & 1 \\ -2 & -1 & 1 \end{vmatrix} = 1 - 2 - 4 - 1$$

$$= -6 = 23$$

$(\det MC)^{-1} = 23^{-1} = 24$

$23^{-1} = x \iff 23x = 1 \text{ în } \mathbb{Z}_{29}$

$MC^{-1} = 24 \cdot MC^{*}$

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

$$\begin{pmatrix} M \\ S \\ J \end{pmatrix} = 24 \cdot \underbrace{\begin{pmatrix} 0 & -2 & 2 \\ -3 & 3 & 3 \\ -3 & -1 & 1 \end{pmatrix}}_{MC^{-1}} \begin{pmatrix} 7 \\ 3 \\ 5 \end{pmatrix} = \begin{pmatrix} 9 \\ 14 \\ 8 \end{pmatrix}$$

$\begin{pmatrix} C \\ O \\ D \end{pmatrix}$

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