13426

Ecuații, sisteme, matrice în $\mathbb{Z}_n$ → CAESAR AFIN

Ec. de gradul I

Ex: $2x+5=3$ în $\mathbb{Z}_7$

$2x=3-5=-2=5$ → fals $2x=-2 \Rightarrow x=-1=6$

$2x=5$ în $\mathbb{Z}_7 \mid \cdot 4=2^{-1}$

$2\cdot 4\cdot x=5\cdot 4 \Rightarrow x=20=6 \Rightarrow x=6$

Ex: $5x+2=1$ în $\mathbb{Z}_{10}$

$5x=1-2=-1=9 \mid \cdot 5^{-1}$ NU există în $\mathbb{Z}_{10}$!

Teoremă a este inversabil în $\mathbb{Z}_n \Leftrightarrow \text{cmmdc}(a,n)=1$

$5x=9$ Rezolvăm prin încercări

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

$\neq 9 \Rightarrow$ Ec. nu are soluție

Sisteme liniare

Ex: $\begin{cases} 2x+3y=1 \\ 5x-y=2 \end{cases}$ în $\mathbb{Z}_7$

Matricea sistemului $A=\begin{pmatrix} 2 & 3 \\ 5 & -1 \end{pmatrix} \in M_2(\mathbb{Z}_7)$

$\det A=-2-15=-17=-14-3=-3=4 \in U(\mathbb{Z}_7)$

$\neq 0$

$\Rightarrow$ sist. este Cramer $\Rightarrow$ are sol. unică

$$\begin{cases} 2x+3y=1 \\ 5x-y=2 \mid \cdot 3 \end{cases} \Rightarrow \begin{cases} 2x+3y=1 \\ \underline{15x-3y=6} \\ \quad (+) \end{cases}$$

$$\Rightarrow 17x=7 \Rightarrow 3x=0 \Rightarrow \underline{x=0}$$

$$2x+3y=1 \Rightarrow 3y=1 \mid \cdot 3^{-1}=5 \Rightarrow \underline{y=5}$$

Ex: $\begin{cases} x+2y=4 \\ 3x+4y=1 \end{cases}$ în $\mathbb{Z}_{10}$

$$A=\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \in \mathcal{M}_2(\mathbb{Z}_{10}) \; ; \det A = 4-6=-2=8$$

$\det A = 8 \notin U(\mathbb{Z}_{10}) \Rightarrow \det A$ este divizor al lui zero.
$(8 \cdot 5 = 0$ în $\mathbb{Z}_{10})$

$\Rightarrow$ Syst NU este Cramer.

$$\begin{cases} x+2y=4 \mid \cdot 2 \\ 3x+4y=1 \end{cases} \Rightarrow \begin{cases} 2x+4y=8 \\ 3x+4y=1 \mid - \end{cases}$$

$$\Rightarrow x=-7=3 \checkmark$$

$x+2y=4 \Rightarrow 3+2y=4 \Rightarrow 2y=1 \Rightarrow y=2^{-1}$ NU există în $\mathbb{Z}_{10}$ ✗

$\Rightarrow$ Syst. nu are soluții.

Ec. de gradul II

Ex: $X^2+3X-1=0$ în $\mathbb{Z}_5$

$a=1;\ b=3;\ c=-1$

$\Delta=b^2-4ac=9+4=13=3$

$\exists\sqrt{3}$ în $\mathbb{Z}_5$? $\sqrt{3}=y \Leftrightarrow y^2=3$ în $\mathbb{Z}_5$ NU

$\mathbb{Z}_5=\{0,1,2,3,4\}$; $P(\mathbb{Z}_5)=\{0,1,4\}\not\ni 3$

(pătrate)

$\Rightarrow \nexists\sqrt{3}$ în $\mathbb{Z}_5 \Rightarrow$ ec. nu are soluții.

Ex: $x^2-5x+7=1$ în $\mathbb{Z}_{11}$

$x^2-5x+6=0$ în $\mathbb{Z}_{11}$ $\qquad 2^{-1}$ în $\mathbb{Z}_{11}=6$

$a=1;\ b=-5;\ c=6$

$\Delta=b^2-4ac=25-24=1$

$\exists\sqrt{1}$ în $\mathbb{Z}_{11}$ DA $\Rightarrow \sqrt{1}\in\{1,10\}$ (-1)

$x_1=(5+1)\cdot 2^{-1}=6\cdot 6=36=3$

$x_2=(5-1)\cdot 2^{-1}=4\cdot 6=24=2$

Dacă iau $\sqrt{1}=10$ — NU sunt necesare!!

$x_3=(5+10)\cdot 2^{-1}=15\cdot 6=4\cdot 6=2$

$x_4=(5-10)\cdot 2^{-1}=-5\cdot 6=-30=-22-8=-8=3$

Inverse matriceale → HILL

Ex: $A = \begin{pmatrix} 2 & -1 & 0 \\ 1 & 1 & 1 \\ -1 & 0 & 1 \end{pmatrix} \in \mathcal{M}_3(\mathbb{Z}_5)$ $A^{-1} = ?$ dacă există

$\det A = 2 + 1 + 1 = 4 \in U(\mathbb{Z}_5) \Rightarrow \exists A^{-1}$.

$(\det A)^{-1} = 4^{-1} = 4$

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

$A^{-1} = (\det A)^{-1} \cdot A^* = 4 \cdot \begin{pmatrix} 1 & 1 & -1 \\ -2 & 2 & -2 \\ 1 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 4 & 4 & -4 \\ -8 & 8 & -8 \\ 4 & 4 & 12 \end{pmatrix}$

$\Rightarrow A^{-1} = \begin{pmatrix} 4 & 4 & 1 \\ 2 & 3 & 2 \\ 4 & 4 & 2 \end{pmatrix}$

Ex: $A = \begin{pmatrix} 2 & 1 & -1 \\ 1 & -2 & 1 \\ 0 & 2 & 0 \end{pmatrix} \in \mathcal{M}_3(\mathbb{Z}_7)$ $A^{-1} = ?$ dacă există

$\det A = -2 - 4 = -6 = 1 \in U(\mathbb{Z}_7) \Rightarrow \exists A^{-1}$

$(\det A)^{-1} = 1^{-1} = 1$

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

$$A^{-1} = (\det A)^{-1} \cdot A^* = 1 \cdot A^* = A^* = \begin{pmatrix} -2 & -2 & -1 \\ 0 & 0 & -3 \\ 2 & -4 & 5 \end{pmatrix}$$

$$\Rightarrow A^{-1} = \begin{pmatrix} 5 & 5 & 6 \\ 0 & 0 & 4 \\ 2 & 3 & 2 \end{pmatrix}$$

$$A \cdot A^{-1} = A^{-1} \cdot A = I_3$$

Logaritmul discret → DIFFIE-HELLMAN

$\log_a b = c \Leftrightarrow a^c = b$ ($\in \mathbb{R}$, in $\mathbb{Z}_n$)

Ex: $\log_3 2$ în $\mathbb{Z}_7$

$\log_3 2 = x \Leftrightarrow 3^x = 2$ în $\mathbb{Z}_7 \Rightarrow x = 2$

$3^0 = 1$; $3^1 = 3$; $3^2 = 9 = 2$

$\Rightarrow \boxed{\log_3 2 = 2 \text{ în } \mathbb{Z}_7}$

Ex: $\log_3 2$ în $\mathbb{Z}_{11}$

$\log_3 2 = x \in \mathbb{N}$ $3^x = 2$ în $\mathbb{Z}_{11}$

Sol1: Calculez puterile lui 3 mod 11

n	0	1	2	3	4	5	6	7	8	9	10
$3^n \bmod 11$	1	3	9	5	4	1	3	9	5	4	1

$\Rightarrow \text{ord}\,3 = 5$ în $\mathbb{Z}_{11}^*$

$\Rightarrow \log_3 2$ nu ex. în $\mathbb{Z}_{11}^*$

Teorema lui Lagrange pt grupuri

G grup finit cu n elemente, $g \in G$

$\Rightarrow \text{ord}\,g \mid n$

În particular, $g^n = e$, el. neutru.

! Multiplicativ, lucrăm cu $\mathbb{Z}_n^* \Rightarrow \#\mathbb{Z}_n^* = n-1$

Sol2: Soluția $3^x = 2$ în $\mathbb{Z}_{11}$ este sol. $3^x = 11k+2$

$11k+2 = \{2, 13, 24, 35, 46, 57, \ldots \ldots \sim 3^{10}\}$

59049

↑ Caut puteri ale lui 3 (dacă există)

Algoritmi criptografici

Caesar, Afin, Hill } flux
pe blocuri < cu padding random
fără padding

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

J	K	L	M	N	O	P	Q	R
9	10	11	12	13	14	15	16	17

S	T	U	V	W	X	Y	Z
18	19	20	21	22	23	24	25

Adăugăm: ␣ . ?
26 27 28

⇒ Lucrăm în $\mathbb{Z}_{29}$

Caesar: Flux (stream cipher) = 0 cheie pt tot mesajul

- Ec. de criptare: $m + K = c$, $\forall m \in$ Mesaj, K = cheie
- Ec. de decriptare: $m = c - K$ ↗ $c \in$ Cod (cifru)

Ex: Mesaj: MIERCURI ; K=11

[M,I,E,R,C,U,R,I] → [12,8,4,17,2,20,17,8] $\xrightarrow[+11]{+K}$

→ [23,19,15,28,13,31,28,19] $\xrightarrow[\text{mod}29]{}$

→ [23,19,15,28,13,2,28,19] → XTP?NC?T

Concluzie: MIERCURI $\xrightarrow{+11}$ XTP?NC?T

(Caesar, flux)

Decriptare:

[X,T,P,?,N,C,?,T] → [23,19,15,28,13,2,28,19] $\xrightarrow[-11]{-K}$

→ [12,8,4,17,2,-9,17,8] $\xrightarrow[\text{mod}29]{}$ [12,8,4,17,2,20,17,8]

→ MIERCURI.

Pe blocuri - fără padding

↓ ↓

câte o cheie pt. fiecare bloc — cel mult un bloc mai scurt

Ex: Mesaj: MIERCURI ; bloc=5 ⇒ MIERC, K1=12
URI, K2=15

$[M,I,E,R,C] \to [12,8,4,17,2] \xrightarrow[+12]{+K1} [24,20,16,29,14]$

$\xrightarrow[mod29]{} [24,20,16,0,14] \to [Y,U,Q,A,O] \to YUQAO$

$[U,R,I] \to [20,17,8] \xrightarrow[+15]{+K2} [35,32,23] \xrightarrow[mod29]{}$

$[6,3,23] \to GDX$

Concluzie: MIERCURI $\to$ YUQAOGDX

Caesar pe blocuri cu <u>padding random</u>

toate blocurile de aceeași lungime
+ format

Ex: Mesaj: MARTI

bloc: 3 $\Rightarrow$ MAR
TI E $\to$ padding random

K1=10; K2=15

$[M,A,R] \longrightarrow [12,0,17] \xrightarrow[+10]{+K1} [22,10,27] \longrightarrow$

$\to [W,K,\cdot] \to WK.$

$[T,I,E] \to [19,8,4] \xrightarrow[+15]{+K2} [34,23,19] \xrightarrow[mod29]{} [5,23,19]$

$\to FXT$

MARTIE → WK.FXT

Cifrul afin - Flux

Ec. de criptare: $m \cdot K1 + K2 = c$, $\forall m \in Mesaj$, $K1, K2$ chei, $c \in Cod$

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

Ex: Mesaj: AZi ; K1 = 11 ; K2 = 17

$[A, Z, i] \to [0, 25, 8] \xrightarrow[\cdot 11 + 17]{} [17, 292, 105]$

$\xrightarrow{mod\ 29} [17, 2, 18] \to RCS$

AZi $\xrightarrow{afin}$ RCS

Decriptare: $[R, C, S] \to [17, 2, 18] \xrightarrow[-17 \cdot 8]{-K2 \cdot K1^{-1}} [0, -120, 8]$

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

$-120 = -116 - 4 = -4 = 25$

$116 = 0$

Hill: Flux

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

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

Mesaj, Cod $\in \mathcal{M}_{3,1}(\mathbb{Z}_{29})$

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

Ex: Mesaj: URA, $MC = \begin{pmatrix} 2 & 1 & -1 \\ 0 & 1 & 2 \\ -1 & 2 & 0 \end{pmatrix} \in \mathcal{M}_3(\mathbb{Z}_{29})$

$(U, R, A) \rightarrow \begin{pmatrix} 20 \\ 17 \\ 0 \end{pmatrix}$

Criptarea: $\begin{pmatrix} 2 & 1 & -1 \\ 0 & 1 & 2 \\ -1 & 2 & 0 \end{pmatrix} \cdot \begin{pmatrix} 20 \\ 17 \\ 0 \end{pmatrix} = \begin{pmatrix} 57 \\ 17 \\ 14 \end{pmatrix} \bmod 29$

$= \begin{pmatrix} 28 \\ 17 \\ 14 \end{pmatrix} = ?RO$

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

$\det A = -2 - 1 - 8 = -11 = 18 \in U(Z_{29})$

$(\det A)^{-1} = 18^{-1} = 21$

$A \to A^t = \begin{pmatrix} 2 & 0 & -1 \\ 1 & 1 & 2 \\ -1 & 2 & 0 \end{pmatrix} \longrightarrow A^* = \begin{pmatrix} -4 & -2 & 3 \\ -2 & -1 & -4 \\ 1 & -5 & 2 \end{pmatrix}$

$A^{-1} = (\det A)^{-1} \cdot A^* = 21 \cdot \begin{pmatrix} -4 & -2 & 3 \\ -2 & -1 & -4 \\ 1 & -5 & 2 \end{pmatrix}$

$\begin{pmatrix} ? \\ R \\ 0 \end{pmatrix} = \begin{pmatrix} 28 \\ 17 \\ 14 \end{pmatrix} \longrightarrow 21 \cdot \begin{pmatrix} -4 & -2 & 3 \\ -2 & -1 & -4 \\ 1 & -5 & 2 \end{pmatrix} \begin{pmatrix} 28 \\ 17 \\ 14 \end{pmatrix} = \begin{pmatrix} 20 \\ 17 \\ 0 \end{pmatrix}$

-8

$\begin{pmatrix} -1 \\ -12 \\ -15 \end{pmatrix}$

Examen: Criptați cu Caesar fluxurile de familie cu cheia personală (sau invers).

NF: MANEA = Mesaj
P : ADRIAN = Cheie

M	A	N	E	A
+	+	+	+	+
A	D	R	I	A

12	0	13	4	0
+	+	+	+	+
0	3	17	8	0

---

12 3 30 12 0 ⟶ (mod 29) ⟶ 12 3 1 12 0

↓

M D B M A

Temă: 1) Caesar flux, Mesaj = numele de familie
Cheia = luna nașterii
+ decriptare

2) Caesar pe blocuri, fără padding, Mesaj = prenume,
blocuri = 3, Cheie = ultimele cifre din nr. telefon
+ decriptare

3) Afin flux, Mesaj: Orașul nașterii
cheie1 = luna nașterii, cheie2 = ziua nașterii
+ decriptare

4) Hill, Mesaj = JOI ; $MC = \begin{pmatrix} 2 & 1 & -1 \\ 2 & 1 & 0 \\ -1 & -2 & -1 \end{pmatrix}$

Teste de primalitate

INPUT: $n \in \mathbb{N}$ (n impar)

OUTPUT: n prim/compus

1) Ciurul / Sita lui Eratostene
2) Teorema lui Fermat
3) Teorema Solovay-Strassen

- Varianta deterministă = sigură
  + 100% certitudine
  − ineficientă
- Varianta probabilistă
  − probabilitate
  + rapidă
  +/− sigur compus / probabil prim

Ciurul lui Eratostene - Varianta sigură

INPUT: $n \in \mathbb{N}$

OUTPUT: lista de nr prime $\leq n$

Ex: $n = 25$

~~2~~ ~~3~~ ~~4~~ ~~5~~ ~~6~~ ~~7~~ ~~8~~ ~~9~~ ~~10~~ ~~11~~ ~~12~~ ~~13~~

~~14~~ ~~15~~ ~~16~~ ~~17~~ ~~18~~ ~~19~~ ~~20~~ ~~21~~ ~~22~~ ~~23~~ ~~24~~

~~25~~ OUTPUT: 2, 3, 5, 7, 11, 13, 17, 19, 23 prime ≤ 25

Testul Fermat - Varianta deterministă

Mica Teoremă Fermat

n prim $\Rightarrow a^{n-1} \equiv 1 \bmod n, \forall a \in \{1, \dots, n-1\}$

Echivalent: n prim $\overset{?}{\Rightarrow} a^{n-1} = 1$ în $\mathbb{Z}_n, \forall a \in \mathbb{Z}_n$

Exemplu: $n = 7 \Rightarrow \forall a \in \mathbb{Z}_7, a^6 = 1$ în $\mathbb{Z}_7$

$a = 1 \Rightarrow 1^6 = 1$ ✓

$a = 2 \Rightarrow 2^6 = 64 = 63 + 1$ ✓

$a = 3 \Rightarrow 3^6 = (3^2)^3 = (9)^3 = 2^3 = 8 = 7 + 1$ ✓

$a = 4 \Rightarrow 4^6 = (2^6)^2 = 1^2 = 1$ ✓

$a = 5 \Rightarrow 5^6 = (-2)^6 = 2^6 = 1$ ✓

$a = 6 \Rightarrow 6^6 = 2^6 \cdot 3^6 = 1 \cdot 1 = 1$ ✓

$\Rightarrow 7$ este <u>sigur</u> prim (cf. Fermat)

Exemplu: $n = 9 \overset{?}{\Rightarrow} \forall a \in \mathbb{Z}_9, a^8 = 1$ în $\mathbb{Z}_9$

$a = 1 \Rightarrow 1^8 = 1$ ✓

$a = 2 \Rightarrow 2^8 = 2^3 \cdot 2^3 \cdot 2^2 = (-1) \cdot (-1) \cdot 2^2 = 4 \neq 1$

$\Rightarrow n = 9$ nu este prim, $a = 2$ martor (witness)

Format - probabilist

Testez (aleatoriu) mostre $a \in \mathbb{Z}_n$ dacă

$$a^{n-1} = 1 \text{ în } \mathbb{Z}_n.$$

Exemplu: $n = 17$, $t = 3$ mostre, $a \in \{3, 4, 5\}$

- $a = 3 \Rightarrow 3^{16} = 1$ în $\mathbb{Z}_{17}$

$$(3^4)^4 = (81)^4 = (-4)^4 = 2^8 = (2^4)^2 = 16^2 = (-1)^2 = 1 \checkmark$$

- $a = 4 \Rightarrow 4^{16} = 1$ în $\mathbb{Z}_{17}$

$$(4^4)^4 = (2^8)^4 = 1^4 = 1 \checkmark$$

- $a = 5 \Rightarrow 5^{16} = 1$ în $\mathbb{Z}_{17}$

$$(5^3)^5 \cdot 5 = 125^5 \cdot 5 = 6^5 \cdot 5 = 2^5 \cdot 3^5 \cdot 5$$

$$= 2^4 \cdot 2 \cdot 3^4 \cdot 3 \cdot 5 = 16 \cdot 81 \cdot 2 \cdot 15 = (-1) \cdot (-4) \cdot 2 \cdot (-2)$$

$$= -16 = 1 \checkmark$$

$\Rightarrow n = 17$ probabil prim, $p = \frac{3}{16}$.

Simbolul Jacobi

$$\left(\frac{b}{n}\right) = \begin{cases} 0 & \text{dacă } n \mid b \\ 1 & \text{dacă } b \text{ este pătrat în } \mathbb{Z}_n^* \\ -1 & \text{altfel} \end{cases}$$

n impar

Ex: $\left(\frac{2}{7}\right) = ?$ $\quad 7 \nmid 2$

x	1	2	3	4	5	6	$\in \mathbb{Z}_7^*$
x^2	1	4	**2**				

2 este pătrat în $\mathbb{Z}_7 \Rightarrow \left(\frac{2}{7}\right) = 1$

Ex: $\left(\frac{12}{3}\right) = 0$ pt că $3 \mid 12$

Ex: $\left(\frac{3}{5}\right) = -1$

x	1	2	3	4	$\in \mathbb{Z}_5$
x^2	1	4	4	1	

Testul Solovay-Strassen - Sigur

Teoremă n prim $\Rightarrow b^{\frac{n-1}{2}} = \left(\frac{b}{n}\right)$ în $\mathbb{Z}_n^*$,

$\forall b \in \mathbb{Z}_n^*$.

Ex: $n=7 \overset{?}{\Rightarrow} b^{\frac{7-1}{2}} = b^3 = \left(\frac{b}{7}\right)$, $\forall\, b \in \mathbb{Z}_7$?

- $b=1 \Rightarrow 1^3 = \left(\frac{1}{7}\right)$

  $1 = 1$ pt că $1 = 1^2$ în $\mathbb{Z}_7$

- $b=2 \Rightarrow 2^3 = \left(\frac{2}{7}\right)$

  $8 = 1$ pt că $2 = 3^2$ în $\mathbb{Z}_7$

- $b=3 \Rightarrow 3^3 = 27 = 6 = -1$

  $\left(\frac{3}{7}\right) = -1$

x	1	2	3	4	5	6
x^2	1	4	1	2	4	1

- $b=4 \Rightarrow 4^3 = 2^6 = 64 = 63 + 1 = 1$

  $\left(\frac{4}{7}\right) = 1$ pt că $4 = 2^2 = 5^2$

- $b=5 \Rightarrow 5^3 = 25 \cdot 5 = 4 \cdot 5 = 20 = 6 = -1$

  $\left(\frac{5}{7}\right) = -1$

- $b=6 \Rightarrow 6^3 = 2^3 \cdot 3^3 = 1 \cdot (-1) = -1$

  $\left(\frac{6}{7}\right) = -1$

$\Rightarrow n=7$ sigur prim (Solovay-Strassen)

Ex: $n=15 \Rightarrow b^{\frac{15-1}{2}} = \left(\frac{b}{15}\right)$, $\forall b \in \mathbb{Z}_{15}^*$

b^7

- $b=1 \Rightarrow 1^7 = 1 \Rightarrow \left(\frac{1}{15}\right) = 1$ pt că $1 = 1^2$
- $b=2 \Rightarrow 2^7 = 2^4 \cdot 2^3 = 16 \cdot 8 = 1 \cdot 8 = 8$

$\left(\frac{2}{15}\right) \neq 8 \Rightarrow$ 2 martor $\Rightarrow$ $n=15$ compus.

Variantă probabilistă

Alg t mostre $b \in \mathbb{Z}_n^*$, $b^{\frac{n-1}{2}} = \left(\frac{b}{n}\right) \in \mathbb{Z}_n$

$\Rightarrow$ răspuns { Sigur nu (dacă găsesc martor)
probabil da ($p = \frac{t}{n-1}$).

Alg. Diffie-Hellman, El Gamal, RSA

Diffie-Hellman

Baza matematică: Logaritmul discret = = logaritmul în $\mathbb{Z}_n$

Def $\log_a b = c \Leftrightarrow a^c = b$ (în $\mathbb{R}$, în $\mathbb{Z}_n$)

$d\log_a b = c \Leftrightarrow a^c = b$ (în $\mathbb{Z}_n$)

OBS) 1) Ec. $\log_a b = c$ nu are mereu soluții în $\mathbb{Z}_n$

2) Căutarea soluțiilor este scumpă computațional.

Ex: $\log_2 3$ în $\mathbb{Z}_5$ =? dacă există

$\log_2 3 = a \Leftrightarrow 2^a = 3$ în $\mathbb{Z}_5$

a	0	1	2	3	4
2^a	1	2	4	3	1

$\rightarrow \log_2 3 = 3$ în $\mathbb{Z}_5$

$(d\log_2 3 = 3$ în $\mathbb{Z}_5)$

Ex: $\log_2 3$ în $\mathbb{Z}_7$ =? dacă există

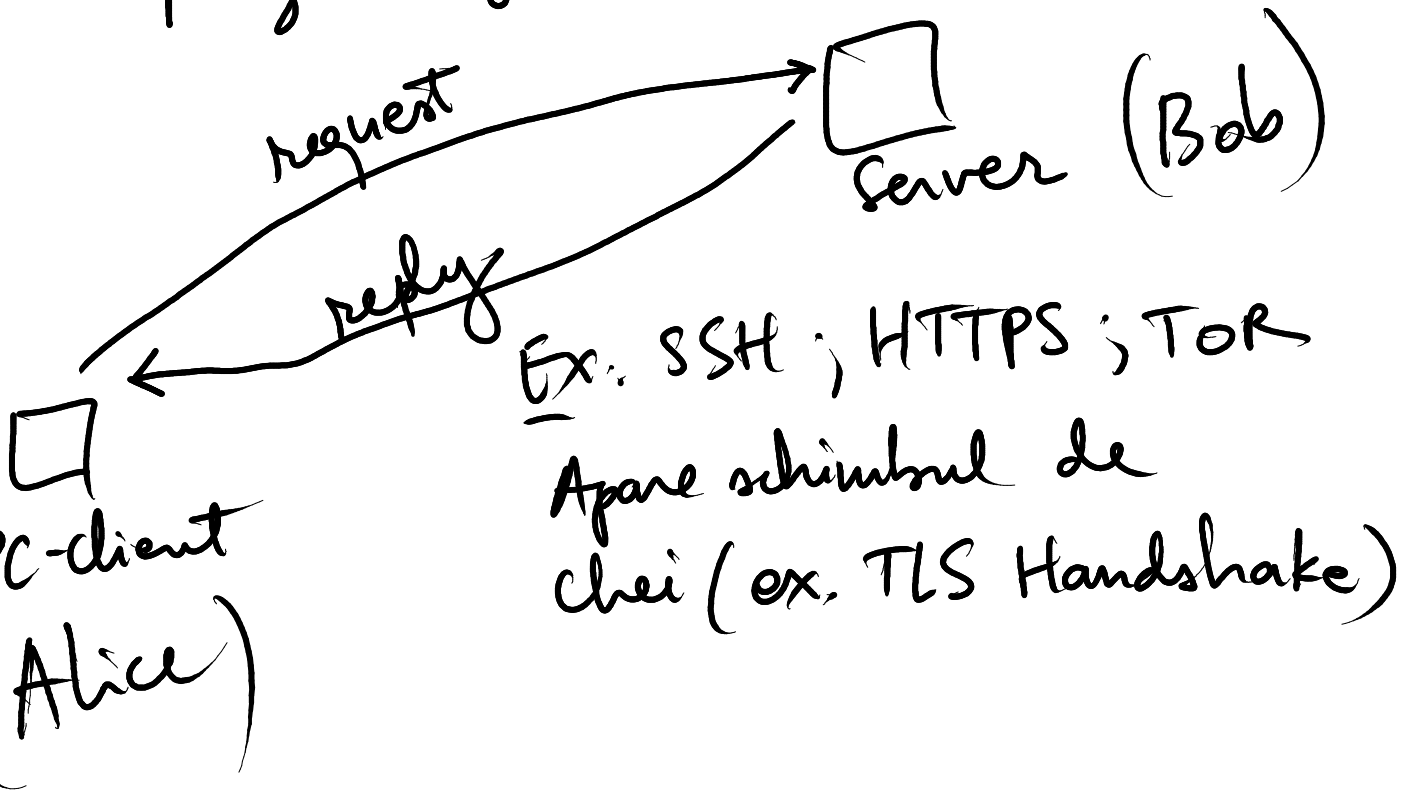
$\log_2 3 = a \Leftrightarrow 2^a = 3$ în $\mathbb{Z}_7$

a	0	1	2	3	4	5	6
2^a	1	2	4	1	2	4	1

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

Algoritmul

- Aplicația: Schimbul de chei = Stabilirea unui canal securizat de comunicare
- NU criptează mesaje!



Algoritmul: Exemplu

1. A alege $a = 6$
2. B alege $b = 7$
3. A&B aleg prim $p = 11$, $\alpha = 4$, publice
4. A calculează $A = \alpha^a \bmod p$

$$A = 4^6 \bmod 11$$

$$A = (4^2)^3 = 5^3 = 5^2 \cdot 5$$

$$A = 3 \cdot 5 = 4$$

A = 4

5. B calculează $B = \alpha^b \bmod p$

$$B = 4^7 \bmod 11$$

$$B = 4 \cdot 4 = 5$$

6. Cheie comună (Shared Key) $K = B^a = A^b \bmod p$.

$B^a = 5^b \bmod 11 = (5^2)^3 = 3^3 = 5$

Verificare: $A^b = 4^7 = 5$

Cheie comună: $K = 5$

Alg. El Gamal

Baza matematică: generatori și grupuri ciclice

Def: Dacă în Z_n^* există $a \in Z_n^*$ a.î. $\text{ord}(a) = n-1 \Rightarrow a$ s.n. **generator** și Z_n^* s.n. **grup ciclic**, generat de a.

Not: $Z_n^* = \langle a \rangle$.

OBS: Dacă există, generatorul nu este neapărat unic!

Ex: $Z_5^* = \{1, 2, 3, 4\}$

$\text{ord}1 = 1$;

x	1	2	3	4
2^x	2	4	3	1

$\Rightarrow \text{ord}2 = 4$

$\Rightarrow 2$ generator

x	1	2	3	4
3^x	3	4	2	1

$\Rightarrow ord\,3 = 4$

$\Rightarrow 3$ generator

x	1	2	3	4
4^x	4	1		

$\Rightarrow ord\,4 = 2$

$\Rightarrow 4$ nu este generator.

$\Rightarrow \mathbb{Z}_5^* = \langle 2 \rangle = \langle 3 \rangle \Rightarrow \mathbb{Z}_5^*$ grup ciclic.

Alg. El Gamal

Exemplu:

I Generarea cheii

Aleg $\mathbb{Z}_7^*$ ciclic?

x	1	2	3	4	5	6
2^x	2	4	1			

$ord_2 = 3$

x	1	2	3	4	5	6
3^x	3	2	6	4	5	1

$ord\,3 = 6$

$\Rightarrow 3$ generator

$\Rightarrow Z_7^* = \langle 3 \rangle$. $G = Z_7^*, q = 7$

$g = 3$; $e = 1$

A alege $x \in \{1,2,3,4,5,6\}$ $x = 5$

A calculează $h = g^x \bmod q$

$h = 3^5 \bmod 7 = 5$

cheie publică: $PuK = (G, q, g, h)$

$PuK = (Z_7^*, 7, 3, 5)$

Criptarea:

B alege mesajul $M \xrightarrow[\text{bijectivă}]{f} m \in Z_7^*$

Alg $M = 2$, $f = id$. $\Rightarrow f(M) = m = 2$.

B alege aleatoriu $y \in \{1,2,3,4,5,6\}$

$y = 6$.

B calculează: $s = h^y \bmod q = 5^6 \bmod 7$

$5^6 = (-2)^6 = 2^6 = 64 = \underline{1 = s}$

B calculează $c_1 = g^y \bmod q = 3^6 \bmod 7 = 1$

$c_2 = m \cdot s = 2 \cdot 1 = 2$

Cifrul $(c_1, c_2) = (1,2)$.

Criptare: $2 \longmapsto (1,2)$.

Decriptare:

A calculează $s = c_1^x \bmod q = h^y \bmod q$

$c_1^x \bmod q = 1^5 \bmod 7 = 1$

$h^y \bmod q = 5^6 \bmod 7 = 1$

s^{-1} în $\mathbb{Z}_7^*$ $\quad 1^{-1} = 1$

$m = c_2 \cdot s^{-1} = 2 \cdot 1 = 2$

Algoritmul RSA

Baza matematică: Problema factorizării

Indicatorul lui Euler

Def $\varphi(n) = \#\{x \in \mathbb{N} \mid \text{cmmdc}(x,n) = 1\}$

Ex: $\varphi(10) = ?$

$\{x \in \mathbb{N} \mid \text{cmmdc}(x,10) = 1\} = \{1,3,7,9\}$

$\Rightarrow \varphi(10) = 4.$

Teoremă: Dacă p prim $\Rightarrow \varphi(p) = p-1$

Dacă $n = p_1 \cdot p_2 \cdot p_3 \cdots p_k \Rightarrow$

$\Rightarrow \varphi(n) = (p_1-1)(p_2-1)\cdots(p_k-1).$

RSA - Exemplu

Alegerea cheilor

$p = 5$ $q = 7$ prime (mari)

Modulul de criptare: $n = p \cdot q = 35$

$\varphi(n) = \varphi(5 \cdot 7) = 4 \cdot 6 = 24$

Alg $e \in \{3, 4, \dots, 23\}$ a.î.

$\text{cmmdc}(e, \varphi(n)) = 1$

Alg $e = 5$

Alg d a.î. $d \cdot e \equiv 1 \pmod{\varphi(n)}$

$d \cdot 5 \equiv 1 \pmod{24} \Rightarrow d = 5^{-1}$ în $\mathbb{Z}_{24}$

$\Rightarrow \underline{d = 5}$

$P_u K = (e, n) = (5, 35)$

$P_2 K = (d, n) = (5, 35)$

Criptarea:

Alg $m \in \{0, 1, \dots, 34\}$, $\underline{m = 10}$

Calculez $c = m^e \bmod n$

$c = 10^5 \bmod 35$

$c = (10^2)^2 \cdot 10 = 100^2 \cdot 10$

$c = (-5)^2 \cdot 10 = 5^2 \cdot 10$

$c = 5 \cdot 50 = 5 \cdot 15 = 5$

Cifrul: $c = 5$.

$m = 10 \xrightarrow{RSA} c = 5$.

Decriptarea:

$m' = c^d \bmod n = 5^5 \bmod 35$

$= (5^2)^2 \cdot 5 = (-10)^2 \cdot 5 = 10^2 \cdot 5$

$= -5 \cdot 5 = -25 = n_0$

$m' = m$ ⇒ OK.