13416

Aritmetică în $\mathbb{Z}_n$

Ecuații de gradul I → CAESAR AFIN

Ex: $5x+1=3$ în $\mathbb{Z}_7$

$5x = 3-1=2 \mid \cdot 5^{-1}=3$

$\underbrace{5\cdot 3}_{1}\cdot x = 2\cdot 3 \Rightarrow x=6$

Ex: $6x+2=1$ în $\mathbb{Z}_{10}$

$6x=1-2=-1=9 \mid \cdot 6^{-1}$ NU există în $\mathbb{Z}_{10}$

Teoremă: x^{-1} există în $\mathbb{Z}_n \Leftrightarrow \text{cmmdc}(x,n)=1$

$6x=9$ rezolv prin încercări

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

$\Rightarrow$ ec nu are sol.

Sisteme liniare

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

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

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

$\Rightarrow$ sistem Cramer $\Rightarrow$ sol. unică.

$$\begin{cases} 2x + 3y = 1 \\ 5x - y = 2 \mid \cdot 3 \end{cases} \Rightarrow \begin{cases} 2x + 3y = 1 \\ 15x - 3y = 6 \end{cases} \xrightarrow{(+)} 17x = 7$$

$3x = 0$

$\Rightarrow x = 0$

$5 \cdot 0 - y = 2 \Rightarrow y = -2 = 5$

Ex: $\begin{cases} 2x + y = 3 \\ 4x + 2y = 1 \end{cases}$ în $\mathbb{Z}_{11}$

$A = \begin{pmatrix} 2 & 1 \\ 4 & 2 \end{pmatrix} \in M_2(\mathbb{Z}_{11}) \Rightarrow \det A = 0 \Rightarrow$ sist. nu este Cramer.

$$\begin{cases} 2x + y = 3 \mid \cdot 2 \\ 4x + 2y = 1 \end{cases} \Rightarrow \begin{cases} 4x + 2y = 6 \\ 4x + 2y = 1 \end{cases}$$

$\Rightarrow 0 = 5 \Rightarrow$ incompat.

Def: $a \mid b$ în $X \Leftrightarrow \exists c \in X$ a.î. $a \cdot c = b$

Ecuații de gradul II

Ex: $3X^2 - X + 2 = 0$ în Z_7

$a = 3, b = -1, c = 2$

$\Delta = b^2 - 4ac = 1 - 4 \cdot 2 \cdot 3 = 1 - 24 = -23 \overset{P}{=} -21 - 2$

$= -2 = 5$

$\exists \sqrt{5}$ în Z_7? $\sqrt{5} = y \Leftrightarrow y^2 = 5$

$Z_7 = \{0, 1, 2, 3, 4, 5, 6\}$ $P(Z_7) = \{0, 1, 4, 2\} \neq 5$

↑ pătratele

$\Rightarrow \nexists \sqrt{5}$ în $Z_7 \Rightarrow$ nu are soluții.

Ex: $X^2 - 5X + 7 \overset{\text{în } Z_{11}}{=} 1 \Leftrightarrow X^2 - 5X + 6 = 0$ în Z_{11}

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

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

2^{-1} în $Z_{11} = 6$

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

$x_1 = (5 + 1) \cdot 2^{-1} = 6 \cdot 6 = 36 \overset{0}{=} 33 + 3 = 3$

$x_2 = (5 - 1) \cdot 2^{-1} = 4 \cdot 6 = 24 \overset{0}{=} 22 + 2 = 2$

$x_3 = (5 + 10) \cdot 2^{-1} = 15 \cdot 6 = 90 = 88 + 2 = 2$ NU convine

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

Inverse matriceale → HILL

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

$\det A = 1 \underbrace{+4}_{0} - 1 + 2 = 1 \in U(\mathbb{Z}_5)$

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

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

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

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

Ex: $A = \begin{pmatrix} 2 & -1 & 3 \\ 5 & 2 & 1 \\ 7 & 1 & 4 \end{pmatrix}$ în $\mathcal{M}_3(\mathbb{Z}_{11})$ $A^{-1} = ?$ dacă există

$\det A = 16 - 7 + 15 - 42 - 2 + 20$

$= 5 + 4 + 4 + 4 - 4 - 2 = 11 = 0 \Rightarrow \nexists A^{-1}$

Logaritm discret → DIFFIE-HELLMAN

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

Ex: $\log_2 5$ în $\mathbb{Z}_7$

$\log_2 5 = x \Leftrightarrow 2^x = 5$ în $\mathbb{Z}_7$

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

$\neq 5$

→ $\text{ord}\, 2 = 3$

⇒ $\log_2 5$ nu există în $\mathbb{Z}_7$.

Teorema lui Lagrange pt grupuri

G grup finit, cu n elemente.

$\forall g \in G$, $\text{ord}\, g \mid n$

În particular, $g^n = e$, elem. neutru.

Multiplicativ, lucrăm cu $\mathbb{Z}_n^* = \mathbb{Z}_n - \{0\}$

$\#\mathbb{Z}_n^* = n-1 \Rightarrow \forall x \in \mathbb{Z}_n^*$, $x^{n-1} = 1$

Ex: $\log_3 2$ în $\mathbb{Z}_{11}$

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

Sol 1: Calculez puteri

x	0	1	2	3	4	5	6	7	8	9	10
3^x	1	3	9	5	4	1	3	9	5	4	1

$\neq 2$

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

$3^4 = 3^3 \cdot 3 = 5 \cdot 3 = 15 = 4$

$3^5 = 3^4 \cdot 3 = 4 \cdot 3 = 1$

$\Rightarrow \log_3 2$ nu există în $\mathbb{Z}_{11}$

Sol 2: $3^x = 2$ în $\mathbb{Z}_{11} \Leftrightarrow 3^x = 11K+2$

Enumăr elem. $11K+2$ și văd o putere a lui 3

$11K+2 = \{2, 13, 24, 35, 46, \ldots, 3^{10} \sim 50{,}000\}$

↑

Văd puterile de puteri ale lui 3

Algoritmi criptografici

Caesar, Afin, Hill } flux (stream cipher)

pe blocuri (block cipher)
- cu padding random
- fără padding

A	B	C	D	E	F	G	H	I	J
0	1	2	3	4	5	6	7	8	9

K	L	M	N	O	P	Q	R	S	T
10	11	12	13	14	15	16	17	18	19

U	V	W	X	Y	Z
20	21	22	23	24	25

Adaug ␣ . ?
26	27	28

$\Rightarrow$ lucrăm în $\mathbb{Z}_{29}$

Caesar - flux: o cheie pt tot mesajul

Ecuația de criptare: $m + K = C$, $\forall m \in$ Mesaj, K cheie

$\rightarrow C \in$ Cod (Cifru)

Ec. de decriptare: $m = C - K$

$Enc(m) = m + K$; $Dec(c) = C - K$

Ex: Mesaj: LABORATOR
cheie: K = 15

[L, A, B, O, R, A, T, O, R] ⟶ [11, 0, 1, 14, 17, 0, 19, 14, 17]

$\xrightarrow[+15]{+K}$ [26, 15, 16, 29, 32, 15, 34, 29, 32] $\xrightarrow{\text{mod } 29}$

[26, 15, 16, 0, 3, 15, 5, 0, 3] → ␣PQADPEAD

Concluzie: LABORATOR $\xrightarrow[\text{Caesar}]{+15}$ ␣PQADPEAD.

Decriptare: [␣, P, Q, A, D, P, E, A, D] → [26, 15, 16, 0, 3, 15, 5, 0, 3]

$\xrightarrow[-15]{-K}$ [11, 0, 1, -15, -12, 0, -10, -15, -12] $\xrightarrow{\text{mod } 29}$

[11, 0, 1, 14, 17, 0, 19, 14, 17] ⟶ LABORATOR

Caesar pe blocuri, fără padding

o cheie/bloc

cel mult un bloc mai scurt

Ex: Mesaj: LABORATOR
bloc: 5

⇒ LABOR, K1 = 15
ATOR, K2 = 11

[L, A, B, 0, R] → ␣PQAD

[A, T, 0, R] → [0, 19, 14, 7] $\xrightarrow[+11]{+K2}$ [11, 30, 25, 18] $\xrightarrow{\text{mod } 29}$

[11, 1, 25, 18] → LBZS

LABORATOR $\xrightarrow[\text{pe blocuri}]{\text{Caesar}}$ ␣PQADLBZS

Caesar pe blocuri, cu padding random

Ex. Mesaj: MARTI → MAR
TIE → padding random

Bloc: 3

K1=5; K2=10

[M, A, R] → [12, 0, 17] $\xrightarrow[+5]{+K1}$ [17, 5, 22] → RFW

[T, I, E] → [19, 8, 4] $\xrightarrow[+10]{+K2}$ [29, 18, 14] $\xrightarrow{\text{mod } 29}$ [0, 18, 14]

→ ASO

MARTIE → RFWASO

padding lasă așa

Cifrul afin - varianta 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: CRIPTO ; $K1 = 7$; $K2 = 13$

$[C, R, I, P, T, O] \rightarrow [2, 17, 8, 15, 19, 14] \xrightarrow[\cdot 7 + 13]{\cdot K1 + K2}$

$[27, 132, 69, 118, 146, 111] \xrightarrow{mod\ 29}$

$[27, 16, 11, 2, 1, 24] \rightarrow [., Q, L, C, B, Y]$

$132 = 116 + 16 = 16$

$4 \cdot 29 = 116$

$\rightarrow .QLCBY$

Decriptare: $[., Q, L, C, B, Y] \rightarrow [27, 16, 11, 2, 1, 24]$

$\xrightarrow[-13 \cdot 25]{-13 \cdot 7^{-1}} [350, 75, -50, -275, -300, 275] \xrightarrow{mod\ 29}$

$[2, 17, 8, 15, 19, 14] \rightarrow CRIPTO.$

Hill - Flux

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

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

Matrice de criptare $\in M_3(Z_{29})$, inversabilă

Mesaj, Cod $\in M_{3,1}(Z_{29})$

Ex: Mesaj: YES ; Mat. cr. $= \begin{pmatrix} -1 & 2 & 1 \\ 0 & 1 & 2 \\ -2 & 0 & 1 \end{pmatrix} = A$

$\det(A) = -1 - 8 + 2 = -7 = 22$

$\begin{pmatrix} Y \\ E \\ S \end{pmatrix} = \begin{pmatrix} 24 \\ 4 \\ 18 \end{pmatrix}$; $\begin{pmatrix} -1 & 2 & 1 \\ 0 & 1 & 2 \\ -2 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 24 \\ 4 \\ 18 \end{pmatrix} = \begin{pmatrix} -24+8+18 \\ 4+36 \\ -48+18 \end{pmatrix}$

$= \begin{pmatrix} 2 \\ 40 \\ -30 \end{pmatrix} \bmod 29 = \begin{pmatrix} 2 \\ 11 \\ 28 \end{pmatrix} = CL?$

Descriptare $A^{-1} = ?$

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

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

$$A^{-1} = (\det A)^{-1} \cdot A^* = 22^{-1} \cdot \begin{pmatrix} 1 & -2 & 3 \\ -4 & 1 & 2 \\ 2 & -4 & -1 \end{pmatrix} = 4 \cdot \begin{pmatrix} 1 & -2 & 3 \\ -4 & 1 & 2 \\ 2 & -4 & -1 \end{pmatrix}$$

$$= \begin{pmatrix} 4 & -8 & 12 \\ -16 & 4 & 8 \\ 8 & -16 & -4 \end{pmatrix}$$

$$\text{Mesaj} = \begin{pmatrix} 4 & -8 & 12 \\ -16 & 4 & 8 \\ 8 & -16 & -4 \end{pmatrix} \cdot \begin{pmatrix} 2 \\ 11 \\ 28 \end{pmatrix} = \begin{pmatrix} Y \\ E \\ S \end{pmatrix}$$

Ex de examen: Criptați cu Caesar-flex numele de familie, ca cheia = prenume (sau invers).

Mesaj: MANEA
Cheia: ADRIAN

M	A	N	E	A	← m
+	+	+	+	+	
A	D	R	I	A	← k

12 0 13 4 0
+ 0 3 17 8 0
12 3 30 12 0 → 12, 3, 1, 12, 0 = ...

Tema: 1) Criptați cu Caesar - flux + decriptare

Mesaj: Numele de familie

Cheia: Luna nașterii.

2) Criptați cu Caesar pe blocuri fără padding

Mesaj: Prenume; b=3; Chei: ultimele cifre ale numărului de telefon.

+ decriptare

3) Criptați cu afin - flux, Mesaj = Orașul de naștere, K1 = luna de naștere, K2 = ziua de naștere

+ decriptare

---

4) Hill: Mesaj: Joi; $MC = \begin{pmatrix} -2 & 1 & 0 \\ 2 & -1 & -1 \\ 1 & 1 & 1 \end{pmatrix}$.

+ decriptare.

Teste de primalitate

INPUT: $n \in \mathbb{N}$, impar
OUTPUT: n prim/compus

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

→ Teste deterministe (sigure)
+ sigure
- ineficiente

→ Teste probabiliste
+ eficiente
- probabiliste
+/- sigur nu, probabil da

Ciurul lui Eratostene - sigur

INPUT: $n \in \mathbb{N}$
OUTPUT: lista de nr prime $\leq n$

Ex: $n = 20$

~~1~~ 2 3 ~~4~~ 5 ~~6~~ 7 ~~8~~ ~~9~~ ~~10~~ 11
~~12~~ 13 ~~14~~ ~~15~~ ~~16~~ 17 ~~18~~ 19 ~~20~~

OUTPUT: 2, 3, 5, 7, 11, 13, 17, 19 prime ≤ 20

Ex: $n=21$

2 3 4 5 6 7 8 9 10 11 12

13 14 15 16 17 18 19 20 21

21 compus

Testul Fermat – Varianta simplă

Mica Teoremă a lui Fermat

n prim $\Rightarrow a^{n-1} \equiv 1 \pmod n, \forall a \in \{1,2,\dots,n-1\}$

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

Exemplu: $n=7 \overset{?}{\Rightarrow} a^{7-1} = 1$ în $\mathbb{Z}_7^*$

$a=1 \Rightarrow 1^6 = 1$ ok

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

$a=3 \Rightarrow 3^6 = (3^2)^3 = 2^3 = 1$ ok

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

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

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

$\Rightarrow n=7$ prim (cf. Fermat)

Varianta probabilistă

Alg. t mostre pentru $a \in \mathbb{Z}_n^*$ și verific dacă n e.

Ex: $n = 11$, $t = 3$, $a \in \{3, 5, 8\}$

$a^{10} = 1$ în $\mathbb{Z}_{11}^*$?

$3^{10} = (3^2)^5 = 9^5 = (-2)^5 = -32 = -33 + 1 = 1$ ok

$5^{10} = (5^2)^5 = 3^5 = 3^2 \cdot 3^2 \cdot 3 = (-2) \cdot (-2) \cdot 3$

$= 12 = 1$ ok

$8^{10} = (-3)^{10} = 3^{10} = 1$ ok

$\Rightarrow$ $n = 11$ probabil prim $1 - p = \frac{3}{10} = 30\%$

Ex: $n = 9$, $t = 3$ mostre, $a \in \{2, 3, 4\}$

$a = 2 \Rightarrow 2^8 = 1$ în $\mathbb{Z}_9^*$?

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

$\Rightarrow$ $n = 9$ compus (sigur!)

$a = 2$ witness (martor)

Simbolul Jacobi

$n \in \mathbb{N}^*$ impar, $b \in \mathbb{N}$

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

Ex: $\left(\frac{3}{7}\right) = ?$ $\quad 7 \neq 3$

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

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

Ex: $\left(\frac{4}{11}\right) = ?$ $\quad 11 \nmid 4$, $4 = 2^2 \Rightarrow \left(\frac{4}{11}\right) = 1$

Ex: $\left(\frac{18}{3}\right) = 0$ pt că $3 \mid 18$

Dem $\left(\frac{18}{3}\right) = \left(\frac{0}{3}\right) = 0$ pt că $3 \mid 0$.

Testul Solovay-Strassen

Teorema: n prim $\Rightarrow b^{\frac{n-1}{2}} = \left(\frac{b}{n}\right) \in \mathbb{Z}_n^*$.

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

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

$b=1 \Rightarrow 1^3 = 1$; $\left(\frac{1}{7}\right)=1$ pt că $1=1^2$ ok

$b=2 \Rightarrow 2^3 = 1$; $\left(\frac{2}{7}\right)=1$ pt că $2=3^2=4^2$ ok

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

$b=3 \Rightarrow 3^3 = 27 = 6 = -1$; $\left(\frac{3}{7}\right)=-1$ ok

$b=4 \Rightarrow 4^3 = (2^2)^3 = (2^3)^2 = 1$; $\left(\frac{4}{7}\right)=1$ pt că $4=2^2$ ok

$b=5 \Rightarrow 5^3 = 5^2 \cdot 5 = 4 \cdot 5 = 6 = -1$; $\left(\frac{5}{7}\right)=-1$ ok

$b=6 \Rightarrow 6^3 = 2^3 \cdot 3^3 = 1 \cdot (-1) = -1$; $\left(\frac{6}{7}\right)=-1$ ok

$\Rightarrow n=7$ prim.

Ex: $n=15 \Rightarrow \forall a \in \mathbb{Z}_{15}^*$, $a^{\frac{15-1}{2}} = a^7 = \left(\frac{a}{15}\right)$?

$a=1$ ok

$a=2 \Rightarrow 2^7 = 2^4 \cdot 2^3 = 1 \cdot 2^3 = 8 \neq \left(\frac{2}{15}\right)$

$\Rightarrow$ $n=15$ Compus, $a=2$ martor.

Solovay - Strassen probabilist

Alg t martor $b \in \mathbb{Z}_n^*$ si testez $b^{\frac{n-1}{2}} = \left(\frac{b}{n}\right)$.

Ex: $n=17$; $t=3$, $a \in \{5, 9, 13\}$

$a=5 \Rightarrow$ $5^{\frac{17-1}{2}} = 5^8 = \left(\frac{5}{17}\right) \in \mathbb{Z}_{17}^*$

$5^8 = 5^3 \cdot 5^3 \cdot 5^2 = 125 \cdot 125 \cdot 5^2 = 6 \cdot 6 \cdot 5^2$

$119 = 17 \cdot 7$

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

$= 2^2 \cdot 15^2$ OK

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

$= 4 \cdot 4 = 16 = 1$

$9 = 3^{16} = \left(3^4\right)^4 = 81^4 = (-4)^4 = 4^4 = 16 \cdot 16 = 1 \cdot 1 = 1$ OK

$\left(\frac{5}{17}\right) = -1$

x	1	2	3	4	5	6	7	8	9	10
x^2	1	4	9	16	8	2	15	13	13	15

x	11	12	13	14	15	16
x^2	2	8	16	9	4	1

$\left(\frac{9}{17}\right) = 1$ pt că $9 = 3^2$

$13^8 = (-4)^8 = 4^8 = (4^2)^4 = (-1)^4 = 1$

$\left(\frac{13}{17}\right) = 1$ pt că $13 = 8^2 = 9^2$ OK

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

Alg. Diffie-Hellman, El Gamal, RSA

Diffie-Hellman

Baza matematică: Problema logaritmului discret

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

pt $\mathbb{Z}_n$, $dlog_a b$

Obs: 1) Exponențierea este ușoară computațional.

2) dlog nu există mereu.

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

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

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

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

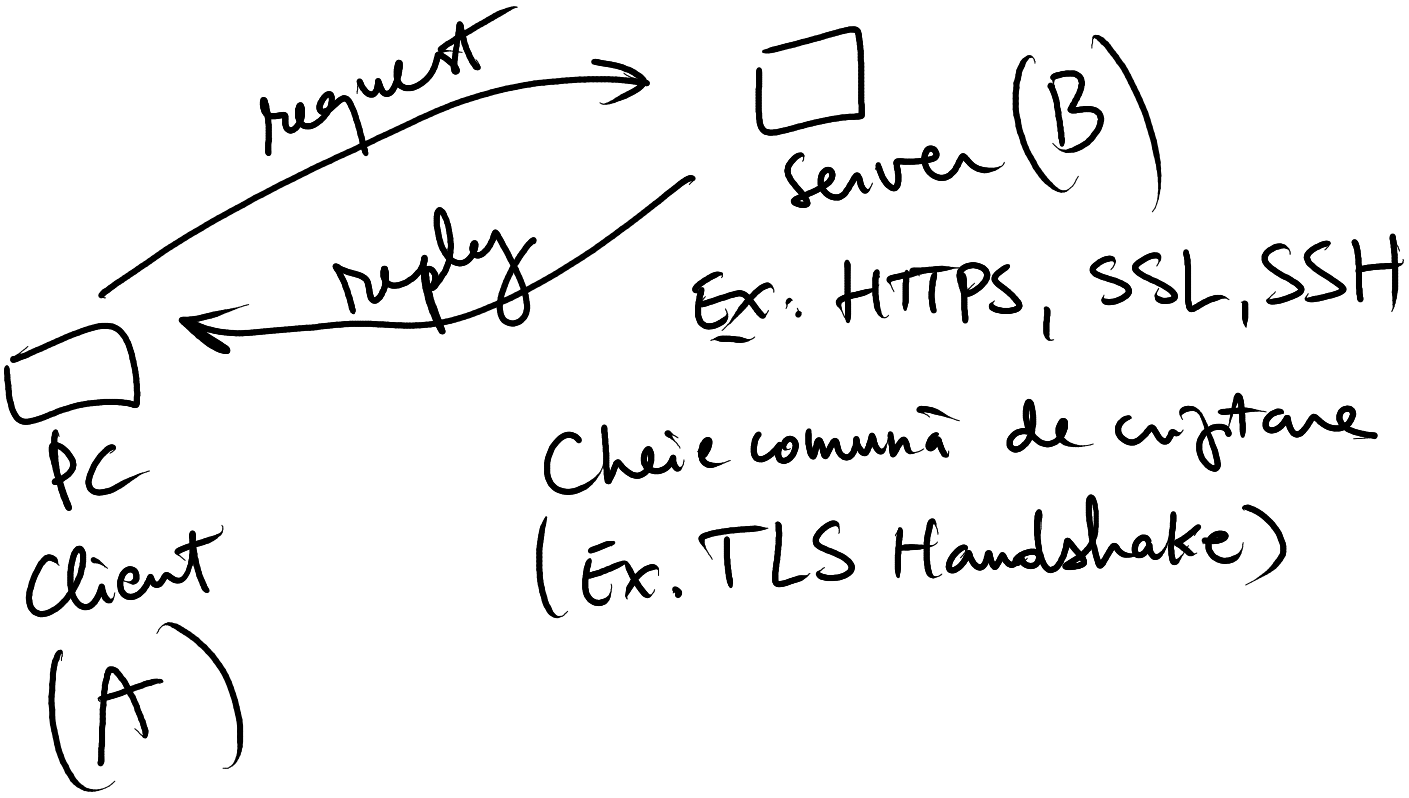
Ex: $\log_2 3 \in \mathbb{Z}_7$? dacă există

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

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

↓ ord 2 = 3

Algoritmul: Se folosește pt securizarea canalului de comunicare, nu criptează mesaje!



Ex: HTTPS, SSL, SSH

Cheie comună de criptare (Ex. TLS Handshake)

Exemplu:

1. A alege cheie privată $a = 7$
2. B — " — $b = 2$
3. p prim, $p = 13$; $\alpha = 6$
4. $A = \alpha^a \bmod p = 6^7 \bmod 13$

$6^7 = (6^2)^3 \cdot 6 = (-3)^3 \cdot 6$

$= -1 \cdot 6 = -6 = 7 = A$

5. $B = \alpha^b \bmod p = 6^2 \bmod 13 = -3 = 10$
6. Cheie comună

$K = B^a \bmod p = A^b \bmod p$

$B^a \bmod p = 10^7 \bmod 13 = (-3)^7 \bmod 13$

$= (-3^2)^3 \cdot 3 = 4^3 \cdot 3 = 4^2 \cdot 4 \cdot 3$

$= 3(-1) = -3 = 10$

$A^b \bmod p = 7^2 \bmod 13 = 10$

Cheia de criptare $\underline{K = 10}$

El Gamal

Baza matematică: Generatori și grupuri ciclice

Def: În $\hat{Z}_n^*$, dacă există $a \in Z_n^*$ a.î. $\text{ord}(a) = n-1$, spunem că a este generator și Z_n^* este grup ciclic, generat de a, not. $Z_n^* = \langle a \rangle$.

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

$1^K = 1 \Rightarrow \text{ord } 1 = 1$

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

$\Rightarrow \text{ord } 2 = 4 = 5-1$

$\Rightarrow 2$ generator

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

OBS: Dacă există, generatorul nu este neapărat unic.

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

$\Rightarrow \text{ord } 3 = 4$

$\Rightarrow$ 3 generator

$\mathbb{Z}_5^* = \langle 3 \rangle$.

a	1	2	3	4
4^a	4	1		

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

El Gamal - Exemplu

I Generarea cheii

$G = \mathbb{Z}_7^*$ ciclic?

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

$\Rightarrow \text{ord } 2 = 3 \neq 6$

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

$\Rightarrow \text{ord } 3 = 6$

$\Rightarrow \mathbb{Z}_7^*$ ciclic

3 generator

$G = \mathbb{Z}_7^*$; $q - 1 = 6 \Rightarrow q = 7$; $g = 3$

$e = 1$

Aleg aleatoriu $x \in \{1, 2, 3, 4, 5, 6\}$

$x = 5$

$h = g^x \bmod q = 3^5 \bmod 7 = 5$

$PuK = (G, q, g, h) = (\mathbb{Z}_7^*, 7, 3, 5)$

II Criptarea

$M \xrightarrow{f \text{ bijectivă}} m \in G$

Alg $f = id \Rightarrow M = m = 3$

Alg $y \in \{1,2,3,4,5,6\}$

$y = 4$

$s = h^y \bmod q = 5^4 \bmod 7 = (-2)^4$

$= 2^4 = 16 = 2$

$c_1 = g^y \bmod q = 3^4 \bmod 7 = 4$

$c_2 = m \cdot s = 3 \cdot 2 = 6$

Cifrul: $(c_1, c_2) = (4,6)$

$M \xrightarrow{id} m = 3 \xrightarrow{\text{El Gamal}} (4,6)$

Decriptarea:

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

$s = c_1^x \bmod q = 4^5 \bmod 7 = (4^2)^2 \cdot 4$

$= 2^2 \cdot 4 = 2$

$S^{-1} \in \mathbb{Z}_7^*$ $\quad 2^{-1} = 4$

$m = c_2 \cdot S^{-1} = 6 \cdot 4 = 3$ ✓

RSA

Baza matematică: Problema factorizării = descompunerea în factori primi

Indicatorul lui Euler

Def $n \in \mathbb{N}$

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

Ex: $\varphi(10) = ?$

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

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

Teorema: p prim $\Rightarrow \varphi(p) = p-1$.

In particular, dacă $n = p_1 p_2 p_3 \cdots p_k$

$\Rightarrow \varphi(n) = (p_1-1)(p_2-1)(p_3-1)\cdots(p_k-1)$.

$\varphi(10) = \varphi(2\cdot 5) = 1\cdot 4 = 4$.

RSA - Exemplu

I Generarea cheilor

$p = 5 \quad q = 7$

$n = p \cdot q = 35$

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

$e \in \{3, 4, \ldots, 23\}$ a.î. $\text{cmmdc}(e, 24) = 1$

Alg: $e = 5$

d aî. $d \cdot e = 1 \bmod \varphi(n)$

$d \cdot 5 = 1 \bmod 24 \Rightarrow d = 5^{-1}$

$\underline{d = 5}$

$PuK = (e, n) = (5, 35)$ ← publică

$PrK = (d, n) = (5, 35)$ ← privată

Criptarea:

$mesaj \in \{0, 1, \ldots, 34\}$

$m = 30$

$c = m^e \bmod n = 30^5 \bmod 35$

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

$= (-25) \cdot (-25) \cdot (-5)$

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

$= (-5) \cdot (-5) = 25$

$m = 30 \xrightarrow{\text{RSA}} c = 25$

Decryption

$$m' = c^d \bmod n \overset{?}{=} m$$

$$= 25^5 \bmod 35$$

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

$$= -100 \cdot (-100) \cdot (-10)$$

$$= \underbrace{5 \cdot 5}_{-10} \cdot (-10) = 100 = -5 = 30$$

$$\| \quad m$$

BK