13429)

Ecuații de gradul I în $\mathbb{Z}_n$

Ex: $5x+3=1$ în $\mathbb{Z}_{11}$

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

$5x = 9 \mid \cdot 5^{-1} = 9$

$9 \cdot \underbrace{5}_{1} x = 9 \cdot 9 \Rightarrow x = 81 = 77 + 4 = 4$ ($77 \equiv 0$)

$x = 4$

Ex: $6x+5=2$ în $\mathbb{Z}_{10}$

$6x = 2-5 = -3 = 7$

$6x = 7 \mid \cdot 6^{-1}$ NU există în $\mathbb{Z}_{10}$ pt că $(6,10) = 2$

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

Rezolv prin încercări

x	0	1	2	3	4	5	6	7	8	9
$6x \bmod 10$	0	6	2	8	4	0	6	2	8	4

$\Rightarrow$ Ecuația nu are soluție.

Sisteme liniare

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

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

$\det A = -9-10 = -19 = -14-5 = -5 = 2 \in U(Z_7) \Rightarrow$

$\Rightarrow$ sistem Cramer $\Rightarrow$ soluție unică

$$\begin{cases} 3x+2y=1 \\ 5x-3y=2 \end{cases} \Rightarrow 5x = 2+3y \;|\cdot 5^{-1}=3$$

$$x = 3(2+3y) = 6+9y = 6+2y$$

$3(6+2y)+2y = 1$

$18+6y+2y = 1$

$4+y = 1 \Rightarrow y = 1-4 = -3 = 4$

$x = 6+2y = 6+2\cdot 4 = 6+8 = 14 = 0$

$(x,y) \in \{(0,4)\}$

$a^{-1} = \frac{1}{a}$ $\qquad a^{-1}\cdot a = \frac{1}{a}\cdot a = 1$

Ex: $\begin{cases} 2x+3y=5 \\ x+4y=1 \end{cases}$ în Z_{10}

$A = \begin{pmatrix} 2 & 3 \\ 1 & 4 \end{pmatrix} \in M_2(Z_{10})$; $\det A = 8-3 = 5$

$5 \notin U(Z_{10}) \Rightarrow$ sist. nu este Cramer

$\Rightarrow S = \emptyset$ sau $\#S = \infty$

$$\begin{cases} 2x+3y=5 \\ x+4y=1 \mid \cdot 2 \end{cases} \Rightarrow \begin{cases} 2x+3y=5 \\ 2x+8y=2 \end{cases}$$

$(-)$

$5y = -3 = 7$

Rezolv prin încercări

x	0	1	2	3	4	5	6	7	8	9
$5x \bmod 10$	0	5	0	5	0	5	0	5	0	5

$\Rightarrow 5y = 7$ nu se poate în Z_{10}

$\Rightarrow S = \phi$.

Ec. de gradul II

Ex: $2x^2 - 3x + 1 = 0$ în Z_5

$a = 2;\ b = -3;\ c = 1$

$\Delta = b^2 - 4ac = 9 - 4 \cdot 2 = 1$

$\exists \sqrt{\Delta} \in Z_5$? $\sqrt{1} \in \{1, 4\}$

$x_1 = (-b + \sqrt{\Delta}) \cdot (2a)^{-1} = (3+1) \cdot 4^{-1} = 4 \cdot 4^{-1} = 1$

$x_2 = (-b - \sqrt{\Delta}) \cdot (2a)^{-1} = (3-1) \cdot 4^{-1} = 2 \cdot 4 = 3$

$x_3 = (3+4) \cdot 4^{-1} = 2 \cdot 4 = 3$

$x_4 = (3-4) \cdot 4^{-1} = 4 \cdot 4^{-1} = 1$

↑ NU E NEVOIE

Ex: $x^2+2x+3=1$ în $\mathbb{Z}_7$

$x^2+2x+2=0$

$a=1;\ b=2;\ c=2$

$\Delta = 4-4\cdot 2\cdot 1 = -4 = 3$

$\exists \sqrt{3}$ în $\mathbb{Z}_7$? $\quad \sqrt{3}=n \Leftrightarrow n^2=3$ în $\mathbb{Z}_7$

$\mathbb{Z}_7=\{0,1,2,3,4,5,6\}$ $\quad P(\mathbb{Z}_7)=\{0,1,4,2\}\neq 3$

(↑ pătrate)

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

Logaritmi în $\mathbb{Z}_n$

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

Ex: $\log_2 3$ în $\mathbb{Z}_7$

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

a	0	1	2	3	4	5	6	7	8	...
$2^a \bmod 7$	1	2	4	1	2	4	1	...		

↳ $\operatorname{ord} 2 = 3$

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

Teorema lui Lagrange pt grupuri

G grup, $\#G = n$.

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

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

Lucrăm <u>multiplicativ</u> pt $\log_a b$ $(\mathbb{Z}_n^*, \cdot)$

$\Rightarrow \#\mathbb{Z}_n^* = n-1$

$\Rightarrow$ Pt a calcula $\log_a b$ în $\mathbb{Z}_n$ este suficient să calculez $a^0, a^1, a^2, a^3, \dots, a^{n-1} = 1$

Ex: $\log_3 5$ în $\mathbb{Z}_{11}$

Calculez $3^0, 3^1, 3^2, \dots, 3^{10} = 1$

a	0	1	2	3	4	5	6	7	8	9	10
3^a în $\mathbb{Z}_{11}$	1	3	9	5	4	1					1

$\operatorname{ord} 3 = 5$ în $\mathbb{Z}_{11}$

$3^3 = 3^2 \cdot 3 = 9 \cdot 3 = 27 = 5$

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

$\log_3 5 = 3$ în $\mathbb{Z}_{11}$

Inverse matriceale $M_3(Z_n)$

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

Ex: $A = \begin{pmatrix} -1 & 2 & 1 \\ 0 & 1 & 2 \\ 2 & 0 & 1 \end{pmatrix} \in M_3(Z_5)$ $A^{-1} = ?$ dacă există

$\det A = -1 + 8 - 2 = 5 = 0 \Rightarrow A^{-1}$ nu există

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

$\det A = -2 - 2 + \underbrace{6+1}_{0} = -4 = 3 \in U(Z_7)$

$\Rightarrow$ există A^{-1}

$(\det A)^{-1} = 3^{-1}$ în $Z_7 = 5$ $\quad (-1)^{\text{linie+col.}}$

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

$A^{-1} = (\det A)^{-1} \cdot A^* = 5 \cdot \begin{pmatrix} 2 & 1 & -2 \\ -1 & 1 & 4 \\ -1 & -2 & 1 \end{pmatrix} = \begin{pmatrix} 10 & 5 & -10 \\ -5 & 5 & 20 \\ -5 & -10 & 5 \end{pmatrix}$

$\Rightarrow A^{-1} = \begin{pmatrix} 3 & 5 & 4 \\ 2 & 5 & 6 \\ 2 & 4 & 5 \end{pmatrix} \in M_3(Z_7)$

Obs: $A^{-1} \cdot A = A \cdot A^{-1} = I_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$

Algoritmi criptografici

I Flux (stream cipher)

II Pe blocuri (block cipher)

1) Caesar
2) Afin
3) Hill

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

I	J	K	L	M	N	O	P
8	9	10	11	12	13	14	15

Q	R	S	T	U	V	W	X
16	17	18	19	20	21	22	23

Y	Z
24	25

Lucrăm în $\mathbb{Z}_{29}$

Adaug ␣ . ?

26 27 28

Caesar - flux
↳ o cheie pt tot mesajul

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

K cheie
$C \in Cod\ (Cifru)$

$Enc(m) = m + K$

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

$Dec(c) = C - K$

Exemplu: Mesaj = MARTI

Cheia = 11

$[M, A, R, T, I] \to [12, 0, 17, 19, 8] \xrightarrow[+11]{+K}$

$[23, 11, 28, \underline{30}, 19] \xrightarrow[mod\ 29]{} [23, 11, 28, 1, 19]$

→ XL?BT

Concluzie: $MARTI \xrightarrow[+11]{Caesar} XL?BT$

Decriptare $[X, L, ?, B, T] \longrightarrow [23, 11, 28, 1, 19]$

$\xrightarrow[-11]{-K} [12, 0, 17, \underline{-10}, 8] \xrightarrow[mod\ 29]{} [12, 0, 17, 19, 8] \to$

→ MARTI ✓

Caesar pe blocuri: o cheie pt fiecare bloc

a) Fără padding: ≤ 1 bloc mai scurt

Ex: Mesaj: NOIEMBRIE, b = 6 ⇒ NOIEMB ; K1 = 15
RIE ; K2 = 21

[N, O, I, E, M, B] → [13, 14, 8, 4, 12, 1] $\xrightarrow[+15]{+K1}$

→ [28, 29, 23, 19, 27, 16] $\xrightarrow{\text{mod } 29}$ [28, 0, 23, 19, 27, 16]

→ ?AXT.Q

[R, I, E] → [17, 8, 4] $\xrightarrow[+24]{+K2}$ [38, 29, 25] $\xrightarrow{\text{mod } 29}$

[9, 0, 25] → JAZ

NOIEMBRIE → ?AXT.QJAZ

b) Cu padding random: toate blocurile au aceeași lungime

Ex: Mesaj: MARTI, b = 3 ⇒ MAR ; K1 = 5
TIE ; K2 = 7
↳ padding random

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

[T, I, E] → [19, 8, 4] $\xrightarrow[+7]{+K2}$ [26, 15, 11] → ␣PL

MARTIE → RFW␣PL

Ex. suplimentar

Examen: Criptați cu Caesar numele de familie cu cheia = primul prenume (sau invers).

Ex: NF: MANEA

P: ADRIAN

	M	A	N	E	A
	12	0	13	4	0
+	A	D	R	I	A
→	0	3	17	8	0

12 3 30 12 0 mod 29

↓

12 3 1 12 0

M D B M A

Cifrul afin

Ec. de criptare: $m \cdot K1 + K2 = C$, $\forall m \in Mesaj$
$k1, k2$ chei
$C \in Cod$

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

Flux: Mesaj: MARTI; K1 = 3; K2 = 7

$[M, A, R, T, I] \rightarrow [12, 0, 17, 19, 8] \xrightarrow[\cdot 3 + 7]{\cdot K1 + K2} [43, 7, 58, 64, 31]$

$\xrightarrow{mod\ 29} [14, 7, 0, 6, 2] \rightarrow$ O H A G C

Descriptare: (OHAGC) → [14, 7, 0, 6, 2] $\xrightarrow[-7 \cdot 3^{-1}]{[-K2; K]^{-1}}$ $-7, \cdot 10$

$[70, 0, -70, -10, -50] \xrightarrow{\text{mod } 29} [12, 0, 17, 19, 8]$

$-70 = -58 - 12 = -12 = 17$ → MARTI

$-50 = -29 - 21 = -21 = 8$

Hill - flux

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

$\in \mathcal{M}_3(\mathbb{Z}_{29})$ $\quad$ $\in \mathcal{M}_{3,1}(\mathbb{Z}_{29})$

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

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

$\det A = 2 - 2 - 1 = -1 = 28 \in U(\mathbb{Z}_{29})$

$\begin{pmatrix} Y \\ E \\ S \end{pmatrix} = \begin{pmatrix} 24 \\ 4 \\ 18 \end{pmatrix}$

$$\begin{pmatrix} -1 & 0 & 1 \\ 2 & 1 & 0 \\ 1 & -1 & -2 \end{pmatrix} \cdot \begin{pmatrix} 24 \\ 4 \\ 18 \end{pmatrix} = \begin{pmatrix} -6 \\ 52 \\ -16 \end{pmatrix} \bmod 29 = \begin{pmatrix} 23 \\ 23 \\ 13 \end{pmatrix} = \begin{matrix} X \\ X \\ N \end{matrix}$$

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

$$A^{-1} = (\det A)^{-1} \cdot A^* = 28^{-1} \cdot \begin{pmatrix} -2 & -1 & -1 \\ 4 & 1 & 2 \\ -3 & -1 & -1 \end{pmatrix}$$

$$4$$

$$28 \cdot \begin{pmatrix} -2 & -1 & -1 \\ 4 & 1 & 2 \\ -3 & -1 & -1 \end{pmatrix} = \begin{pmatrix} -56 & -28 & -28 \\ 112 & 28 & 56 \\ -84 & -28 & -28 \end{pmatrix}$$

$$\text{Mesaj} = \begin{pmatrix} -56 & -28 & -28 \\ 112 & 28 & 56 \\ -84 & -28 & -28 \end{pmatrix} \cdot \begin{pmatrix} 23 \\ 23 \\ 13 \end{pmatrix} = \begin{matrix} 24 \\ 4 \\ 18 \end{matrix} \begin{matrix} Y \\ E \\ S \end{matrix}$$

Exerciții

1. Caesar flux, mesaj = nume de familie, cheie = luna de naștere. Descriptare.
2. Caesar pe blocuri, mesaj = prenume, b = 3, cheie: ultimele cifre numărul din nr. de telefon. Descriptare.
3. Afin flux, mesaj = orașul de naștere, k1 = luna de naștere, k2 = ziua de naștere. Descriptare.

4. Hill, Mesaj = OPT, $MC = \begin{pmatrix} -1 & 2 & -1 \\ 0 & 1 & -1 \\ 2 & -2 & 1 \end{pmatrix}$. Decriptare.

Teste de primalitate

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

OUTPUT: n prim/compus

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

Teste
- sigure (deterministe)
- probabiliste

Ciurul lui Eratostene

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

OUTPUT: lista de nr prime $\leq n$

Ex: n = 20

2 3 ~~4~~ 5 ~~6~~ 7 ~~8~~ ~~9~~ ~~10~~

11 ~~12~~ 13 ~~14~~ ~~15~~ ~~16~~ 17 ~~18~~ 19

20

Alternativă: Putem decide dacă n este prim.

$n=13$ 2 3 ~~4~~ 5 ~~6~~ 7

~~8~~ ~~9~~ ~~10~~ 11 ~~12~~ 13 ← 13 prim

Testul Fermat

Mica Teoremă a lui Fermat (~ sec XVII)

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

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

Ex: $n=7 \Rightarrow \mathbb{Z}_7^* = \{1,2,3,4,5,6\}$

$\forall a \in \mathbb{Z}_7^*, a^6 = 1$?

$1^6 = 1$ OK

$2^6 = 64 = 63+1 = 1$ OK

$3^6 = (3^2)^3 = 2^3 = 1$ OK

$4^6 = (2^2)^6 = (2^6)^2 = 1$ OK

$5^6 = (-2)^6 = 2^6 = 1$ OK

$6^6 = 2^6 \cdot 3^6 = 1$ OK

$\Rightarrow n=7$ prim.

Ex: $n = 9$ $\mathbb{Z}_9^* = \{1, 2, 3, 4, 5, 6, 7, 8\}$

$a^8 = 1$ în $\mathbb{Z}_9^*$, $\forall a \in \mathbb{Z}_9^*$?

$1^8 = 1$ OK

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

$\Rightarrow n = 9$ compus, $a = 2$ witness (martor)

Total Fermat probabilist

Încerc t motive $a \in \mathbb{Z}_n^*$ și aplic MTF dacă pt ele $\Rightarrow$ concluzie cu prob $= \frac{t}{n-1}$.

Ex: $n = 17$ $t = 3$ $a \in \{12, 5, 10\}$

$a = 12 \Rightarrow 12^{16} = 1$ în $\mathbb{Z}_{17}^*$?

$$12^{16} = (2^2 \cdot 3)^{16} = 2^{32} \cdot 3^{16} = (2^4)^8 \cdot (3^4)^4$$

$$= \underbrace{(-1)^8}_{1} \cdot (-4)^4 = 4^4 = (2^2)^4 = (2^4)^2 = (-1)^2 = 1$$

OK

$a=5 \Rightarrow 5^{16} = (5^3)^5 \cdot 5 = C^5 \cdot 5$

$= 2^5 \cdot 3^5 \cdot 5 = \underbrace{2^4}_{(-1)} \cdot 2 \cdot \underbrace{3^4}_{-4} \cdot 3 \cdot 5 = 4 \cdot 2 \cdot 3 \cdot \underbrace{5}_{-2}$

$= 8 \cdot (-2)$

$= -16 = 1$ ok

$a=10 \Rightarrow 10^{16} = 2^{16} \cdot \underbrace{5^{16}}_{1} = (2^4)^4 = (-1)^4 = 1$ ok

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

Simbolul lui Jacobi

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

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

Ex: $\left(\frac{2}{5}\right) = -1$

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

$\mathbb{Z}_5^*$

Ex: $\left(\frac{4}{7}\right) = 1$ pt că $4 = 2^2 = 5^2 \in \mathbb{Z}_7$

Ex: $\left(\frac{13}{11}\right) = \left(\frac{2}{11}\right) = -1$

x	1	2	3	4	5	6	7	8	9	10	$\mathbb{Z}_{11}^*$
x^2	1	4	9	5	4	3	5	9	4	1	

Ex: $\left(\frac{21}{3}\right) = 0$ pt că $3 \mid 21$

$\parallel$

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

Testul Solovay-Strassen

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

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

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

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

$a = 2 \Rightarrow 2^3 = 8 = 1$; $\left(\frac{2}{7}\right) = 1$ pt că $2 = 3^2 = 4^2$

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

$\mathbb{Z}_7^*$

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

$a=4 \Rightarrow 4^3 = (2^2)^3 = (2^3)^2 = 1$; $\left(\frac{4}{7}\right) = 1$ pt că $4 = 2^2 = 5^2$

$a=5 \Rightarrow 5^3 = (-2)^3 = -2^3 = -1$; $\left(\frac{5}{7}\right) = -1$

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

$\Rightarrow n=7$ prim.

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

$a=1$ ok

$a=2 \Rightarrow 2^7 = 2^4 \cdot 2^3 = 1 \cdot 2^3 = 8$

$\left(\frac{a}{15}\right) \neq 8$, $\forall a$

$\Rightarrow a \neq 2$ martor

$n=15$ compus.

Diffie-Hellman, El Gamal, RSA

Diffie Hellman

Bază matematică: logaritmul discret

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

$\uparrow$ $d\log_a b$

OBS: 1) Exponențierea este ușoară computațional.

2) log discret 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	

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

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

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

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

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

Diffie-Hellman NU criptează mesaje!

Algoritmul:

A alege cheie privată $a = 6$

B alege cheie privată $b = 7$

Nr. prim $p = 11$; $\alpha \in \mathbb{N}$, $\alpha = 10$

$$A = \alpha^a \bmod p$$

$$= 10^6 \bmod 11 = (-1)^6 = 1$$

$$B = \alpha^b \bmod p = 10^7 \bmod 11$$

$$= (-1)^7 = -1 = 10$$

Cheia comună $K = B^a = A^b \bmod p$

$B^a \bmod p = 10^6 \bmod 11 = (-1)^6 \bmod 11 = 1$

$A^b \bmod p = 1^6 \bmod 11 = 1$.

El Gamal

Baza matematică: grupuri ciclice

Def: Dacă în Z_n^* există $x \in Z_n^*$ a.î.

$\text{ord}\, x = n-1$ ($x^{n-1} = 1$ și $n-1$ este minimal)

$\Rightarrow Z_n^*$ s.n. **ciclic**, iar x s.n. **generator**.

Not. $Z_n^* = \langle x \rangle$.

OBS: Dacă există, generatorul nu este neapărat unic.

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

$2^1 = 2$; $2^2 = 4$; $2^3 = 3$; $2^4 = 1 \Rightarrow \text{ord}\, 2 = 4$

$\Rightarrow 2$ este generator $\Rightarrow Z_5^*$ ciclic

$3^1 = 3$; $3^2 = 4$; $3^3 = 2$; $3^4 = 1 \Rightarrow 3$ este gen.

$4^1 = 4$; $4^2 = 1 \Rightarrow \text{ord}\, 4 = 2 \Rightarrow 4$ nu este generator

$\Rightarrow Z_5^* = \langle 2 \rangle = \langle 3 \rangle$.

El Gamal-algoritm

I Generarea cheii

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

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

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

$\Rightarrow \mathbb{Z}_7^* = \langle 3 \rangle$.

$g = 3$; $e = 1$

$x \in \{1, 2, \dots, 6\} \Rightarrow x = 6$

$h = g^x \bmod q = 3^6 \bmod 7 = 1$

$PuK = (G, q, g, h) = (\mathbb{Z}_7^*, 7, 3, 1)$

$PrK = x = 6$

II Criptarea

Mesaj $M=3 \xrightarrow[\text{bijectivă}]{f} m \in Z_7^*$

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

$y \in \{1,2,\dots,6\} \Rightarrow y=4$

$s=h^y \bmod q = 1^4 \bmod 7 = 1$

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

$c_2 = m \cdot s = 3 \cdot 1 = 3.$

Cifrul transmis: $(c_1, c_2) = (4,3)$

$M=3 \xrightarrow{id} m=3 \xrightarrow{ElG} (4,3).$

III Decriptarea

$\underbrace{c_1^x \bmod q}_{} = h^y \bmod q = s$

$4^6 \bmod 7 = 2^{12} = (2^3)^4 = 1^4 = 1 = s$

$5^{-1} \in \mathbb{Z}_7^* = 1$

Decriptarea: $m = c_2 \cdot 5^{-1} = 3 \cdot 1 = 3 \xrightarrow{f^{-1}} M$

RSA

Baza matematică: factorizarea = descompunerea în factori primi

Indicatorul lui Euler (Euler's TOTIENT function)

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

$$\varphi(n) = \#\{x \leq n \mid cmmdc(x,n) = 1\}$$

Ex: $n = 10$

$$\{x \leq 10 \mid cmmdc(x,10) = 1\} \Rightarrow \{1,3,7,9\}$$

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

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

2) $n = p_1 \cdot p_2 \cdots p_t$, p_i prime

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

3* $\varphi(n) = \#U(\mathbb{Z}_n)$

RSA: Algoritmul

1. Alegerea cheilor

$p = 5 \qquad q = 7$

$n = p \cdot q = 35$

$\varphi(n) = (p-1)(q-1) = 4 \cdot 6 = 24$

Alg $e \in \{3, 4, \dots, 23\}$; $e = 17$

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

$d \cdot e = 1 \mod \varphi(n) \Rightarrow d = e^{-1} \mod \varphi(n)$

17^{-1} în $\mathbb{Z}_{24} = 17 = d$

$PuK = (e, n) = (17, 35)$

$PrK = (d, n) = (17, 35)$

Şifreleme

$m \in \{0, 1, \ldots, 34\}$ mesaj, $m = 23$

Key

$$c = m^e \bmod n = 23^{17} \bmod 35$$

$$= (-12)^{17} = (-1) \cdot (2^2)^{17} \cdot 3^{17} \bmod 35$$

$$= -(2^5)^6 \cdot 2^4 \cdot (3^5)^3 \cdot 3^2$$

$$= -(-3)^6 \cdot 2^4 \cdot (-2)^3 \cdot 3^2$$

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

$$= -2^8 \cdot 3^3 = -2^5 \cdot 2^3 \cdot 3^3$$

$$= 3 \cdot 2^3 \cdot 3^3 = 81 \cdot 8$$

$$= 11 \cdot 8 = 88 = 18$$

$$m = 23 \xrightarrow{RSA} c = 18.$$

III Decryptage

$$m' = c^d \bmod n = 18^{17} \bmod 35$$

$$= 2^{17} \cdot 3^{34} = (2^5)^3 \cdot 2^2 \cdot (3^5)^6 \cdot 3^4$$

$$= (-3)^3 \cdot 2^2 \cdot (-2)^6 \cdot 3^4$$

$$= -3^7 \cdot 2^8 = -3^5 \cdot 2^5 \cdot 3^2 \cdot 2^3$$

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

$$= -16 \cdot 27 = -12 = 23 = m.$$