13419

Ecuații de gradul I în $\mathbb{Z}_n$

Ex 1) $5x+3=1$ în $\mathbb{Z}_7$

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

$5x = 5$ în $\mathbb{Z}_7 \mid \cdot 5^{-1} = 3$

$3 \cdot 5 \cdot x = 5 \cdot 3 \Rightarrow x = 1$

Ex 2: $4x + 5 = 3$ în $\mathbb{Z}_{10}$

$4x = 3-5 = -2 = 8 \mid \cdot 4^{-1}$ NU există

$(4,10) = 2 \neq 1$

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

$4x = 8$

Regula simplificării $\Rightarrow x = 2$

$x = 7$

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

Sisteme liniare

Ex: $\begin{cases} 3x+2y=1 \\ 5x-3y=2 \end{cases}$ în $\mathbb{Z}_{11}$

Matricea sistemului: $A = \begin{pmatrix} 3 & 2 \\ 5 & -3 \end{pmatrix} \in \mathcal{M}_2(\mathbb{Z}_{11})$

$\det A = -9-10 = -19 = -11-8 = -8 = 3 \in U(\mathbb{Z}_{11})$

$\Rightarrow$ S.S.t. Cramer $\Rightarrow$ soluție unică

$$\begin{cases} 3x+2y=1 \\ 5x-3y=2 \Rightarrow 5x = 2+3y \mid \cdot 5^{-1} = 9 \end{cases}$$

$\Rightarrow x = 9(2+3y) = 18+27y = 7+5y$

$3(7+5y)+2y = 1$

$21+15y+2y = 1$

$10+6y = 1 \Rightarrow 6y = -9 = 2 \mid \cdot 6^{-1} = 2$

$\Rightarrow \boxed{y=4}$ $\quad x = 7+5\cdot 4 = 27 = 5$

$\boxed{x=5}$

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

$A = \begin{pmatrix} 3 & 1 \\ 2 & 2 \end{pmatrix}$; $\det A = 6-2 = 4 \notin U(\mathbb{Z}_{10})$

$\Rightarrow$ sist. NU este Cramer

$$\begin{cases} 3x+y=4 \mid \cdot 2 \\ 2x+2y=3 \end{cases} \Rightarrow \begin{cases} 6x+2y=8 \\ 2x+2y=3 \end{cases} \quad (-)$$

$4x = 5 \mid \cdot 4^{-1}$ NU există

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

$4x=5$ nu are sol. în $\mathbb{Z}_{10}$.

$\Rightarrow S = \emptyset$

Ec. de gradul al II-lea

Ex: $3x^2 - 2x + 1 = 0$ în $\mathbb{Z}_7$

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

$\Delta = b^2 - 4ac = 4 - 4 \cdot 1 \cdot 3 = -8 = -7 - 1 = -1 = 6$

$\exists \sqrt{6}$ în $\mathbb{Z}_7$?

x	0	1	2	3	4	5	6	
$x^2 \bmod 7$	0	1	4	2	2	4	1	$\neq 6$

$\Rightarrow \nexists \sqrt{\Delta} \Rightarrow$ nu avem sol.

Ex: $5x^2+3x+2=4$ în $\mathbb{Z}_{11}$

$5x^2+3x-2=0$

$a=5;\ b=3;\ c=-2$

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

$\Delta = 9+40 = 49 = 44+5 = 5$

$\exists \sqrt{5}$ în $\mathbb{Z}_{11}$?

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

$\sqrt{5} \in \{4, 7\}$

$x_1 = (-b+\sqrt{\Delta})\cdot(2a)^{-1} = (-3+4)\cdot 10^{-1} = 1\cdot 10^{-1} = 10$

$x_2 = (-b-\sqrt{\Delta})\cdot(2a)^{-1} = (-3-4)\cdot 10^{-1} = -7\cdot 10^{-1} = 4\cdot 10$

$= 40 = 33+7 = 7$

$x_3 = (-3+7)\cdot 10^{-1} = 4\cdot 10 = 40 = 7$

$x_4 = (-3-7)\cdot 10^{-1} = -10\cdot 10^{-1} = 1\cdot 10^{-1} = 10$

↑ NU E NECESAR

Logaritmi în $\mathbb{Z}_n$

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

Ex: $\log_3 5$ în $\mathbb{Z}_7$ $\quad \log_3 5 = a \iff 3^a = 5$ în $\mathbb{Z}_7$

a	0	1	2	3	4	5	6	7	8	9	...
3^a mod 7	1	3	2	6	4	5	1	3	2	6	4 5 ...

$3^3 = 3^2 \cdot 3 = 2 \cdot 3$ $\quad \Rightarrow 3^5 = 5 \mod 7$

$3^4 = 3^3 \cdot 3 = 6 \cdot 3$ $\quad \Rightarrow \log_3 5 = 5$ în $\mathbb{Z}_7$.

Teorema lui Lagrange pt grupuri

G grup, $\#G = n$ $\longrightarrow$ cel mai mic t a.î. $g^t = e$

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

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

Dacă lucrăm multiplicativ $\Rightarrow (\mathbb{Z}_n^*, \cdot)$ grup

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

Ex: $\log_3 2 \in \mathbb{Z}_{11}$ $\quad 3^9 = 2 \in \mathbb{Z}_{11}$

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

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

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

Inverse matriceale $\mathcal{M}_3(\mathbb{Z}_n)$

$$A = \begin{pmatrix} 2 & -1 & 0 \\ 1 & 2 & -1 \\ -2 & 0 & 1 \end{pmatrix} \in \mathcal{M}_3(\mathbb{Z}_5)$$

$A^{-1} = ?$ dacă există

Teoremă: A este inversabilă în $\mathcal{M}_n(\mathbb{Z}_t)$ $\Leftrightarrow \det A \in U(\mathbb{Z}_t)$

$\det A = 4 - 2 + 1 = 3 \in U(\mathbb{Z}_5)$

$(\det A)^{-1} = 3^{-1} = 2$

$(-1)^{\text{linie + coloană}}$

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

$$A^{-1} = (\det A)^{-1} \cdot A^* = 2 \cdot \begin{pmatrix} 2 & 1 & 1 \\ 1 & 2 & 2 \\ 4 & 2 & 0 \end{pmatrix} = \begin{pmatrix} 4 & 2 & 2 \\ 2 & 4 & 4 \\ 8 & 4 & 0 \end{pmatrix}$$

$$\Rightarrow A^{-1} = \begin{pmatrix} 4 & 2 & 2 \\ 2 & 4 & 4 \\ 3 & 4 & 0 \end{pmatrix} \in \mathcal{M}_3(\mathbb{Z}_5)$$

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

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

$\det A = 1 + 4 = 5 \in U(\mathbb{Z}_7) \Rightarrow \exists A^{-1}$

$(\det A)^{-1} = 5^{-1} = 3$

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

$$A^{-1} = (\det A)^{-1} \cdot A^* = 3 \cdot \begin{pmatrix} 6 & 5 & 2 \\ 5 & 1 & 6 \\ 5 & 3 & 6 \end{pmatrix} = \begin{pmatrix} 18 & 15 & 6 \\ 15 & 3 & 18 \\ 15 & 9 & 18 \end{pmatrix}$$

$$\Rightarrow A^{-1} = \begin{pmatrix} 4 & 1 & 6 \\ 1 & 3 & 4 \\ 1 & 2 & 4 \end{pmatrix} \in \mathcal{M}_3(\mathbb{Z}_7).$$

Algoritmi criptografici

I Flux (stream cipher)

II Pe blocuri (block cipher)

1) Caesar
2) Afin
3) Hill

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

H	I	J	K	L	M	N
7	8	9	10	11	12	13

O	P	Q	R	S	T	U
14	15	16	17	18	19	20

V	W	X	Y	Z
21	22	23	24	25

Adaug	␣	.	?
	26	27	28

=) lucrăm în $\mathbb{Z}_{29}$

Caesar - flux: ocheie pt tot mesajul.

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

k cheie

$C \in Cod(alfa)$

$Enc(m) = m + K$

Ec. de decriptare: $m = C - K$ ✓

$Dec(C) = C - K$

Ex: Mesaj: MARTI | K = 13

$[M, A, R, T, I] \rightarrow [12, 0, 17, 19, 8] \xrightarrow[+13]{+K}$

$[25, 13, 30, 32, 21] \xrightarrow{mod\,26} [25, 13, 1, 3, 21]$

→ ZNBDV

Concluzie: MARTI $\xrightarrow[+13]{\text{Caesar}}$ ZNBDV.

Decriptare: $[Z, N, B, D, V] \rightarrow [25, 13, 1, 3, 21] \xrightarrow{-K}_{-13}$

$\rightarrow [12, 0, -12, -10, 8] \xrightarrow{mod\,26} [12, 0, 17, 19, 8] \rightarrow$

→ MARTI ✓

Caesar pe blocuri fără padding

o cheie/bloc ≤ 1 bloc mai scurt

Ex: Mesaj: LABORATOR ; 6 = 5

→ LABOR ; K1 = 7

ATOR ; K2 = 15

$[L, A, B, O, R] \rightarrow [11, 0, 1, 14, 17] \xrightarrow[+7]{+K1} [18, 7, 8, 21, 24]$

→ SHIVY

$[A,T,O,R] \rightarrow [0,19,14,17] \xrightarrow[+15]{+K2} [15,34,29,32]$

$\xrightarrow[\text{mod } 29]{} [15,5,0,3] \rightarrow$ PFAD

LABORATOR → 5HIVYPFAD

Caesar pe blocuri cu padding random

toate blocurile de aceeași lungime, dar cu zgomot

Ex: Mesaj: MARTI , b = 3 ⇒

MAR ; K1 = 11

TIE ; K2 = 12

↳ padding random

$[M,A,R] \rightarrow [12,0,17] \xrightarrow[+11]{+K1} [23,11,28] \rightarrow$ XL?

$[T,I,E] \rightarrow [19,8,4] \xrightarrow[+12]{+K2} [31,20,16] \xrightarrow[\text{mod } 29]{} [2,20,16]$

$\rightarrow [C,U,Q]$

MARTIE → XL? CUQ

↳ zgomot

Examen: Criptați folosind Caesar-flux

Mesaj = nume de familie, cheia = prim prenume (sau invers).

Mesaj: MANEA

Cheia: 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 - 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: MARTI

$K1 = 3$; $K2 = 7$

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

$\xrightarrow{mod\ 29} [14, 7, 0, 6, 2] \rightarrow OHAGC$

Decriptare: OHAGC $\to [14,7,0,6,2] \xrightarrow{-K2 \cdot K1^{-1}} -7, \cdot 3^{-1} \; -7, \cdot 10$

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

$\downarrow$

MARTI

$70 = 58 + 12$

$-70 = -58 - 12 = -12 = 17$

$-50 = -58 + 8 = 8$

Hill - flux

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

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

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

Ex: Mesaj = AȘI

$Mc = \begin{pmatrix} -1 & 2 & 1 \\ 0 & 1 & 1 \\ -2 & 1 & -1 \end{pmatrix}$ $\qquad$ $\det Mc = 1 - 4 + 2 + 1$

$= 0$

$\Rightarrow Mc$ nu este inversabilă

$\Rightarrow$ nu se poate realiza decriptarea!

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

$$\begin{pmatrix} -1 & 2 & 1 \\ 0 & 1 & 1 \\ -2 & 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 25 \\ 8 \end{pmatrix} = \begin{pmatrix} 58 \\ 33 \\ 17 \end{pmatrix} \bmod 29 = \begin{pmatrix} 0 \\ 4 \\ 17 \end{pmatrix} \begin{matrix} A \\ E \\ R \end{matrix}$$

Decriptare: $\det MC = 2$; $(\det MC)^{-1} = 2^{-1} = 15$

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

$$MC^{-1} = (\det MC)^{-1} \cdot MC^* = 15 \cdot \begin{pmatrix} -2 & 3 & 1 \\ -2 & 3 & 1 \\ 2 & -3 & -1 \end{pmatrix}$$

Exerciții

1. Criptați numele de familie cu cheia dată de luna de naștere, folosind Caesar flux - Decriptare.
2. Criptați primul prenume folosind Caesar pe blocuri, $b = 3$. Cheile = ultimele cifre numele din nr. de telefon. Decriptare.
3. Criptați orașul de naștere cu cifrul afin - flux, K1 = luna de naștere, K2 = ziua de naștere.

4. Hill: Mesaj: YES

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

Teste de primalitate

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

OUTPUT: n prim/compus

1) Ciurul/Sita lui Eratostene

2) Testul Fermat

3) Testul Solovay-Strassen

a) Teste sigure (determinate)

+ răspund cu certitudine

- ineficiente

b) Teste probabiliste

+ eficiente

- nu sunt certe

---

1. Ciurul lui Eratostene

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

OUTPUT: lista de nr prime $\leq n$

Ex. n = 23

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

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

~~20~~ ~~21~~ ~~22~~ 23

out: 2, 3, 5, 7, 11, 13, 17, 19, 23.

Alternativă: Verific dacă n este prim.

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 - variantă simplă

Mica Teoremă a lui Fermat

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

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

Ex: $n=7 \Rightarrow a^6=1$ în Z_7^*, $\forall a \in Z_7^*$?

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

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

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

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

Ex: $n=9 \Rightarrow \forall a \in Z_9^*, a^8=1$ în Z_9^* ?

$a=1 \Rightarrow 1^8=1$ ok

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

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

Fermat probabilist

Aleg t moduli din $a \in Z_n^*$ și testez doar pe acela.

Concluzia va fi cu prob $= \frac{t}{n-1}$

Ex: $n=17$, $t=3$, $a \in \{5, 9, 11\}$

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

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

$125 = 119 + 6$

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

$$= 4 \cdot 2 \cdot 3 \cdot 5 = 8 \cdot (-2) = -16 = 1$$

$5 = -2$

ok

$a=9 \Rightarrow 9^{16} = (9^2)^8 = (-4)^8 = 4^8 = (4^2)^4 = (-1)^4 = 1$

ok

$a=11 \Rightarrow 11^{16} = (11^2)^8 = 2^8 = (2^4)^2 = (-1)^2 = 1$ ok

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

Simbolul Jacobi

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

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

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

Ex: $\left(\frac{15}{3}\right) = 0$ pt că $3 \mid 15$

Ex: $\left(\frac{11}{7}\right) = \left(\frac{4}{7}\right) = 1$

Testul Solovay-Strassen

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

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

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

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

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

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

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

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

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

$\Rightarrow n=7$ prim.

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

$b=1$ ok

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

$\Rightarrow n=15$ compus, $b=2$ martor.

Diffie-Hellman, El Gamal, RSA

Diffie-Hellman

Bază matematică: logaritmul discret (în $\mathbb{Z}_n$)

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

$\underbrace{\text{dlog}_a b}$

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	1

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

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

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

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

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

Diffie-Hellman-Algoritmul

OBS: NU criptează mesaje!

Ex: Alice alege $a = 8$

Bob alege $b = 10$

p prim $= 13$; $\alpha \in \mathbb{N}$, $\alpha = 23$

(p, α) = publice

$$A = \alpha^a \bmod p = 23^8 \bmod 13$$

$$= 10^8 \bmod 13 = (-3)^8 \bmod 13$$

$$= \underbrace{(3^3)^2} \cdot 3^2 = 9$$

1

$$B = \alpha^b \bmod p = 23^{10} \bmod 13$$

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

$$= (-1)^3 \cdot 3 = -3 = 10$$

Cheia comună

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

$$K = B^a = 10^8 \bmod 13 = (-3)^8 \bmod 13$$

$$= \underbrace{(3^3)^2}_{1} \cdot 3^2 = 9$$

$$A^b = 9^{10} \bmod 13 = 3^{20} = \underbrace{(3^3)^6}_{1} \cdot 3^2$$

$$K = 9$$

$$\boxed{K = 9}$$

El Gamal

Bază matematică: grupuri ciclice

Def: $(\mathbb{Z}_n^*, \cdot)$ s.n. **ciclic** dacă $\exists x \in \mathbb{Z}_n^*$ a.î. $\operatorname{ord} x = n-1$. În acest caz, x s.n. **generator**, not. $\mathbb{Z}_n^* = \langle x \rangle$.

OBS: Dacă există, generatorul nu este neapărat unic.

Ex: $\mathbb{Z}_5^*$

a	1	2	3	4	
2^a	2	4	3	1	$\Rightarrow \operatorname{ord} 2 = 4 \Rightarrow$ 2 generator
3^a	3	4	2	1	$\Rightarrow \operatorname{ord} 3 = 4 \Rightarrow$ 3 generator
4^a	4	1	4	1	$\Rightarrow \operatorname{ord} 4 = 2$

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

El Gamal - Algoritmul

I Generarea cheii

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

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

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

$\Rightarrow$ 3 generator

$e = 1$.

Alg $x \in \{1, 2, \dots, q-1\} \to \{1, \dots, 6\}$

$x = 5$

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

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

$PrK = x = 5$.

El Criptarea

$$M = \text{mesaj} \xrightarrow[\text{bijectiva}]{f} m \in \mathbb{Z}_7^*$$

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

Alg $y \in \{1, 2, \dots, q-1\} = \{1, \dots, 6\}$

$y = 6$

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

$$= (-2)^6 \bmod 7 = (2^3)^2 = 1$$

Cifrul: $c_1 = g^y \bmod q = 3^6 \bmod 7 = 1$

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

$$M \xrightarrow{f} m \xrightarrow{EG} (c_1, c_2) = (1, 3).$$

Decriptarea

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

$$S^{-1} = 1$$

$$m = c_2 \cdot S^{-1} = 3 \cdot 1 = 3 \xrightarrow{f^{-1}} M = 3.$$

RSA

Baza matematică: factorizarea = descompunerea în factori primi

Indicatorul lui Euler (TOTIENT function)

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

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

Ex: $n = 10$

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

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

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

2) Dacă $n = p_1 p_2 p_3 \cdots p_t \Rightarrow$

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

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

RSA: Algoritmul

I Alegem cheile

$p = 5 \quad q = 7$

$n = p \cdot q = 35$

$\varphi(n) = \varphi(35) = 4 \cdot 6 = 24$

Alegem $e \in \{3, 4, \ldots, 23\}$ a.î.

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

$e = 13$

$d \cdot e = 1 \mod \varphi(n) \Rightarrow d = e^{-1} \in Z_{24}$

$d = 13^{-1} \in Z_{24} = 13$

$PuK = (e, n) = (13, 35)$

$PrK = (d, n) = (13, 35)$

Criptarea

Alegem mesajul $m \in \{0, 1, \dots, 34\}$

$m = 33$

Cifrul: $c = m^e \mod n = 33^{13} \mod 35$

$= (-2)^{13} = -(2^5)^2 \cdot 2^3 = -(-3)^2 \cdot 2^3$

$= -72 = -70 - 2 = -2 = 33.$

$m = 33 \xrightarrow{RSA} c = 33.$

III Дешифрация

$m' = c^d \bmod n = 33^{13} \bmod 35 = 33$

ФБС: $m' = m$ V