1341a

Algoritmi de criptare bazați pe $\mathbb{Z}_n$

- Context: $\mathbb{Z}_{29}$

A	B	C	D	.....	Z	!	␣	.	!
0	1	2	3		25	26	27	28	$\mathbb{Z}_{29}$

$(\mathbb{Z}_{29}, +, \cdot)$ corp comutativ

- Cifruri (coduri) flux (stream cipher)
  = o cheie / mesaj

  Cifruri bloc / pe blocuri (block cipher)
  = mesajul se împarte în blocuri,
  o cheie / bloc

  → cu padding = toate blocurile au aceeași lungime

  → fără padding: ≤ 1 bloc mai scurt

Caesar $\quad c = m + k$

Ec. de criptare: Cod = Mesaj + Cheie

Ec. de decriptare: Mesaj = Cod − cheie

$m = c - k$

Flux: Mesaj: MESAJ

cheia: 11

$[M,E,S,A,J] \to [12,4,18,0,9] \xrightarrow{+K}$

$\to [23,15,29,11,20] \xrightarrow{\%29} [23,15,0,11,20]$

$\to [X,P,A,L,U] \to$ XPALU

decriptare $[X,P,A,L,U] \to [23,15,0,11,20] \xrightarrow[-11]{-K}$

$[M,E,S,A,J]$

Pe blocuri fără padding: Mesaj: MERE

bloc: 3 => MER, E

K1 = 40; K2 = 71

$[M,E,R] \to [12,4,17] \xrightarrow[+40]{+K1} [52,44,57] \xrightarrow{\%29}$

$\to [23,15,28] \to [X,P,?]$

$[E] \to [4] \xrightarrow[+71]{+K2} [75] \xrightarrow{\%29} [17] = R$

XP?R

MERE $\to$ XP?R

Cu padding

Mesaj: MERE

Bloc: $b=3 \rightarrow$ MER

$K1=40, 71=K2$ ENS

$[M, E, R] \rightarrow$ XP?

$[E, N, S] \rightarrow [4, 13, 18] \xrightarrow{+71} [75, 84, 89]$

$\xrightarrow{:29} [17, 26, 2] \rightarrow [R, \sqcup, C]$

MERE NS $\rightarrow$ XP? R␣C

Afin: Ec. de gradul I

Criptare: $Cod = Mesaj \cdot K1 + K2$

Decriptare: $Mesaj = (Cod - K2)K1^{-1}$

Hill: Ec. matriceală

Criptare: $Cod = MC \cdot \begin{pmatrix} M \\ E \\ S \\ A \\ J \end{pmatrix}$

Decriptare: $\begin{pmatrix} M \\ E \\ S \\ A \\ J \end{pmatrix} = MC^{-1} \cdot Cod$

Ex: Mesaj: Noi → $\begin{pmatrix} N \\ O \\ I \end{pmatrix} = \begin{pmatrix} 13 \\ 14 \\ 8 \end{pmatrix}$

MC: $\begin{pmatrix} 1 & -1 & 2 \\ 0 & 3 & -1 \\ 2 & -2 & 1 \end{pmatrix}$

Criptarea: $\begin{pmatrix} 1 & -1 & 2 \\ 0 & 3 & -1 \\ 2 & -2 & 1 \end{pmatrix}\begin{pmatrix} 13 \\ 14 \\ 8 \end{pmatrix} = \begin{pmatrix} 15 \\ 34 \\ 6 \end{pmatrix} \% 29$

$= \begin{pmatrix} 15 \\ 5 \\ 6 \end{pmatrix} \rightarrow PFG$

Decriptarea $\begin{pmatrix} 1 & -1 & 2 \\ 0 & 3 & -1 \\ 2 & -2 & 1 \end{pmatrix}^{-1}\begin{pmatrix} 15 \\ 5 \\ 6 \end{pmatrix} = \begin{pmatrix} 13 \\ 14 \\ 8 \end{pmatrix} \begin{matrix} N \\ O \\ I \end{matrix}$

Hill afin:

Ec. de criptare: $Cod = MC_1 \cdot \begin{pmatrix} M \\ E \\ S \\ A \\ J \end{pmatrix} + MC_2$

Decriptarea: $\begin{pmatrix} M \\ E \\ S \\ A \\ J \end{pmatrix} = MC_1^{-1}(Cod - MC_2)$

Teste de primalitate

- INPUT: $n \in \mathbb{N}$
- OUTPUT: A/F dacă n este prim

Opțional, dacă $n \in \mathbb{N}$ NU este prim (compus), se afișează un divizor propriu (martor).

1) Teste deterministe = sigure, dar ineficiente
2) Teste probabiliste = probabile, mai eficiente

↳ se bazează pe mostre (exemple) de numere care ar putea fi divizori.

Testul direct:

- INPUT: $n \in \mathbb{N}$ impar
- Testul: $\forall x \in \{2, \dots, n-1\}$,

→ dacă $\exists x / n \Rightarrow n$ compus (x martor)

Altfel: n prim

Testul (Ciurul) lui Eratostene

Ex.

2	3	~~4~~	5	~~6~~	7	~~8~~
~~9~~	~~10~~	11	~~12~~	13	~~14~~	~~15~~
~~16~~	17	~~18~~	19	~~20~~	~~21~~	~~22~~
23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29

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

OUTPUT: lista de nr prime $\leq n$

Testul Fermat

Mica Teoremă a lui Fermat

Dacă p prim $\Rightarrow a^{p-1} = 1$ în $\mathbb{Z}_p$, $\forall a \in \mathbb{Z}_p^*$.

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

$1^6 = 1$; $2^6 = 64 = 1$; $3^6 = (3^2)^3 = 9^3 = 2^3 = 8 = 1$

$4^6 = (4^2)^3 = 2^3 = 8 = 1$;

$5^6 = (5^2)^3 = 4^3 = 2^6 = 1$

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

$\Rightarrow p=7$ este prim.

Ex: $p=9$, $\mathbb{Z}_9^* = \{1, \dots, 8\}$

$1^8 = 1$; $2^8 = (2^4)^2 = 7^2 = 49 = 4 \neq 1$

$\Rightarrow p=9$ este compus; $a=2$ martor

Simbolul Jacobi

$\left(\frac{b}{n}\right)$ $\quad b, n \in \mathbb{N}$, n impar $= \begin{cases} n \mid b \Rightarrow \left(\frac{b}{n}\right) = 0 \\ b \text{ este pătrat în } \mathbb{Z}_n \Rightarrow = 1 \\ -1 \text{ în rest} \end{cases}$

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

Pătratele din $\mathbb{Z}_{11}^* = \{1, 4, 9, 5, 3\} \not\ni 11$

$\Rightarrow \left(\frac{7}{11}\right) = -1$

Soloray - Strassen

Teoremă: n prim $\Rightarrow \forall b \in \mathbb{Z}_n^*$,

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

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

$b^3 = \left(\frac{b}{7}\right)$ în $\mathbb{Z}_7$, $\forall b \in \mathbb{Z}_7^*$

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

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

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

Pătratele din $\mathbb{Z}_7^* = \{1,4,2\}$

$4^3 = 64 = 1$; $\left(\frac{4}{7}\right) = 1$ pt că $\bar{2}^2 = 4$ OK

$5^3 = 6$; $\left(\frac{5}{7}\right) = -1 = 6$ OK

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

$\Rightarrow$ 7 este prim.