1341b

Wednesday, 5 November, 2025 9:51

Cifruri simple (Caesar, afin, Hill)

Coduri
- flux (stream cipher): același cheie pt tot mesajul
- pe blocuri (block cipher)
  - fără padding
    - ultimul bloc mai scurt
  - cu padding
    - toate blocurile au aceeași lungime (ex. salted hashes)

A	B	C	D	E	F	G	H	I	J	K	L
0	1	2	3	4	5	6	7	8	9	10	11

M	N	O	P	Q	R	S	T	U	V	W	X
12	13	14	15	16	17	18	19	20	21	22	23

Y	Z
24	25

Ar trebui să lucrez în $\mathbb{Z}_{26} = \{0, 1, \dots, 25\}$, dar de ex., nr pare nu au invers în $\mathbb{Z}_{26}$ ($\nexists 2^{-1}, 4^{-1}, 6^{-1}, 8^{-1}, \dots$)

Adaug ␣ . ! ⇒ lucrez în $\mathbb{Z}_{29}$

␣	.	!
26	27	28

29 prim ⇒ $U(\mathbb{Z}_{29}) = \mathbb{Z}_{29} - \{0\}$.

Cifrul Caesar

- Varianta flux

Ecuația de criptare: cod = mesaj + cheie (în $\mathbb{Z}_{29}$)

Ecuația de decriptare: mesaj = cod − cheie

Ex: mesaj: MESAj

cheie: 19

[M E S A j] → [12, 4, 18, 0, 97] + cheie → [31, 23, 37, 19, 28]

cheie : 19

Criptarea : [M, E, S, A, J] → [12, 4, 18, 0, 9] $\xrightarrow[+19]{+\text{cheie}}$ [31, 23, 37, 19, 28]

$\xrightarrow[\text{mod } 29]{}$ [2, 23, 8, 19, 28] → C X I T !

Decriptarea: [C, X, I, T, !] → [2, 23, 8, 19, 28] $\xrightarrow[-19]{-\text{cheie}}$

→ [-17, 4, -11, 0, 9] $\xrightarrow[\text{mod } 29]{}$ [12, 4, 18, 0, 9] → MESAJ

Pe blocuri: cu padding random

Ex: mesaj: ASTAZi

Blocuri de lungime 3 ⇒ AST : cheie1 = 15

AZi : cheie2 = 20

Blocuri de lung 4

ASTA

ZIPS

padding random

[A, S, T] → [0, 18, 19] $\xrightarrow[+15]{+\text{cheie1}}$ [15, 33, 34] $\xrightarrow{\text{mod } 29}$ [15, 4, 5] → PEF

[AZi] → [0, 25, 8] $\xrightarrow[+20]{+\text{cheie2}}$ [20, 45, 28] $\xrightarrow{\text{mod } 29}$ [20, 16, 28] → UQ!

ASTAZi → PEFUQ!

Cifrul afin

Varianta flux : Ec. de criptare : Cod = mesaj · cheie 1 + cheie 2

Ec. de decriptare : Mesaj = (Cod − cheie2) · cheie1^{-1}

Ex: mesaj: MESAJ

cheie1 = 10 ; cheie2 = 17

[M, E, S, A, J] → [12, 4, 18, 0, 9] $\xrightarrow[\cdot 10, +17]{\cdot \text{cheie1}, +\text{cheie2}}$ [137, 57, 197, 17, 107]

$\xrightarrow[\text{mod } 29]{}$ [21, 28, 23, 17, 20] → V ! X R U

137 = 116 + 21 = 21

(116 = 0)

57 = 58 − 1 = −1 = 28

192 − 137 + 60 − 137 + 58 + 2 = 21 + 0 + 2 = 23

$57 = 58 - 1 = -1 = 28$

$197 = 137 + 60 = 137 + 58 + 2 = 21 + 0 + 2 = 23$

$107 = 137 - 30 = 21 - 30 = -9 = 20$

MESAJ → V!.XRU.

Decriptare: [V, !, X, R, U] → [21, 28, 23, 17, 20] $\xrightarrow{-17,\ \cdot 10^{7}}$ (3)

[12, 33, 18, 0, 9] → [12, 4, 18, 0, 9] → MESAJ

Cifrul Hill

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

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

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

Ex. mesaj: $\begin{pmatrix} Y \\ E \\ S \end{pmatrix} = \begin{pmatrix} 24 \\ 4 \\ 18 \end{pmatrix}$ mat. $= \begin{pmatrix} -1 & 0 & -1 \\ 2 & -1 & -1 \\ 1 & 0 & -1 \end{pmatrix}$

$\det(\text{mat.}) = -1 - 1 = -2 = 27 \in U(\mathbb{Z}_{29})$

$(\det(\text{mat.}))^{-1} = 27^{-1} = 14$

Criptare: $\overset{\text{mat}}{\begin{pmatrix} -1 & 0 & -1 \\ 2 & -1 & -1 \\ 1 & 0 & -1 \end{pmatrix}} \cdot \overset{\text{msj.}}{\begin{pmatrix} 24 \\ 4 \\ 18 \end{pmatrix}} = \begin{pmatrix} -42 \\ 26 \\ 6 \end{pmatrix} \bmod 29 = \begin{pmatrix} 16 \\ 26 \\ 6 \end{pmatrix}$ Q W G

$-42 = -29 - 13 = -13 = 16$

Decriptare: $\text{mat}^t = \begin{pmatrix} -1 & 2 & 1 \\ 0 & -1 & 0 \\ -1 & -1 & -1 \end{pmatrix} \longrightarrow \text{mat}^* = \begin{pmatrix} 1 & 0 & -1 \\ 1 & 2 & -3 \\ 1 & 0 & 1 \end{pmatrix}$

$$\det = \begin{vmatrix} -1 & -1 & -1 \\ 1 & 0 & 1 \\ 1 & 2 & -3 \end{vmatrix}$$

$$mat^{-1} = (\det(mat))^{-1} \cdot mat^* = 14 \cdot \begin{pmatrix} 1 & 0 & -1 \\ 1 & 2 & -3 \\ 1 & 0 & 1 \end{pmatrix}$$

$$14 \cdot \begin{pmatrix} 1 & 0 & -1 \\ 1 & 2 & -3 \\ 1 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 16 \\ 26 \\ 6 \end{pmatrix} = \begin{pmatrix} 24 \\ 4 \\ 18 \end{pmatrix}$$

Teste de primalitate

Ciurul (sita) lui Eratostene

Primește $n \in \mathbb{N}^*$

Produce toate nr prime $\leq n$

Ex: $n = 29$

~~1~~ 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

$\{2, 3, 5, 7, 11, 13, 17, 19, 23, 29\}$ prime ≤ 29

În particular $n = 29$ prim.

Testul Fermat

Mica Teoremă a lui Fermat

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

Negația: Dacă $\exists\, a \in \mathbb{Z}_n^*$ a.î. $a^{n-1} \neq 1$ în $\mathbb{Z}_n^* \Rightarrow n$ compus.

Negație: Dacă $\exists a \in \mathbb{Z}_n$ a.î. $a^{n-1} \neq 1$ în $\mathbb{Z}_n \Rightarrow n$ compus.

Ex: $n = 11 \overset{?}{\Rightarrow} \forall a \in \mathbb{Z}_{11}^*, a^{10} = 1$

$a = 1 \Rightarrow 1^{10} = 1$ ✓

$a = 2 \Rightarrow 2^{10} = (2^4)^2 \cdot 2^2 = 5^2 \cdot 2^2 = 100 = 99 + 1 = 1$ ✓

$a = 3 \Rightarrow 3^{10} = (3^2)^5 = (-2)^5 = -32 = -33 + 1 = 1$ ✓

$a = 4 \Rightarrow 4^{10} = (2^2)^{10} = (2^{10})^2 = 1$ ✓

$a = 5 \Rightarrow 5^{10} = (5^2)^5 = 3^5 = (3^2)^2 \cdot 3 = (-2)^2 \cdot 3 = 12 = 1$ ✓

$a = 6 \Rightarrow 6^{10} = 2^{10} \cdot 3^{10} = 1$ ✓

$a = 7 \Rightarrow 7^{10} = (-4)^{10} = 4^{10} = 1$ ✓

$a = 8 \Rightarrow 8^{10} = 2^{10} \cdot 4^{10} = 1$ ✓

$a = 9 \Rightarrow 9^{10} = (3^2)^{10} = (3^{10})^2 = 1$ ✓

$a = 10 \Rightarrow 10^{10} = 2^{10} \cdot 5^{10} = 1$ ✓

$\Rightarrow n = 11$ prim (Fermat)

Ex: $n = 51 \overset{?}{\Rightarrow} \forall a \in \mathbb{Z}_{51}^*, a^{50} = 1$ în $\mathbb{Z}_{51}^*$

$a = 1$ ✓

$a = 2 \Rightarrow 2^{50} = (2^6)^8 \cdot 2^2 = 13^8 \cdot 2^2 = (13^2)^4 \cdot 2^2 = 16^4 \cdot 2^2$

$13^2 = 169$
$51 \cdot 3 = 153$
$\Rightarrow 169 = 153 + 16 = 16$

$= (2^4)^4 \cdot 2^2 = 2^{18} = (2^6)^3 = 13^3 = 13^2 \cdot 13 = 16 \cdot 13$

$= \underbrace{4 \cdot 4 \cdot 13}_{52} = 4 \neq 1 \Rightarrow$ $n = 51$ compus
$a = 2$ witness (martor)

↑

↑

Teste exacte (deterministe) = știu sigur n prim/compus

Testul Fermat probabilist

Aleg t mostre din $\mathbb{Z}_n^*$, $\{a_1, \dots, a_t\}$ și testez teorema doar cu ele. ($a_i^{n-1} \stackrel{?}{=} 1$ în $\mathbb{Z}_n^*$)

→ Dacă a_i verifică ⇒ n probabil prim, cu prob $\frac{1}{n-1}$

⇒ Dacă ∃ a_j care nu verifică ⇒ n compus și GATA.

Ex: $n = 21$

3 mostre: $\{6, 8, 13\}$

$6^{20} = 1$ în $\mathbb{Z}_{21}^*$?

$6^{20} = 2^{20} \cdot 3^{20} = (2^4)^5 \cdot (3^3)^6 \cdot 3^2 = (-5)^5 \cdot 6^6 \cdot 3^2 =$

$= -5 \cdot (5^2)^2 \cdot (6^2)^3 \cdot 3^2 = -5 \cdot 4^2 \cdot 15^3 \cdot 3^2 =$

$= \underbrace{-5 \cdot (-5)}_{4} \cdot (-6)^3 \cdot 3^2 = \underbrace{4 \cdot 9}_{36 = 15 = (-6)} \cdot (-6) \cdot (-6) = -6^3 = -6 \cdot 36$

$= -6 \cdot 15$

$= -6 \cdot (-6) = 15 \neq 1$

⇒ { n = 21 compus și GATA
  { a = 6 martor

Testul Solovay - Strassen

Testul Solovay - Strassen

Simbolul Jacobi

Def: Fie $a, n \in \mathbb{N}$, $n \neq 0$ impar

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

Ex: $\left(\frac{2}{7}\right) = 1$ pt

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

că $2 = 3^2 = 4^2$ în $\mathbb{Z}_7$

$\left(\frac{16}{7537}\right) = 1$ pt că $16 = 4^2 = (7533)^2$

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

$\left(\frac{57}{3}\right) = 0$ pt că $3 \mid 57$

$\left(\frac{71}{11}\right) = \left(\frac{5}{11}\right) = 1$ pt că $5 = 4^2$

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

Teoremă (Solovay - Strassen)

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

Ex: $n=11 \overset{?}{\Rightarrow} a^5 = \left(\frac{a}{11}\right)$, $\forall a \in \mathbb{Z}_{11}$.

$a=0$, $a=1$ ✓ $\qquad \left(\frac{0}{11}\right)=0$ pt că $11 \mid 0$.

$a=2 \Rightarrow 2^5 = 32 = 10 = -1$

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

$\left(\frac{2}{11}\right) = -1$ ✓

$a=3 \Rightarrow 3^5 = (3^2)^2 \cdot 3 = (-2)^2 \cdot 3 = 4 \cdot 3 = 12 = 1$; $\left(\frac{3}{11}\right) = 1$ ($3 = 5^2$) ✓

$a=4 \Rightarrow 4^5 = (2^2)^5 = (2^5)^2 = (-1)^2 = 1$; $\left(\frac{4}{11}\right) = 1$ ($4 = 2^2$) ✓

$a=5 \Rightarrow 5^5 = (5^2)^2 \cdot 5 = 3^2 \cdot 5 = 45 = 1$; $\left(\frac{5}{11}\right) = 1$ ($5 = 4^2$) ✓

$a=6 \Rightarrow 6^5 = 2^5 \cdot 3^5 = (-1) \cdot 1 = -1$; $\left(\frac{6}{11}\right) = -1$ ✓

$a=7 \Rightarrow 7^5 = (-4)^5 = -4^5 = -1$; $\left(\frac{7}{11}\right) = -1$ ✓

$a=8 \Rightarrow 8^5 = (-3)^5 = -3^5 = -1$; $\left(\frac{8}{11}\right) = -1$ ✓

$a=9 \Rightarrow 9^5 = (-2)^5 = -2^5 = 1$; $\left(\frac{9}{4}\right) = 1$ ($9 = 3^2$) ✓

$a=10 \Rightarrow 10^5 = (-1)^5 = -1^5 = -1$; $\left(\frac{10}{11}\right) = -1$ ✓

$\Rightarrow n=11$ prim (SS).

Ex: $n=111 \overset{?}{\Rightarrow} \forall a \in \mathbb{Z}_{111}, a^{55} = \left(\frac{a}{111}\right)$

$a=2 \Rightarrow 2^{55} = \left(2^7\right)^7 \cdot 2^6 = 128^7 \cdot 2^6 = 17^7 \cdot 2^6 = \underline{17 \cdot 2^3} \cdot 17 \cdot 2^3 \cdot 17^5$

$a=2 \Rightarrow 2^{55} = (2^7)\cdot 2^0 = 128 \cdot 2 = 17 \cdot 2 = \underline{17\cdot 2}\cdot 17\cdot 2\cdot 17$

$128 = 111 + 17$

$= 136\cdot 136\cdot 17^5 = 25\cdot 25\cdot 17^5 = 5\cdot 125\cdot 17^5$

$= 5\cdot 14\cdot 17^5 = 5\cdot 14\cdot 67^2\cdot 17 = 5\cdot 67^2\cdot 238$

$17^2 = 289 = 222 + 67$

$289 - 51 = 238$

$= 5\cdot 67^2\cdot 16 = 5\cdot 67\cdot 67\cdot 16$

$= 335\cdot 67\cdot 16 = 2\cdot 67\cdot 16$

$= 134\cdot 16 = 23\cdot 16$

$= 23\cdot 8\cdot 2 = 184\cdot 2 = 73\cdot 2 = 146$

$= 35$

$2^{55} = 35 \neq 2_{111}$, $\left(\frac{a}{111}\right) \neq 35$, $\forall a \in Z_{111}$

$\Rightarrow \left(\frac{2}{111}\right) \neq 2^{55} \Rightarrow 111$ compus, $a=2$ martor.

Obs: Testul SS are și o variantă probabilistă.