

Cifruri simple / Caesar, afin, Hill)

Coduri - flux (stream cipher) : aceeași cheie pt tot mesajul

pe blocuri (block cipher)

fără "padding"
ultimul bloc mai scurt

cu padding
toate blocurile
au același lungime
(ex. salted hashes)

A	B	C	D	E	F	G	H	I	J	K	L
O	I	2	3	4	5	6	7	8	9	10	11
M	N	0	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 are invers în \mathbb{Z}_{26} ($\nexists 2^{-1}, 4^{-1}, 6^{-1}, 8^{-1}, \dots$)

Adaug $\sqcup . !$ \Rightarrow lucrez în \mathbb{Z}_{29}

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

Cifrul Caesar

- varianta flux

Ecuatia de criptare: cod = mesaj + cheie

in \mathbb{Z}_{29}

Ecuatia de decriptare: mesaj = cod - cheie

Ex: mesaj: MESAj

cheie: 19

$$\Gamma_m = c \sqcup i \rightarrow \Gamma_{12, 4, 18, 0, 9} \xrightarrow{\text{cheie}} \Gamma_{21, 23, 37, 19, 28}$$

cheie : 19

$$\text{Criptarea: } [M, E, S, A, J] \rightarrow [12, 4, 18, 0, 9] \xrightarrow[\mod 29]{+ \text{cheie}} [31, 23, 37, 19, 28]$$

$$\xrightarrow{\mod 29} [2, 23, 8, 19, 28] \rightarrow CXIT!$$

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

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

Pe blocuri: cu padding random

Ex: mesaj: ASTAZI

Blocuri de lungime 3 \Rightarrow

AST: cheie1 = 15

AZI: cheie2 = 20

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

$$[A_2, i] \rightarrow [0, 25, 8] \xrightarrow[\mod 29]{+20} [20, 45, 28] \xrightarrow{\mod 29} [20, 16, 28] \rightarrow \text{UQ!}$$

ASTAZI \rightarrow PEFUQ!

Blocuri de lung 4
ASTA
IPS
padding
random

Cifrul afin

Varianta flux: Ec. de criptare: Cod = mesaj · cheie1 + cheie2

Ec. de decriptare: Mesaj = $(\text{Cod} - \text{cheie2}) \cdot \text{cheie}_1^{-1}$

Ex: mesaj: MESAJ

cheie1 = 10; cheie2 = 17

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

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

$$137 = 116 + 21 = 21$$

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

$$107 - 137 + 60 - 137 + 58 + 2 = 21 + 0 + 2 = 23$$

$$57 = 58 - 1 = -1 = 29$$

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

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

MESAJ $\rightarrow V, !, X, R, U.$

Decriptare: $[V, !, X, R, U] \rightarrow [21, 28, 23, 17, 20] \xrightarrow{-17, -10, 3} [12, 33, 18, 0, 9] \rightarrow [12, 4, 18, 0, 9] \rightarrow \text{MESAJ}$

Cifrul Hill

Matrice de criptare $\in M_3(\mathbb{Z}_{29})$

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

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

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

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

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

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

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

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

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

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

Teste de primalitate

Ciunul (sita) lui Eratostene

Primeste $n \in \mathbb{N}^*$

Producă toate nr prime $\leq n$

Ex: $n = 29$

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

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

Negation: Dacă $\exists a \in \mathbb{Z}_n$ astfel că $a^{10} \neq 1$ în $\mathbb{Z}_n \Rightarrow n$ compus.

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

$$a=1 \Rightarrow 1^{10} = 1 \checkmark$$

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

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

$$a=4 \Rightarrow 4^{10} = (2^2)^{10} = (2^5)^2 = 1 \checkmark$$

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

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

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

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

$$a=9 \Rightarrow 9^{10} = (3^2)^{10} = (3^5)^2 = 1 \checkmark$$

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

$\Rightarrow n=11$ prim (Fermat)

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

$$a=1 \checkmark$$

$$a=2 \Rightarrow 2^{50} = (2^6)^8 \cdot 2^2 = 13^8 \cdot 2^2 = (13^2)^4 \cdot 2^2 = 16^4 \cdot 2^2 \\ 13^2 = 169 \\ 51 \cdot 3 = 153 \quad] = 169 = 153 + 16 = 16$$

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

$$= 4 \cdot \underbrace{4 \cdot 13}_{52} = 4 \neq 1 \Rightarrow \begin{cases} n=51 \text{ compus} \\ a=2 \text{ witness (murder)} \end{cases}$$

↑



Teste exakte (deterministe) = stiu sigur n prim/compos

Testul Fermat probabilist

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

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

→ Dacă $\exists a_j$ care nu verifică \Rightarrow n compus SigUR.

Ex: $n=21$

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

$6^{20} = 1$ în \mathbb{Z}_{21}^* ?

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

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

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

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

$\Rightarrow \begin{cases} n=21 \text{ compus SigUR} \\ a=6 \text{ martor} \end{cases}$

Testul Solovay-Strassen

Teoreul Solovay - Strassen

Simbolul Jacobi

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

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

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

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

$$\bar{a}^2 = 3^2 = 4^2 \text{ în } \mathbb{Z}_7$$

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

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

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

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

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

Teoremul (Solovay - Strassen)

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

1 1

$$\underline{\text{Ex: }} n=11 \stackrel{?}{\Rightarrow} a^5 = \left(\frac{a}{11} \right) \text{ für } a \in \mathbb{Z}_{11}.$$

$$\begin{array}{l} a \neq 0 \checkmark \\ a = 1 \end{array} \quad \left(\frac{0}{11} \right) = 0 \text{ ist kein } 11 \mid 0.$$

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

-	0	1	2	3	4	5	-5	-4	-3	-2	-1
x		0	1	4	9	5	3	3	5	9	4
x2		0	1	4	9	5	3	3	5	9	4

$$\left(\frac{2}{11} \right) = -1 \checkmark$$

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

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

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

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

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

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

$$a=9 \Rightarrow 9^5 = (-2)^5 = -2^5 = -1 \ ; \ \left(\frac{9}{11} \right) = 1 \quad (9=3^2) \checkmark$$

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

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

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

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

$$a=2 \Rightarrow 2^{17} = (2^1) \cdot 2^{16} = 128 \cdot 2 = 17 \cdot 2 = \underline{17 \cdot 2 \cdot 17 \cdot 2 \cdot 17}$$

$$128 = 111 + 17$$

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

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

$$17^2 = 289 = 222 + 67 = 5 \cdot 67^2 \cdot 16 = 5 \cdot 67 \cdot 67 \cdot 16$$

$$289 - 51 = 238 = 335 \cdot 67 \cdot 16 = 2 \cdot 67 \cdot 16$$

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

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

$$= 35$$

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

$$\Rightarrow \left(\frac{2}{111} \right) \neq 2^{55} \Rightarrow 111 \text{ comunitate}, a=2 \text{ membru}.$$

OBS: Testul SS are și o variantă probabilistică.

Ordinele unui element într-un grup

Def: Fix $(G, *)$ grup și $g \in G$.

$\text{ord } g = n$ dacă $\underbrace{g * g * \dots * g}_n = e$ și n este cel mai mic număr propriu-natural

OBS: Dacă nu există $(g^n \neq e, \forall n)$, te putem $\text{ord } g = \infty$.

Ex: \mathbb{Z}_7 $\text{ord } 2 = ?$

$$2^1 = 2; 2^2 = 4; 2^3 = 8 = 1 \Rightarrow \text{ord } 2 = 3$$

$$2^1 = 2; 2^2 = 4; 2^3 = 8 \equiv 1 \Rightarrow \text{ord}_2 = 3.$$

$$\text{ord}_5 = ?$$

\times	1	2	3	4	5	6
$5 \times$	5	4	6	2	3	1

$$5^3 = 5^2 \cdot 5 = 4 \cdot 5 = 20 = 6$$

Teorema (Fermat)

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

Teorema (Lagrange)

Fie G grup finit, $\text{ord}G = \#G = n$ de elemente ale mulțimii G .

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

Ex: \mathbb{Z}_{11}^* , $\text{ord } 2 = ?$ $\text{ord } 4 = ?$

\times	1	2	3	4	5	6	7	8	9	10
$2 \times$	2	4	8	5	10	9	7	3	6	1 (Fermat)
$4 \times$	4	5	9	3	(1)	4	5	9	3	1

$\Rightarrow \text{ord } 2 = 10 \quad \text{in } \mathbb{Z}_{11}^* \quad (\text{ord } \mathbb{Z}_{11}^* = \# \mathbb{Z}_{11}^* = 10)$
 $\text{ord } 4 = 5$

Logaritmul discret

Def: $\log_a b = c \Leftrightarrow a^c = b \quad (a \in \mathbb{R}, a \neq 1, b \in \mathbb{Z}_n)$

Obs 1) Calculul log discret este scump computațional.

Obs 1) Calculul log discret este scump comparativ.

2) log discret poate să nu existe.

Ex: $\log_3 2 \text{ în } \mathbb{Z}_7 = ?$

$$\begin{aligned} \log_3 2 = x \Leftrightarrow 3^x &= 2 \text{ în } \mathbb{Z}_7 \\ 3^2 &= g_2 \quad \Rightarrow x = 2 \\ \log_3 2 &= 2 \text{ în } \mathbb{Z}_7. \end{aligned}$$

$$\begin{aligned} \text{Ex: } \log_5 3 \text{ în } \mathbb{Z}_{11} &= x \Leftrightarrow 5^x = 3 \text{ în } \mathbb{Z}_{11} \\ 5^2 &= 25 = 22 + 3 = 3 \Rightarrow \\ \Rightarrow 5^2 &= 3 \Rightarrow \log_5 3 = 2 \text{ în } \mathbb{Z}_{11}. \end{aligned}$$

Ex: $\log_7 2 \text{ în } \mathbb{Z}_{13} = ?$

$$7^x = 2 \text{ în } \mathbb{Z}_{13}$$

x	1	2	3	4	5	6	7	8	9	10	11	12
7^x	7	10	5	9	11	12	6	3	8	4	2	1

$$\Rightarrow \log_7 2 = 11 \text{ în } \mathbb{Z}_{13}.$$

Grupuri ciclice și generatori

Def: Fie G grup și $g \in G$. Pp că tot g^n

$$\langle g \rangle = \{g, g^2, g^3, g^4, \dots, g^n = e\} \quad \text{s.n. subgrupul generat de } g -$$

'j' | j'j' 0'0' 0 1 generator de g-

Dacă $\langle g \rangle = G$, atunci G este grup ciclic, iar g este generator.

Ex: \mathbb{Z}_{13} $\langle 4 \rangle = ?$

x	1	2	3	4	5	6	7	8	9	10	11	12
$4x$	4	3	12	9	10	1						1

$$\Rightarrow \langle 4 \rangle = \{1, 3, 4, 9, 10, 12\} \Rightarrow 4 \text{ este generator pt } \mathbb{Z}_{13}$$

\mathbb{Z}_{13} $\langle 5 \rangle = ?$

x	1	2	3	4	5	6	7	8	9	10	11	12
$5x$	5	12	8	1								1

$$\Rightarrow \langle 5 \rangle = \{1, 5, 8, 12\} \Rightarrow 5 \text{ este generator}$$

\mathbb{Z}_{11} $\langle 5 \rangle = ?$

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

$$\Rightarrow \langle 5 \rangle = \{1, 3, 4, 5, 9\} \Rightarrow 5 \text{ este generator}$$

$\langle 2 \rangle = ?$

x	1	2	3	4	5	6	7	8	9	10
$2x$	2	4	8	5	10	9	7	3	6	1 (\text{Fermat})

$\frac{x}{2^x}$	1	2	4	8	5	10	9	7	3	6	1 (Fermat)
$\Rightarrow \langle 2 \rangle = \mathbb{Z}_{11}^* = \mathbb{Z}_{11}$, este ciclic, 2 generator.											un

Indicatorul lui Euler

Def: Fie $n \in \mathbb{N}$, $\varphi(n) = \#\{x \leq n \mid \text{cumpr. } \text{c.c.}(x, n) = 1\}$

Prop: 1) Dacă n este prim $\Rightarrow \varphi(n) = n - 1$

2) $\varphi(a \cdot b) = \varphi(a)\varphi(b)$, $a, b \in \mathbb{N}$.

Ex: $\varphi(153) = ?$

$$153 = 3^2 \cdot 17 \Rightarrow \varphi(153) = \varphi(3^2) \cdot \varphi(17) = (\varphi(3))(\varphi(3))\varphi(17) = 2 \cdot 2 \cdot 16 = 64.$$

$$\begin{array}{c|c} 153 & 3 \\ 51 & 3 \\ 17 & 17 \end{array}$$

$$\text{a prim } \varphi(a^k) = \underbrace{\varphi(a)\varphi(a) \cdots \varphi(a)}_k = \varphi(a)^k = (a-1)^k$$

$$\varphi(183) = \varphi(3 \cdot 61) = \varphi(3)\varphi(61) = 2 \cdot 60 = 120.$$

$$\begin{array}{c|c} 183 & 3 \\ 61 & 61 \end{array}$$