1342a

Wednesday, 5 November, 2025 8:01

# Coduri simple (Caesar, afin, Hill)

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

· pe **blocuri** (block cipher): chei diferite pt blocuri de mesaj

- 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 | M | N |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 |
| O | P | Q | R | S | T | U | V | W | X | Y | Z | | |
| 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | | |

Ar trebui să lucrăm în $Z_{26} = \{0, 1, \dots, 25\}$, dar

nr pare nu au invers multiplicativ ($\not\exists 2^{-1}, 4^{-1}, 6^{-1}, \dots$)

$\Rightarrow$ creează probleme la decriptare

Adaug ␣ . ! (26 27 28) $\Rightarrow$ lucrez în $Z_{29}$, 29 prim $\Rightarrow$

$\Rightarrow U(Z_{29}) = Z_{29} - \{0\}$.

## Cifrul Caesar

- Varianta flux: Ecuația de criptare: cod = mesaj + cheie (în $Z_{29}$)

  Ecuația de decriptare: mesaj = cod − cheie

Ex: mesaj = ASTAZi

cheie = 21

$[A, S, T, A, Zi] \to [0, 18, 19, 0, 25, 8] \xrightarrow{+\text{cheie}, +21}$

$[21, 39, 40, 21, 46, 29] \xrightarrow{\bmod 29} [21, 10, 11, 21, 17, 0]$

$\to$ VKLVRA

ASTAZi $\to$ VKLVRA

→ V K L V R A

ASTAZi → VKLVRA

Decriptare:

$[V,K,L,V,R,A] \to [21,10,11,21,17,0] \xrightarrow[-21]{-\text{cheie}} [0,-11,-10,0,-4,-21]$

$\xrightarrow[\text{mod } 29]{} [0,18,19,0,25,8] \to$ ASTAZi

Varianta pe blocuri

Blocuri de lungime 3 : ASTAZi → AST → cheie1 = 15
A2i → cheie2 = 23

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

$[A,2,i] \to [0,25,8) \xrightarrow[+\text{cheie2}]{+23} [23,48,31] \xrightarrow[\text{mod } 29]{} [23,19,2] \to$ XTC

ASTAZi → PEFXTC

Cu padding random: Lungimea blocurilor = 5

ASTAZi → ASTAZ ; cheie1 = 10
ix!BU ; cheie2 = 15
(padding random)

Cifrul afin

Ecuația de criptare: Cod = mesaj · cheie1 + cheie 2

Ecuația de decriptare: Mesaj = (cod − cheie2) · cheie1$^{-1}$

Ex: Mesaj: CRIPTO, cheie 1 = 6, cheie2 = 11

$[C,R,I,P,T,O) \to [2,17,8,15,19,14] \xrightarrow[\cdot 6,+11]{\cdot \text{cheie1},+\text{cheie2}}$

$[23,-61,59,101,-49,-79] \xrightarrow[\text{mod } 29]{} [23,26,1,14,9,8]$

$17 \cdot 6 + 11 = (-12) \cdot 6 + 11 = -72 + 11 = -61 = -58 - 3 = -3 = 26$

$101 = 58 + 43 = 43 = 14$

$-49 = -58 + 9 = 9$ ; $-79 = -58 - 21 = -21 = 8$

X␣BOJI

Decriptare:

Decriptare:

$X \sqcup Boji \to [23,26,1,|4,9,8] \xrightarrow[-11,\ \cdot 6^{-1}=5]{-cheie2,\ \cdot cheie1^{-1}} [60,75,-50,15,-10,-15]$

$\xrightarrow[mod\ 29]{} [2,17,8,15,19,14] \to CRIPTO$

$-50 = -58+8 = 8$

---

## Cifrul Hill

- Foloseşte matrice de criptare

La noi, matricea ra ți $\in \mathcal{M}_3(\mathbb{Z}_{29})$

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: $\begin{pmatrix} M \\ S \\ J \end{pmatrix} = \begin{pmatrix} J \\ o \\ i \end{pmatrix} = \begin{pmatrix} 9 \\ 14 \\ 8 \end{pmatrix}$ ; $Mat = \begin{pmatrix} 1 & -1 & 0 \\ 1 & 0 & -1 \\ -2 & 1 & 0 \end{pmatrix} \in \mathcal{M}_3(\mathbb{Z}_{29})$

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

Criptarea: $\begin{pmatrix} 1 & -1 & 0 \\ 1 & 0 & -1 \\ -2 & 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 9 \\ 14 \\ 8 \end{pmatrix} = \begin{pmatrix} -5 \\ 1 \\ -4 \end{pmatrix} \bmod 29 = \begin{pmatrix} 24 \\ 1 \\ 25 \end{pmatrix} \begin{matrix} Y \\ B \\ Z \end{matrix}$

J → Y
o → B
i → Z

Decriptarea: $Mat^{-1} = ?$

$Mat^t = \begin{pmatrix} 1 & 1 & -2 \\ -1 & 0 & 1 \\ 0 & -1 & 0 \end{pmatrix}$ ; $Mat^* = \begin{pmatrix} 1 & 0 & 1 \\ 2 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix}$

$Mat^{-1} = (\det Mat)^{-1} \cdot Mat^* = 28^{-1} \cdot \begin{pmatrix} 1 & 0 & 1 \\ 2 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix} = 28 \cdot \begin{pmatrix} 1 & 0 & 1 \\ 2 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix}$

$$Mat^{-1} = (\det Mat)^{-1} \cdot Mat^* = 28 \cdot \begin{pmatrix} 11 & 0 & 1 \\ 2 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix} = 28 \cdot \begin{pmatrix} 2 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix}$$

Decriptarea:

$$\underbrace{28 \cdot \begin{pmatrix} 1 & 0 & 1 \\ 2 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix}}_{Mat^{-1}} \cdot \underbrace{\begin{pmatrix} 24 \\ 1 \\ 25 \end{pmatrix}}_{cod} = \underbrace{\begin{pmatrix} 9 \\ 14 \\ 8 \end{pmatrix}}_{mesaj}$$

---

## Teste de primalitate

### Ciurul (Sita) lui Eratostene

Primește $n \in \mathbb{N}^*$

Produce 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

$\Rightarrow$ nr. prime $\leq 29$ : 2, 3, 5, 7, 11, 13, 17, 19, 23, 29

În particular $\Rightarrow n = 29$ este prim.

---

## Testul Fermat

### Teoremă (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 $\mathbb{Z}_n^* \Rightarrow n$ nu e prim (compus)

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

$a=1 \Rightarrow 1^{10}=1$ ok. ✓

$a=2 \Rightarrow 2^{10}=(2^4)^2\cdot 2^2 = 16^2\cdot 2^2 = 5^2\cdot 2^2 = 100 = 1$ ✓

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

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

$a=5 \Rightarrow 5^{10}=(5^2)^5 = 3^5 = (3^2)^2\cdot 3 = (-2)^2\cdot 3 = 4\cdot 3 = 12 = 1$ ✓

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

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

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

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

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

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

↓

$n=11$ prim (Fermat)

Ex: $n=27 \overset{?}{\Rightarrow} \forall a \in \mathbb{Z}_{27}^*, a^{26}=1$

$a=1 \Rightarrow 1^{26}=1$ ✓

$a=2 \Rightarrow 2^{26}=(2^5)^5\cdot 2 = 32^5\cdot 2 = 5^5\cdot 2 = (5^2)^2\cdot 5\cdot 2 = (-2)^2\cdot 5\cdot 2$

$= 4\cdot 5\cdot 2 = 40 = 13 \neq 1 \Rightarrow n=27$ compus

$a=2$ witness (martor)

↓

Test determinist / exact = dă rezultate certe

Teste probabiliste = dau rezultate cu probabilitate

Avantaj: Dacă găsesc un martor → rezultat negativ cert!

Testul Fermat probabilist

Aleg $t$ elemente $a \in \mathbb{Z}_n^*$ (mostre).

Verific teorema doar cu ele.

Verifică teorema doar cu ele.

↳ dacă toate mostrele verifică ⇒
⇒ $n$ este probabil prim, cu prob $= \frac{t}{n-1}$

↳ dacă una dintre mostre este martor
⇒ $n$ este SIGUR compus!

---

## Testul Solovay-Strassen

### Simbolul Jacobi

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

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

| $x$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|---|
| $x^2$ | 0 | 1 | 4 | 2 | 2 | 4 | 1 |

Ex: $\left(\frac{2}{7}\right) = 1$ pt că $2 = 3^2 \equiv 4^2$

$\left(\frac{9}{831}\right) = 1$ pt că $9 = 3^2$

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

$\left(\frac{17}{5}\right) = \left(\frac{2}{5}\right) = -1$

| $x$ | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| $x^2$ | 0 | 1 | 4 | 4 | 1 |

$\left(\frac{52}{13}\right) = 0$ pt că $13 \mid 52$. $\left(\frac{52}{13}\right) = \left(\frac{0}{13}\right) = 0$ pt

$\left|\frac{\cdot}{13}\right| = 0$ pt ... $\left|\frac{13}{13}\right| = 0$

ca $13 \mid 0$.

**Teoremă (Solovay-Strassen)**

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

Ex: $n = 13 \overset{?}{\Rightarrow} a^6 = \left(\frac{a}{13}\right)$, $\forall a \in \mathbb{Z}_{13}$

$a = 0$ ✓

$a = 1$ ✓

$a = 2 \Rightarrow 2^6 = 2^4 \cdot 2^2 = 3 \cdot 2^2 = 12 = -1$

| | | | | | | | | -6 | -5 | -4 | -3 | -2 | -1 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $x$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
| $x^2$ | 0 | 1 | 4 | 9 | 3 | 12 | 10 | 10 | 12 | 3 | 9 | 4 | 1 |

$\Rightarrow \left(\frac{2}{13}\right) = -1$ ✓ ✓

$a = 3 \Rightarrow 3^6 = (3^3)^2 = 1$ ; $\left(\frac{3}{13}\right) = 1$

$a = 4 \Rightarrow 4^6 = (2^2)^6 = (2^6)^2 = (-1)^2 = 1$ ; $\left(\frac{4}{13}\right) = 1$

$a = 5 \Rightarrow 5^6 = (5^2)^3 = (-1)^3 = -1$ ; $\left(\frac{5}{13}\right) = -1$

$a = 6 \Rightarrow 6^6 = 2^6 \cdot 3^6 = (-1) \cdot 1 = -1$ ; $\left(\frac{6}{13}\right) = -1$

$a = 7 \Rightarrow 7^6 = (-6)^6 = 6^6 = -1$ ; $\left(\frac{7}{13}\right) = -1$

$a = 8 \Rightarrow 8^6 = (-5)^6 = 5^6 = -1$ ; $\left(\frac{8}{13}\right) = -1$

$a = 9 \Rightarrow 9^6 = (-4)^6 = 4^6 = 1$ ; $\left(\frac{9}{13}\right) = 1$

$\ldots^6 \ldots^6 \ldots^6 \ldots$ ; $\left(\frac{10}{13}\right) = -1$

$a=10 \Rightarrow 10^6 = (-3)^6 = 3^6 = 1$ ; $\left(\frac{10}{13}\right) = 1$

$a=11 \Rightarrow 11^6 = (-2)^6 = 2^6 = -1$ ; $\left(\frac{11}{13}\right) = -1$

$a=12 \Rightarrow 12^6 = (-1)^6 = 1$ ; $\left(\frac{12}{13}\right) = 1$

$\Rightarrow n=13$ prim.

Ex: $n=51 \overset{?}{\Rightarrow} \forall a \in \mathbb{Z}_{51}$, $a^{25} = \left(\frac{a}{51}\right)$

$a=2 \Rightarrow 2^{25} = \left(2^6\right)^4 \cdot 2 = 13^4 \cdot 2 = 169^2 \cdot 2 = 16^2 \cdot 2$

$51 \cdot 3 = 153$ ; $169 = 153 + 16$

$= 2^8 \cdot 2 = 2^6 \cdot 2^2 \cdot 2 = 13 \cdot 8 = 104 = 2 \neq \left(\frac{2}{51}\right)$.

$51 \cdot 2 = 102$

$\Rightarrow n=51$ compus, $a=2$ martor.

Obs: Testul SS are și el o variantă probabilistă.

---

## Ordinul unui element într-un grup

Def: Fie $(G,*)$ grup, $g \in G$.

$\text{ord}(g) = n$ dacă $\underbrace{g * g * \dots * g}_{n \text{ ori}} = e$ și $n$ este cel mai mic cu această proprietate.

Dacă nu există ($\underbrace{g * g * \dots * g}_{n \text{ ori}} \neq e, \forall n$), spunem $\text{ord}\, g = \infty$.

Ex: $G = (\mathbb{Z}_7^*, \cdot)$, $g = 3$

$3^1 = 3$, $3^2 = 9 = 2$, $3^3 = 3^2 \cdot 3 = 2 \cdot 3 = 6$;

$3^1 = 3$; $3^2 = 9 = 2$; $3^3 = 3^2 \cdot 3 = 2 \cdot 3 = 6$;

$3^4 = 3^3 \cdot 3 = 6 \cdot 3 = 18 = 4$; $3^5 = 3^4 \cdot 3 = 4 \cdot 3 = 12 = 5$;

$3^6 = 3^5 \cdot 3 = 5 \cdot 3 = 15 = 1 \Rightarrow$ $\underline{\text{ord } 3 = 6 \text{ în } \mathbb{Z}_7^*}$

## Teoremă (Lagrange)

Fie $G$ grup. Numim ordinul grupului numărul de elemente. ($\text{ord } G = \#G$).

Dacă $G$ este finit $\Rightarrow \forall g \in G$, $\text{ord } g \mid \text{ord } G$.

Ex: $G = (\mathbb{Z}_5^*, \cdot)$ $\text{ord } \mathbb{Z}_5^* = 4$

$\underline{\text{ord } 1 = 1}$; $\underline{\text{ord } 2 = 4}$

$2^1 = 2$; $2^2 = 4$; $2^3 = 8 = 3$; $2^4 = 16 = 1$.

$\underline{\text{ord } 3 = 4}$

$3^1 = 3$; $3^2 = 9 = 4$; $3^3 = 27 = 2$; $3^4 = 2 \cdot 3 = 6 = 1$

$\underline{\text{ord } 4 = 2}$ pt că $4^2 = 16 = 1$.

## Teoremă (Fermat)

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

## Logaritmul discret

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

Obs 1. În $\mathbb{Z}_n$, log este șanse computațional.

2. În $\mathbb{Z}_n$, log nu există mereu.

$\log_3 2 = x \Leftrightarrow 3^x = 2$ în $\mathbb{Z}_7$

Ex: $\log_3 2$ în $\mathbb{Z}_7$ $\quad \log_3 2 = x \Leftrightarrow 3^x = 2$ în $\mathbb{Z}_7$

$x = 2$ pt că $3^2 \cdot 9 = 2$

$\log_5 3$ în $\mathbb{Z}_7$ =? $\quad \log_5 3 = x \Leftrightarrow 5^x = 3$ în $\mathbb{Z}_7$

| $x$ | 1 | 2 | 3 | 4 | **5** | 6 |
|---|---|---|---|---|---|---|
| $5^x$ | 5 | 4 | 6 | 2 | **3** | 1 (Fermat) |

în $\mathbb{Z}_7$

$\Rightarrow \log_5 3 = 5$ în $\mathbb{Z}_7$

$\log_3 7$ în $\mathbb{Z}_{11}$ =?

| $x$ | 1 | 2 | 3 | 4 | **5** | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|
| $3^x$ | 3 | 9 | 5 | 4 | **1** | 3 | 9 | 5 | 4 | 1 |

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

$\Rightarrow \log_3 7$ nu există în $\mathbb{Z}_{11}$.

## Generatori și grupuri ciclice

**Def**: Fie $G$ grup, $g \in G$. Pp. $\text{ord } g = n$

$$\Rightarrow \langle g \rangle = \{g, g*g, g*g*g, \dots, \underbrace{g*g*\dots*g}_{n \text{ ori}} = e\}$$

↑ Subgrupul generat de $g$.

**Obs**: $\text{ord } g = \text{ord } \langle g \rangle = \# \langle g \rangle$.

**Def**: Dacă $\langle g \rangle = G \Rightarrow g$ s.n. generator și $G$ s.n. grup ciclic.

Ex: $G = \mathbb{Z}_{11}$ ; $\langle 5 \rangle$ =? ; $\langle 3 \rangle$ =?

| $x$ | 1 | 2 | 3 | 4 | **5** | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|
| $5^x$ | 5 | 3 | 4 | 9 | **1** | | | | | 1 |

$\Rightarrow \operatorname{ord} 5 = 5 \Rightarrow \langle 5 \rangle = \{1, 3, 4, 5, 9\}$

$\Rightarrow$ 5 NU este generator.

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

$\Rightarrow \langle 3 \rangle = \{1, 3, 4, 5, 9\} \Rightarrow \operatorname{ord} 3 = 5 \Rightarrow 3$ NU este generator.

$\langle 7 \rangle = ?$

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

$\Rightarrow \operatorname{ord} 7 = 10 \Rightarrow \langle 7 \rangle = \mathbb{Z}_{11}^* \Rightarrow \mathbb{Z}_{11}^*$ ciclic

7 este (un) generator

## Indicatorul lui Euler

**Def**: Fie $n \in \mathbb{N}$. $\varphi(n) = \#\{1 \leq x < n \mid \operatorname{cmmdc}(x, n) = 1\}$

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

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

**Ex**: $\varphi(153) = ?$

| 153 | 3 |
|---|---|
| 51 | 3 |
| 17 | 17 |

$153 = 3^2 \cdot 17 \Rightarrow$

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

Ex: $\varphi(82)$

$82 = 2 \cdot 41$

$\Rightarrow \varphi(82) = \varphi(2)\,\varphi(41) = 1 \cdot 40 = 40.$