Coduri simple (Caesar, afin, Hill)

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

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

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
0	1	2	3	4	5	6	7	8	9	10	11	12

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 $\mathbb{Z}_{26} = \{0, 1, \dots, 25\}$, dar nr pare nu au invers multiplicativ ($\nexists\, 2^{-1}, 4^{-1}, 6^{-1},$

$\Rightarrow$ creează probleme la decriptare

Adaug ␣ · !

␣	.	!
26	27	28

$\Rightarrow$ lucrez în $\mathbb{Z}_{29}$, 29 prim $\Rightarrow$

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

$\rightarrow$ VKLVRA

ASTAZI $\longrightarrow$ VKLVRA

Decriptare:

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

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

Varianta pe blocuri

Blocuri de lungime 3 : ASTAZI $\rightarrow$ AST $\rightarrow$ cheie1 =
AZI $\rightarrow$ cheie2 =

$[A, S, T] \rightarrow [0, 18, 19] \xrightarrow[+\text{cheie}1]{+15} [15, 33, 34] \xrightarrow[\text{mod } 29]{} [15, 4, \ldots$

$[A, Z, I] \rightarrow [0, 25, 8] \xrightarrow[+\text{cheie}2]{+23} [23, 48, 31] \xrightarrow[\text{mod } 29]{} [23, 19, \ldots$

ASTAZI $\rightarrow$ PEFXTC

Cu padding random: Lungimea blocurilor = 5

ASTAZI $\rightarrow$ ASTAZ ; cheie1 = 10
$\underbrace{\text{I X ! B U}}_{\text{padding random}}$; cheie2 = 15

Cifrul afin

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

49 - 9 , 7 1

Decriptare:

$$X \sqcup B O J i \to [23, 26, 1, 14, 9, 8] \xrightarrow[-11,\ \cdot 6^{-1} = 5]{-\text{cheie}_2,\ \cdot \text{chei}^{-1}} [60, 75, -50, 15$$

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

$-50 = -58 + 8 = 8$

Cifrul Hill

- Folosește matrice de criptare

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

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: $\begin{pmatrix} M \\ S \\ J \end{pmatrix} = \begin{pmatrix} J \\ o \\ i \end{pmatrix} = \begin{pmatrix} 9 \\ 14 \\ 8 \end{pmatrix}$; $Mat = \begin{pmatrix} 1 & -1 & 0 \\ 1 & 0 & -1 \\ -2 & 1 & 0 \end{pmatrix}$

$\det(Mat) = -2 + 1 = -$

$\begin{pmatrix} 1 & -1 & 0 \end{pmatrix} \begin{pmatrix} 9 \end{pmatrix} \quad \begin{pmatrix} -5 \end{pmatrix}$

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

Decriptarea:

$$\underbrace{28 \cdot \begin{pmatrix} 1 & 0 & 1 \\ 2 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix}}_{Mat^{-1}} \cdot \underbrace{\begin{pmatrix} 24 \\ 1 \\ 25 \end{pmatrix}}_{cod} = \Big($$

Teste de primalitate

Ciurul (sita) lui Eratostene

Primește $n \in \mathbb{N}^*$

Produce nr. prime $\leq n$

Ex.: $n = 29$

$\boxed{2}$ $\boxed{3}$ $\cancel{4}$ $\boxed{5}$ $\cancel{6}$ $\boxed{7}$ $\cancel{8}$ $\cancel{9}$ $\cancel{10}$ $\boxed{11}$

$\cancel{16}$ $\boxed{17}$ $\cancel{18}$ $\boxed{19}$ $\cancel{20}$ $\cancel{21}$ $\cancel{22}$ $\boxed{23}$ $\cancel{24}$ $\cancel{25}$

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

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

$a=1 \Rightarrow 1^{10} = 1$ ok. ✓

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

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

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

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

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

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

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

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

$\qquad n =$

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

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

$a=1 \Rightarrow 1^{26} = 1$ ✓

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

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

$a=2$ witness (n

Aleg l elemente $a \in \mathbb{Z}_n$ (mostre).
Verific teorema doar cu ele.
↳ dacă toate mostrele ver
$\Rightarrow n$ este probabil

↳ dacă una dintre mostre
$\Rightarrow n$ este SIGUR

Testul Solovay - Strassen

Simbolul Jacobi

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

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

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

x	0	1	2
x^2	0	1	4

$\left(\frac{52}{13}\right) = 0$ pt ca $13 \mid 52$. $\Big($ [illegible]

Teoremă (Solovay-Strassen)

Dacă n este prim $\Rightarrow a^{\frac{n-1}{2}} = \Big($ [illegible]

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

$a = 0$ ✓
$a = 1$

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

x	0	1	2	3	4	5	6	7
x^2	0	1	4	9	3	12	10	10

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

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

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