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