(1) 09.04.24

ElemTNF – 311

CRIPTOSISTEM AFIN PE DIGRAFURI NUMERICE = criptosistem în cadrul căruia digrafurile peste un alfabet cu n litere sunt privite ~~ca nr. de două cifre în baza n (deci, corespunzând~~ ~~[illegible]~~ drept clasele (modulo n^2) ale numerelor corespunzătoare de două cifre în baza n, iar funcția de criptare e de forma $e: \mathbb{Z}_{n^2} \to \mathbb{Z}_{n^2}$,

$e(x) = mx + n$,

$m, n \in \mathbb{Z}_{n^2}$, m inversabil.

Obs: Funcția de decriptare are aceeași formă cu cea de criptare!

Notație $d: \Sigma_{1089} \to \Sigma_{1089}$

$d(x) = mx + n$ funcția de decriptare

$$\text{Știm: } \begin{cases} d(\widehat{NF}) = \widehat{re}_{(33)} \\ d(\widehat{KL}) = \widehat{ar}_{(33)} \end{cases} \quad (5)$$

adelcă

A	Ă	Â	B	C	D	E	F	G	H	I	Î	J
0	1	2	3	4	5	6	7	8	9	10	11	12

K	L	M	N	O	P	Q	R	S	Ș	T	Ț	U	V	W	X
13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28

Y	Z	-	.
29	30	31	32.

$NF_{(33)} = 16 \cdot 33 + 7 = 535$

$re_{(33)} = 20 \cdot 33 + 6 = 666$

$KL_{(33)} = 13 \cdot 33 + 14 = 443$

$a z_{(33)} = 0 \cdot 33 + 20 = 20$.

Le système (S) devient

$$\begin{cases} 535m + n = 666 \\ 443m + n = 20 \end{cases} \quad (\text{dans } \mathbb{Z}/1089\mathbb{Z})$$

$$\begin{cases} 92m = 646 \\ 443m + n = 20 \end{cases} \text{ dans } \mathbb{Z}/1089\mathbb{Z} \iff \begin{cases} 46m = 323 \\ 443m + n = 20 \end{cases}.$$

Résolvons $46m = 323$ dans l'anneau $\mathbb{Z}/1089\mathbb{Z}$ et calculons l'inverse de 46 modulo 1089.

$$\frac{1089}{46} = 23 + \frac{31}{46} = 23 + \frac{1}{1 + \frac{15}{31}} = 23 + \frac{1}{1 + \frac{1}{2 + \frac{1}{15}}}$$

$$23 + \frac{1}{1 + \frac{1}{2}} = \frac{71}{3}.$$

Comme $3 \cdot 1089 - 71 \cdot 46 = 1$, l'inverse de 46 modulo 1089 est -71.

Ce qui donne $m = 323 \cdot (-71) = -64$.

deci $(\exists)$ $\Leftrightarrow$ $\begin{cases} m = -64 \\ m = 20 + 64 \cdot 443 \end{cases}$ $\Leftrightarrow$ (4)

$\Leftrightarrow$ $m = -64$

$m = 58$.

Ca urmare, funcția de descriptare e $d: \mathbb{Z}_{1089} \to \mathbb{Z}_{1089}$ $d(x) = -64x + 58$.

Acum descifrăm mesajul:

$d(\widehat{\_Y}_{(33)}) = -64 \cdot 1052 + 58 = 248 = \widehat{fo}_{(33)}$

$d(\widehat{KL}_{(33)}) = -64 \cdot 443 + 58 = 20 = \widehat{ar}_{(33)}$

$d(\widehat{\tilde{A}F}_{(33)}) = -64 \cdot 38 + 58 = 765 = \widehat{te}_{(33)}$

$d(\widehat{BS}_{(33)}) = -64 \cdot 121 + 58 = 1026 = \widehat{\_b}_{(33)}$

$d(\widehat{NJ}_{(33)}) = -64 \cdot 540 + 58 = 346 = \widehat{in}_{(33)}$

$d(\widehat{S,R}_{(33)}) = -64 \cdot 746 + 58 = 230 = \widehat{e!}_{(33)}$

Deci, mesajul inițial e „foarte_bine!"