Temă 2 Criptografie

Herrmeneanu Mara
Oprian George

① a) MCCLL IMIPP ISKLN UH CGI MCKBI
XCUMTT IPLKX LRIGW MCXLA MWALV
CCAGJ KXYCR

= Analiza frecventei literelor =

C → 9	G → 3	R → 2	T → 1
I → 7	P → 3	A → 1	V → 1
L → 7	A → 2	H → 1	Y → 1.
M → 6	U → 2	J → 1	
K → 4	W → 2	N → 1	
X → 4	B → 1	S → 1	

Presupun că C corespunde lui E și I lui T

Fie $f(x) = ax + b$ funcția de criptare

$f: \mathbb{Z}_{26} \to \mathbb{Z}_{26}$

$\Rightarrow \begin{cases} f(4) = 2 \\ f(19) = 8 \end{cases} \Leftrightarrow \begin{cases} 4a + b = 2 \\ 19a + b = 8 \end{cases} \Rightarrow 5a \equiv 2$

$\Rightarrow a \equiv 16.$

- nu convine. $\gcd(a, 26) \neq 1$

Presupun C corresp lui E și L lui T

$$\Rightarrow \begin{cases} 4a+b=2 \\ 19a+b=11 \end{cases} \Rightarrow 5a=3 \Rightarrow a \equiv 11 \pmod{26}$$

$$\Rightarrow 18a+b=2 \Rightarrow b \equiv -16 \equiv 10 \pmod{26}$$

$$\Rightarrow f(x) = 11x+10$$

$$\Rightarrow \text{funcția de decriptare } f^{-1}: \mathbb{Z}_{26} \to \mathbb{Z}_{26}$$

$$f^{-1}(y) = a^{-1}(y-b) = 19(y-10)$$

	C	I	L	M	K	X	G	P	A	R	U
y	2	8	11	12	10	23	6	15	0	17	20
f^{-1}	4	14	19	12	0	13	2	17	18	3	8
	E	O	T	M	A	N	C	R	S	D	I

	B	W	A	H	J	N	S	T	V	Y
y	1	22	3	7	9	13	18	19	21	24
f^{-1}	11	20	23	21	7	5	22	15	1	6
	L	U	X	V	H	F	W	P	B	G

→ Mesajul devine

MEET TOMORROW AT FIVE COME ALONE IMPORTANT AOCUMENTS MUST BE EXCHANGEA

b) B FNPKK A ÇAI

= Analiza frecvenței literelor =

A → 2 F → 1
A K → 2 I → 1
B → 1 N → 1
C → 1 P → 1

Presupun B corespunde lui I și A lui A (A este mai probabil să apară în mijlocul cuvintelor decât I)

⇒ Fie $f(x) = ax+b$ funcția de criptare

$f: \mathbb{Z}_{26} \to \mathbb{Z}_{26}$. $f(8) = 1$; $f(0) = 3$

Avem: $\begin{cases} 8a+b = 1 \\ b \equiv 3 \end{cases} \Rightarrow a \equiv 3$ $\gcd(a, 26) = 1$.

⇒ $f(x) = 3x+3$ ⇒ funcția de decriptare

$f^{-1}: \mathbb{Z}_{26} \to \mathbb{Z}_{26}$ $f^{-1}(y) = a^{-1}(y-b) = \cancel{19(x-3)}$ $9(x-3)$

	A	K	B	C	F	I	N	P
y	3	10	1	2	5	8	13	15
f^{-1}	0	11	8	17	18	19	12	4
	A	L	I	R	S	T	M	E

$\Rightarrow$ MESAJUL AEVINE:

I SMELL A RAT

② a) b) Card mulț cheilor pt cifrul Hill

$n=2$ $b=(0,0)$ peste $\mathbb{Z}_{26}$, $\mathbb{Z}_{41}$

c) Trebuie să determinăm nr de matrice 2×2 inversab peste $\mathbb{Z}_p$.

Matricea este inversab dacă coloanele sunt vect liniar indep. Pentru prima coloană am p^2-1 posibilități, a.i o pot alege oricum, cu excepția vect $(0,0)$

În ceea ce privește a doua coloană, trebuie să avem grijă ca aceasta să nu fie un multiplu al primei coloane $\Rightarrow$ $p^2-1-(p-1)=p^2-p$ moduri de a o alege (coloana 1 poate fi înmulțită cu $p-1$ scalari)

$\Rightarrow$ Nr de matrice inversab în $\mathbb{Z}_p = (p^2-1)(p^2-p)$

$\Rightarrow$ a) $(26^2-1)(26^2-26)$

b) $(41^2-1)(41^2-41)$

② c) Card mulț cheilor unui cifru Hill cu $n = m$ și $b = (0, \underbrace{0, \dots}_{m} 0)$

La fel ca la a și b, trebuie să det nr de matrice inversab $M_m(\mathbb{Z}_p)$

Matricea este inversab $\Leftrightarrow$ coloanele sunt vect liniar indep.

col 1 → $p^m - 1$ posibilități

col 2 → $p^m - p$ posibil.

col 3 → $p^m - p^2$ posib. (col 3 se poate scrie ca o comb lin a col 1 și 2 în p^2 moduri)

...

col m → $p^m - p^{m-1}$ posib.

$\Rightarrow$ Nr de matrice inversab $M_m(\mathbb{Z}_p) =$

$$(p^m - 1)(p^m - p) \cdots (p^m - p^{m-1})$$