Cifrul Hill

Cifrul Hill - cazul 2×2 / $\mathbb{Z}_{26}$: Fie A o matrice inversabilă 2×2 modulo 26; aceasta va fi cheia pt cifrul Hill. Împărțim mesajul în blocuri de câte 2. Scriem fiecare bloc ca vector coloană, aplicăm matricea A, și reducem modulo 26. Astfel obținem textul cifrat. Pt a decoda, împărțim blocul primit în secțiuni de câte 2 și aplicăm matricea inversă.

Exemplu:

Să criptăm mesajul ET PHONE HOME. Împărțim în blocuri de câte 5 litere pt a obscurizare mesajul (ETPHO NEHOM E). Trebuie să alegem o matrice de 2×2 care să acționeze pe post de cheie (⚠ Matricea aleasă trebuie să fie inversabilă).

Împărțim mesajul în blocuri de lungime 2 deoarece acesta este numărul de rânduri și coloane din matricea cheie. Deci, alegem matricea $\begin{pmatrix} 3 & 6 \\ 1 & 3 \end{pmatrix}$ → cheie și

secționăm mesajul astfel:

ET PH OH EH OM ET

De observat este faptul că, am adăugat o literă în plus (oarecare) pt a obține un număr par de litere ("E[T]").

Fiecare bloc de 2 litere, vă fi tratat ca un vector coloană de numere modulo 26. Din moment ce E corespunde numărului 4 și T corespunde numărului 19, primul bloc din mesajul nostru va fi $\begin{pmatrix} 4 \\ 19 \end{pmatrix}$

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14

P	Q	R	S	T	U	V	W	X	Y	Z
15	16	17	18	19	20	21	22	23	24	25

După ce convertim și celelalte blocuri, vedem că mesajul va corespunde următorilor vectori coloană:

$$\begin{pmatrix} 4 \\ 19 \end{pmatrix}, \begin{pmatrix} 15 \\ 7 \end{pmatrix}, \begin{pmatrix} 14 \\ 13 \end{pmatrix}, \begin{pmatrix} 4 \\ 7 \end{pmatrix}, \begin{pmatrix} 14 \\ 12 \end{pmatrix}, \begin{pmatrix} 4 \\ 19 \end{pmatrix}$$

Pasul de încriptare, presupune să înmulțim fiecare dintre aceste matrici cu matricea cheie modulo 26.

De ex, prima matrice se va transforma în:

$$\begin{pmatrix} 3 & 6 \\ 1 & 3 \end{pmatrix} \begin{pmatrix} 4 \\ 19 \end{pmatrix} = \begin{pmatrix} 3 \cdot 4 + 6 \cdot 19 \\ 1 \cdot 4 + 3 \cdot 19 \end{pmatrix} = \begin{pmatrix} 126 \\ 61 \end{pmatrix} = \begin{pmatrix} 22 \\ 9 \end{pmatrix} \mod 26$$

După ce vom efectua și restul operațiilor, vom obține vectorii caracteristici:

$$\begin{pmatrix} 2 & 2 \\ 9 & \end{pmatrix} \cdot \begin{pmatrix} 9 \\ 10 \end{pmatrix} \cdot \begin{pmatrix} 16 \\ 1 \end{pmatrix} \cdot \begin{pmatrix} 2 \\ 25 \end{pmatrix} \cdot \begin{pmatrix} 10 \\ 24 \end{pmatrix} \cdot \begin{pmatrix} 22 \\ 9 \end{pmatrix}$$

Pt a obține textul cifrat, facem corespondența înapoi la litere și obținem:

WJ JK QB CZ KY WJ și le grupăm.

Prin urmare textul cifrat va fi:

WJJKQ BCZKYW J

Decriptarea funcționează înmulțind cu inversa matricei de criptare. Matricea aleasă de noi este inversabilă modulo 26.

Deci inversa modulo 26 în cazul nostru va fi:

$$A = \begin{pmatrix} 3 & 6 \\ 1 & 3 \end{pmatrix} \quad A^{-1} = ? \quad \mathbb{Z}_{26}$$

$$A^{-1} = \text{inv}(\det A) \cdot \text{adj}_g A^t = \bar{9} \begin{pmatrix} \bar{3} & -\bar{6} \\ -\bar{1} & \bar{3} \end{pmatrix} = \begin{pmatrix} \overline{27} & -\overline{54} \\ -\bar{9} & \overline{27} \end{pmatrix}$$

$$= \begin{pmatrix} \bar{1} & \overline{24} \\ \overline{17} & \bar{1} \end{pmatrix}$$

$-\overline{54} \quad \mathbb{Z}_{26}$

$-54 = 26 \cdot (-?) + ?$

$-54 = -78 + \boxed{24}$

$-54 = -54$

$-9 = 26 \cdot (-?) + ?$ $\quad -\bar{9} \in \mathbb{Z}_{26}$

$-9 = 26 \cdot (-1) + \boxed{17}$

$-9 = -26 + 17$

$-9 = -9$

$\det A = \bar{3} \cdot \bar{3} - \bar{1} \cdot \bar{6} = \bar{3}$

$\text{adj}_3\, A^t = \begin{pmatrix} +\bar{3} & -\bar{1} \\ -\bar{6} & \bar{3} \end{pmatrix}$

$= \begin{pmatrix} \bar{3} & -\bar{6} \\ -\bar{1} & \bar{3} \end{pmatrix}$

$\text{inv } \bar{3} \text{ in } \mathbb{Z}_{26} = ?$

$\gcd(26, 3) = 1 \Rightarrow$

Bezout $26t + 3s = 1$

$26 = 3 \cdot 8 + 2$

$3 = 2 \cdot 1 + 1$

$2 = 1 \cdot 2 + 0$ STOP

$2 = 26 - 3 \cdot 8$

$1 = 3 - 2 \cdot 1$

$26(-1) + 3 \cdot \boxed{9} = 1$

$\Rightarrow$ inv lui „3" el lui $\bar{3}$ în $\mathbb{Z}_{26} = 9$

$1 = 3 - (26 - 3 \cdot 8)$

$= 3 - 26 + 3 \cdot 8$

$= 3 \cdot 9 - 26$

$= 3 \cdot 9 + 26(-1)$

Pt a decripta primul bloc de textul cifrat, ne folosim de inversa matricei de mai sus (inversa)

$\begin{pmatrix} 1 & 24 \\ 17 & 1 \end{pmatrix} \begin{pmatrix} 22 \\ 9 \end{pmatrix} = \begin{pmatrix} 4 \\ 19 \end{pmatrix} \bmod 26$

Am rezultat astfel primul vector sub forma de text, ET.

Restul mesajului se găsește în mod similar.

Descifrarea funcționează deoarece înmulțind cu matricea inversă inversării înmulțirea inițială. O modalitate mai formală de a privi lucrurile este că începem cu un vector $\vec{v}$, aplicăm matricea cheie și obținem $A\vec{v}$, după care aplicăm matricea de descifrare A^{-1}, obținând $A^{-1} \cdot (A\vec{v})$. Înmulțirea matricilor este asociativă, ceea ce ne permite să grupăm parantezele.

Deci, tentativa noastră de a descifra, $A^{-1}(A\vec{v})$ va fi egală cu $(A^{-1} \cdot A) \cdot \vec{v}$ dar vom obține doar $\vec{v}$ de moment ce $A^{-1} \cdot A$ este matricea identitate modulo 26 și $\underline{I} \cdot \vec{v} = \vec{v}$ pt toți vectorii. Putem vedea acest lucru, revizitând descifrarea de mai devreme. În exemplul nostru, avem:

$$\begin{pmatrix} 1 & 24 \\ 17 & 1 \end{pmatrix} \begin{pmatrix} 22 \\ 9 \end{pmatrix} = \begin{pmatrix} 1 & 24 \\ 17 & 1 \end{pmatrix} \begin{pmatrix} 36 \\ 13 \end{pmatrix} \begin{pmatrix} 4 \\ 19 \end{pmatrix}$$

$$= \begin{pmatrix} 10 \\ 01 \end{pmatrix} \begin{pmatrix} 4 \\ 19 \end{pmatrix} = \begin{pmatrix} 4 \\ 19 \end{pmatrix} \bmod 26$$