20/07/23

* Hill cipher :→

COMPUTER

Step 1: Select message to encrypt
COMPUTER

$\begin{bmatrix} - & - & - \\ - & - & - \\ - & - & - \end{bmatrix}_{3\times3} = \begin{bmatrix} \; \end{bmatrix}_{3\times1}$

Step 2: Select a key in dgyf

$\begin{bmatrix} - & - \\ - & - \end{bmatrix}_{2\times2} = \begin{bmatrix} \; \end{bmatrix}_{2\times1}$

$=4$

Step 3: Lets us assign a numerical equivalent

for mod we start for 0.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17

S	T	U	V	W	X	Y	Z
18	19	20	21	22	23	24	25

Step 4: convert the key dbgf to 2x2 matrix to each

$$\text{key } k = \begin{bmatrix} d & b \\ g & f \end{bmatrix} = \begin{bmatrix} 3 & 1 \\ 6 & 5 \end{bmatrix}$$

key is done.

Step 5: convert the message COMPUTER to a "n" component vector.

$$\underbrace{\begin{bmatrix} C \\ O \end{bmatrix}}_{2\times1} \underbrace{\begin{bmatrix} M \\ P \end{bmatrix}}_{2\times1} \underbrace{\begin{bmatrix} U \\ T \end{bmatrix}}_{2\times1} \underbrace{\begin{bmatrix} E \\ R \end{bmatrix}}_{2\times2}$$

$$\begin{bmatrix} 2 \\ 14 \end{bmatrix} \begin{bmatrix} 12 \\ 15 \end{bmatrix} \begin{bmatrix} 20 \\ 19 \end{bmatrix} \begin{bmatrix} 4 \\ 17 \end{bmatrix}$$

Step 6: cipher text = K * P mod 26

$$= \begin{bmatrix} 3 & 1 \\ 6 & 5 \end{bmatrix} \begin{bmatrix} C \\ O \end{bmatrix} \text{ mod } 26$$

$$= \begin{bmatrix} 3 & 1 \\ 6 & 5 \end{bmatrix} \begin{bmatrix} 2 \\ 14 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 3\times2 + 1\times14 \\ 6\times2 + 5\times14 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 6 + 14 \\ 12 + 70 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 20 \\ 82 \end{bmatrix} \bmod 26$$

20 mod 26 = 20 ~ U

82 mod 26 = 4 ~ E

$$= \begin{bmatrix} 20 \\ 4 \end{bmatrix}$$

$$= \begin{bmatrix} U \\ E \end{bmatrix}$$

cipher text = K * P mod 26

$$= \begin{bmatrix} 3 & 1 \\ 6 & 5 \end{bmatrix} \begin{bmatrix} M \\ P \end{bmatrix} \bmod 26$$

$$= \underbrace{\begin{bmatrix} 3 & 1 \\ 6 & 5 \end{bmatrix} \begin{bmatrix} 12 \\ 15 \end{bmatrix}}_{2\times2} \bmod 26$$

$$= \begin{bmatrix} 3\times12 + 12\times15 \\ 6\times12 + 85\times15 \end{bmatrix} \bmod 26$$

$$= \cancel{\begin{bmatrix} 36 & 180 \\ 24 & 225 \end{bmatrix} \bmod 26} = \begin{bmatrix} 51 \\ 147 \end{bmatrix} \bmod 26$$

51 mod 26 = 25 ~ Z

147 mod 26 = 17 ~ R

$$\begin{bmatrix} Z \\ R \end{bmatrix} = \begin{bmatrix} 25 \\ 17 \end{bmatrix}$$

cipher text = K * P mod 26

$$= \begin{bmatrix} 3 & 1 \\ 6 & 5 \end{bmatrix} \begin{bmatrix} U \\ T \end{bmatrix} \text{ mod } 26$$

$$= \begin{bmatrix} 3 & 1 \\ 6 & 5 \end{bmatrix} \begin{bmatrix} 20 \\ 19 \end{bmatrix} \text{ mod } 26$$

$$= \begin{bmatrix} 3 \times 20 + 1 \times 19 \\ 6 \times 20 + 5 \times 19 \end{bmatrix} \text{ mod } 26$$

$$= \begin{bmatrix} 60 + 19 \\ 120 + 95 \end{bmatrix} \text{ mod } 26$$

$$= \begin{bmatrix} 79 \\ 215 \end{bmatrix} \text{ mod } 26$$

79 mod 26

215 mod 26

$$= \begin{bmatrix} 1 \\ 7 \end{bmatrix} \sim \begin{bmatrix} B \\ H \end{bmatrix}$$

cipher text = $K * P \bmod 26$

$$= \begin{bmatrix} 3 & 1 \\ 6 & 5 \end{bmatrix} \begin{bmatrix} E \\ R \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 3 & 1 \\ 6 & 5 \end{bmatrix} \begin{bmatrix} 4 \\ 17 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 3 \times 4 & + & 1 \times 17 \\ 6 \times 4 & + & 5 \times 17 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 12 + 17 \\ 24 + 85 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 29 \\ 109 \end{bmatrix} \bmod 26$$

$29 \bmod 26$

$109 \bmod 26$

$$= \begin{bmatrix} 3 \\ 5 \end{bmatrix} \sim \begin{bmatrix} D \\ F \end{bmatrix}$$

cipher text = $\begin{bmatrix} V \\ E \end{bmatrix} \begin{bmatrix} Z \\ R \end{bmatrix} \begin{bmatrix} B \\ H \end{bmatrix} \begin{bmatrix} D \\ F \end{bmatrix}$

Decryption: →

plain text $= K^{-1} \times C \bmod 26$
(inverse of K)

* inverse of K means invert of a matrix

* 2×2 matrix means of no. $\begin{bmatrix} - & - \\ - & - \end{bmatrix}$

$K^{-1} = \frac{1}{|K|} \text{adj } K$

adj K → adjoint

|K| → determinant

Compute $\frac{1}{|K|}$: → $|K| = \begin{vmatrix} 3 & 1 \\ 6 & 5 \end{vmatrix} = |3\times5 - 6\times1|$

$= |15 - 6|$

$= 9$

Rule:

a mod b = 1

Ex. 9 mod 26

9 mod 26
9×1 mod 26

$\frac{1}{|K|} = \underline{\underline{3}}$

9 mod 26
$\underline{\underline{9}}$

$$26 \overline{)\,27\,}(3$$
$$\underline{-26}$$
$$\underline{\underline{1}}$$

9×2 mod 26
18 mod 26
$\underline{\underline{18}}$

compute adj(K) : →

$K = \begin{bmatrix} 3 & 1 \\ 6 & 5 \end{bmatrix}$

9×3 mod 26
27 mod 26

$= \begin{bmatrix} 5 & -1 \\ -6 & 3 \end{bmatrix}$

$$K^{-1} = \frac{1}{|K|} \text{adj}(K)$$

$$K^{-1} = 3 \cdot \begin{bmatrix} 5 & -1 \\ -6 & 3 \end{bmatrix}$$

$$= \begin{bmatrix} 15 & -3 \\ -18 & 9 \end{bmatrix}$$

$$= \begin{bmatrix} 15 & -3+26 \\ -18+26 & 9 \end{bmatrix}$$

$$\therefore K^{-1} = \begin{bmatrix} 15 & 23 \\ 8 & 9 \end{bmatrix}$$

$$\text{plain text} = K^{-1} \times C \mod 26$$

$$= \begin{bmatrix} 15 & 23 \\ 8 & 9 \end{bmatrix} \times \begin{bmatrix} U \\ E \end{bmatrix} \mod 26$$

$$= \begin{bmatrix} 15 & 23 \\ 8 & 9 \end{bmatrix} \begin{bmatrix} 20 \\ 4 \end{bmatrix} \mod 26$$

$$= \begin{bmatrix} 15 \times 20 + 23 \times 4 \\ 8 \times 20 + 9 \times 4 \end{bmatrix} \mod 26$$

$$= \begin{bmatrix} 300 + 92 \\ 160 + 36 \end{bmatrix} \mod 26$$

$$= \begin{bmatrix} 392 \\ 196 \end{bmatrix} \mod 26$$

$$392 \mod 26$$

$$196 \mod 26$$

$$= \begin{bmatrix} 2 \\ 14 \end{bmatrix} \sim \begin{bmatrix} C \\ O \end{bmatrix}$$

$$\text{plain text} = K^{-1} \times C \bmod 26$$

$$= \begin{bmatrix} 15 & 23 \\ 8 & 9 \end{bmatrix} \begin{bmatrix} Z \\ R \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 15 \cancel{R} & 23 \\ 8 \cancel{\times} & 9 \end{bmatrix} \begin{bmatrix} 25 \\ 17 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 15 \times 25 + 23 \times 17 \\ 8 \times 25 + 9 \times 17 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 766 \\ 353 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 12 \\ 15 \end{bmatrix} \sim \begin{bmatrix} M \\ P \end{bmatrix}$$

$$\text{plain text} = K^{-1} \times C \bmod 26$$

$$= \begin{bmatrix} 15 & 23 \\ 8 & 9 \end{bmatrix} \begin{bmatrix} B \\ H \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 15 & 23 \\ 8 & 9 \end{bmatrix} \begin{bmatrix} 1 \\ 7 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 15 \times 1 + 23 \times 7 \\ 8 \times 1 + 9 \times 7 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 15 + 161 \\ 8 + 63 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 176 \\ 71 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 20 \\ 19 \end{bmatrix} \sim \begin{bmatrix} U \\ T \end{bmatrix}$$

plain text = $K^{-1} \times C \bmod 26$

$$= \begin{bmatrix} 15 & 23 \\ 8 & 9 \end{bmatrix} \begin{bmatrix} D \\ F \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 15 & 23 \\ 8 & 9 \end{bmatrix} \begin{bmatrix} 3 \\ 5 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 15 \times 3 + 23 \times 5 \\ 8 \times 3 + 9 \times 5 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 45 + 115 \\ 24 + 45 \end{bmatrix} \bmod 26$$

160 mod 26

69 mod 26

$$= \begin{bmatrix} 4 \\ 17 \end{bmatrix} \sim \begin{bmatrix} E \\ R \end{bmatrix}$$

plain text = $\begin{bmatrix} C \\ O \end{bmatrix} \begin{bmatrix} M \\ P \end{bmatrix} \begin{bmatrix} U \\ T \end{bmatrix} \begin{bmatrix} E \\ R \end{bmatrix}$