22F-3875 M. Faizan Yousaf Course ⇒ IS BCS-7F

CP#1

"Hill Cipher on 3x3 Matrix"

Given Info ⇒ We have our Plaintext ⇒ Name & Key ⇒ Roll# & course

Plaintext ⇒ ranafizan (using 9 characters for 3x3)

Key ⇒ f223875IS

Note ⇒ Remember all alphabets are small lowercase

Step#1 ⇒ Define Dictionary (Using own choice)

0	1	2	3	4	5	6	7	8	9	a	b
0	1	2	3	4	5	6	7	8	9	10	11
c	d	e	f	g	h	i	j	k	l	m	n
12	13	14	15	16	17	18	19	20	21	22	23
o	p	q	r	s	t	u	v	w	x	y	z
24	25	26	27	28	29	30	31	32	33	34	35

Step2 ⇒ Represent key and Text from Dictionary

$$key = \begin{bmatrix} f & 2 & 2 \\ 3 & 8 & 7 \\ 5 & I & S \end{bmatrix} \Rightarrow \begin{bmatrix} 15 & 2 & 2 \\ 3 & 8 & 7 \\ 5 & 18 & 28 \end{bmatrix}$$

$$Text \Rightarrow \begin{bmatrix} r & a & n \\ a & f & i \\ z & a & n \end{bmatrix}_{3\times3} \Rightarrow \text{Represent into 3 (3x1) pairs} \Rightarrow \begin{bmatrix} r \\ a \\ n \end{bmatrix}_{3\times1}, \begin{bmatrix} a \\ f \\ i \end{bmatrix}_{3\times1}, \begin{bmatrix} z \\ a \\ n \end{bmatrix}_{3\times1}$$

⇒ **Step3 ⇒ Encryption Process** (As we have 36 values so we will take (mod 36) **and solve**

$C = KP \bmod 36$ ⇒ a) $\begin{bmatrix} r \\ a \\ n \end{bmatrix} \Rightarrow \begin{bmatrix} 27 \\ 10 \\ 23 \end{bmatrix}$ So Multiply with "C"

$$C_1 = \begin{bmatrix} 15 & 2 & 2 \\ 3 & 8 & 7 \\ 5 & 18 & 28 \end{bmatrix} \times \begin{bmatrix} 27 \\ 10 \\ 23 \end{bmatrix} \Rightarrow \begin{bmatrix} (15\times27)+(2\times10)+(2\times23) \\ (3\times27)+(8\times10)+(7\times23) \\ (5\times27)+(18\times10)+(28\times23) \end{bmatrix} \Rightarrow$$

$\begin{bmatrix}475\\337\\959\end{bmatrix}$ Mod 36 $\Rightarrow$ $\begin{bmatrix}7\\13\\23\end{bmatrix}$, $C_1 = \begin{bmatrix}7\\13\\23\end{bmatrix} = \begin{bmatrix}r\\a\\n\end{bmatrix}$

2) $\begin{bmatrix}a\\f\\i\end{bmatrix} \Rightarrow \begin{bmatrix}10\\15\\18\end{bmatrix}$ so $C_2 = \begin{bmatrix}15 & 2 & 2\\3 & 8 & 7\\5 & 18 & 28\end{bmatrix} \times \begin{bmatrix}10\\15\\18\end{bmatrix}$

$\Rightarrow \begin{bmatrix}(15\times10)+(2\times15)+(2\times18)\\(3\times10)+(8\times15)+(7\times18)\\(5\times10)+(18\times15)+(28\times18)\end{bmatrix} \Rightarrow \begin{bmatrix}186\\240\\754\end{bmatrix}$ Mod 36

$\Rightarrow \begin{bmatrix}6\\24\\34\end{bmatrix} \Rightarrow C_2 = \begin{bmatrix}6\\24\\34\end{bmatrix} \Rightarrow \begin{bmatrix}g\\f\\i\end{bmatrix}$

3) $\begin{bmatrix}z\\a\\n\end{bmatrix} \Rightarrow \begin{bmatrix}35\\10\\23\end{bmatrix} \Rightarrow C_3 \Rightarrow \begin{bmatrix}15 & 2 & 2\\3 & 8 & 7\\5 & 18 & 28\end{bmatrix} \times \begin{bmatrix}35\\10\\23\end{bmatrix}$

$\Rightarrow \begin{bmatrix}(15\times35+2\times10+2\times23)\\(3\times35+8\times10+7\times23)\\(5\times35+18\times10+28\times23)\end{bmatrix} \Rightarrow \begin{bmatrix}601\\336\\1024\end{bmatrix}$ Mod 36 $\Rightarrow \begin{bmatrix}25\\12\\16\end{bmatrix} \Rightarrow C_3 = \begin{bmatrix}z\\a\\n\end{bmatrix}$

Now get new cipherText from PlainText by Encryption

PlainText $\Rightarrow$ "Ranafizan" , CipherText $\Rightarrow$ [7,13,23,6,24,34,25,12,16]

[7dn6oypcg]

Step4 $\Rightarrow$ Decryption of CipherText

We use Formula $\Rightarrow$ $P = K^{-1}C \mod 36$ First find K^{-1}

$K^{-1} \Rightarrow \frac{1}{|K|} \cdot Adj(K)$ $\Rightarrow$ So Determinant of K

using $\Rightarrow$ $a(ei-fh)+(-b)(di-fg)+c(dh-eg)$

$|K| \Rightarrow \begin{bmatrix}15 & 2 & 2\\3 & 8 & 7\\5 & 18 & 28\end{bmatrix}$

$|K| \Rightarrow 15(8\times28-7\times18)-2((3\times28)-(7\times8)) + 2(3\times18-8\times5)$

$\Rightarrow 15(98)-2(49)+2(14) \Rightarrow 1400$ (Mod 36)

$\Rightarrow 1400$ Mod $36 \Rightarrow 32$ so $|K| \Rightarrow 32$ So no inverse exist can't decrypt

$K^{-1} \Rightarrow (32)^{-1} \Rightarrow (32\times d \equiv 1) \mod 36 \Rightarrow 4 \neq 1$

decryption not possible as MI not exists