02/06/2021

20181CSE0621
Sai Ram. K
6-CSE-10

Part-B

Q.3] **Hill Cipher:**

This Algorithm takes 'm' successive plain text letters and substitutes for them 'm' cipher letters.

- The substitution is determined by 'm' linear equations in which each character is assigned a number or value.

→ **Equations for encryption & Decryption.**

(1) $C = E(P, K) = PK \bmod 26$

(2) $P = E(C, K) = CK^{-1} \bmod 26$.

Here, C → Cipher text ; P → Plain text
K → Key.

→ **Table for hill cipher:**

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

Sai Ram.
20181CSE0621

→ Given, Plain text : Exam
Key : Pass

(i) $Key = \begin{bmatrix} P & A \\ S & S \end{bmatrix} = \begin{bmatrix} 15 & 0 \\ 18 & 18 \end{bmatrix}$

(ii) Writing plain text by splitting into '2×1'

$Plain\ text = \begin{bmatrix} E \\ x \end{bmatrix} \begin{bmatrix} A \\ M \end{bmatrix} = \begin{bmatrix} 4 \\ 23 \end{bmatrix} \begin{bmatrix} 0 \\ 12 \end{bmatrix}$

(iii) We know, $C = K \cdot P \bmod 26$
Hence,

$$C = \begin{bmatrix} 15 & 0 \\ 18 & 18 \end{bmatrix} \times \left(\begin{bmatrix} 4 \\ 23 \end{bmatrix} \begin{bmatrix} 0 \\ 12 \end{bmatrix} \right) \bmod 26$$

$$= \begin{bmatrix} 60 \\ 486 \end{bmatrix} \bmod 26 \cdot \begin{bmatrix} 0 \\ 216 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 8 \\ 18 \end{bmatrix} \cdot \begin{bmatrix} 0 \\ 8 \end{bmatrix}$$

(iv) Mapping with letters $\Rightarrow \begin{bmatrix} 8 \\ 18 \end{bmatrix} \begin{bmatrix} 0 \\ 8 \end{bmatrix} = \begin{bmatrix} i \\ s \end{bmatrix} \begin{bmatrix} a \\ i \end{bmatrix}$

$\therefore C = isai$