Semester: VI Subject: CSS Academic Year: 2023 20 24.

TRANSPOSITION CIPHER:

It is of two types

- * Keyless Transposition Ciphers.
- * Keyed Transposition Ciphers.

KEYLESS TRANSPOSITION CIPHER:

* These are simple transposition ciphers used in past and are keyless.

* There are two methods.

* In the first method, the text is written into a table coloumn by coloumn and then transmitted row by row. It is also called Rail-Fence cipher wherein the plain text is arranged in two lines in a zigzag pattern and the ciphertext is created reading the pattern row by row.

* In the second method, the text is written into the table row and then transmitted coloumn by coloumn. It is coloumnar Transposition Cipher.

Example:

Use the Rail-fence cipher to encrypt the message.
"HAPPY BIRTHDAY TO YOU".
In Rail-Fence cipher, the plaintext is arranged in two lines in a zigzag patterns.

Semester : VI Subject : CSS Academic Year: 2023-2024.

H		P		Y		I		T		D		Y		O		O	
	A		P		B		R		H		A		T		Y		U

The cipher text is created reading the pattern row by row.

Cipher Text :- HPYITDYOOAPBRHATYU.

Example: 2.

Use the keyless transposition cipher to encrypt the message. "We are discovered save yourselfes" in a table of five coloumn.

W	E	A	R	E
D	I	S	C	O
V	E	R	E	D
S	A	V	E	Y
O	U	R	S	E
L	F			

The cipher Text is "WDVSOLEIEAUFASRVRRCEES EODYE".

Semester : VI Subject : CSS Academic Year: 2023- 2024

Keyed Transposition Cipher:

* In this we divide the plaintext into groups of predetermined size, called blocks, and then use a key to permute the characters in each block separately.

* If in a grouping, a block falls short of characters, then add ~~bogus~~ character 'Z' at the end to make the last group as same size as others.

* The key used for encryption and decryption is a permutation key, which shows how the characters are permuted.

Example :
Encrypt the message "ENEMY ATTACKS TONIGHT" using the block size of 5 and the key 31452.

Solution:
Plain Text :- ENEMYATTACKTONIGHT".
Divide plain text into group of block size = 5
as follows : ENEMY, ATTAC, KSTON, IGHTZ.
Arrange the characters in each block as per the given key 31452.

This permulation yielde :

EEMYN , TAALT , TKONS , HITZG .

The cipher text is :

EEMYNTAACTTKONSHITZG .

Keyed Coloumnar Transposition Ciphers:

It combines keyless and keyed Transposition ciphers.

Encryption (or) decryption is done in 3 steps:

Step 1: The text is written row by row into a table.

Step 2: The permutation is done by reordering the coloumns.

Step 3: The new Table is read coloumn by coloumn.

Example:

Encrypt and decrypt the message "ENEMY ATTACKS TONIGHT". with keyed columnar transposition cipher with keyed coloumnar transposition cipher with encryption key "31452" and decryption key "25134".

Solution :

Plain Text : ENEMYATTACKSTONIGHT"

Encrytion key : 31452

Since key size is 5, we write the plaintext row by row in 5 coloumns.

1	2	3	4	5
E	N	E	M	Y
A	T	T	A	C
K	S	T	O	N
I	G	H	T	Z

→

Encryption

3	1	4	5	2
E	E	M	Y	N
T	A	A	C	T
T	K	O	N	S
H	I	T	Z	G

Given encryption key is 31452. So arrange the coloums in key order.

↓

Cipher text: Read coloumn by coloum to get cipher text.

ETTHEAKIMAOTYCNZNTSG

↓

1	2	3	4	5
E	E	M	Y	N
T	A	A	C	T
T	K	O	N	S
H	I	T	Z	G

Since key size is 5, we write the ciphertext coloumn by column into 5 columns.

Decryption.

2	5	1	3	4
E	N	E	M	Y
A	T	T	A	C
K	S	T	O	N
I	G	H	T	Z

- Given decyption key is 25134. So arrange the coloumn in key order.
- Read row by row to get plain Text.

"ENEMYATTACKSTO NIGHTZ."

Semester : VI Subject : CSS Academic Year: 2023-2024.

$$\begin{pmatrix} 08 & 02 \\ 05 & 07 \end{pmatrix} \times \begin{pmatrix} 8 \\ 13 \end{pmatrix} \text{mod } 26 = \begin{pmatrix} 50 \text{ mod } 26 \\ 131 \text{ mod } 26 \end{pmatrix} = \begin{pmatrix} 24 \\ 01 \end{pmatrix} = \begin{matrix} Y \\ B \end{matrix}.$$

$$\begin{pmatrix} 03 & 02 \\ 05 & 07 \end{pmatrix} \times \begin{pmatrix} 0 \\ 13 \end{pmatrix} \text{mod } 26 = \begin{pmatrix} 26 \text{ mod } 26 \\ 91 \text{ mod } 26 \end{pmatrix} = \begin{pmatrix} 0 \\ 13 \end{pmatrix} = \begin{matrix} A \\ N \end{matrix}.$$

$$\begin{pmatrix} 03 & 02 \\ 05 & 07 \end{pmatrix} \times \begin{pmatrix} 08 \\ 13 \end{pmatrix} \text{mod } 26 = \begin{pmatrix} 50 \text{ mod } 26 \\ 131 \text{ mod } 26 \end{pmatrix} = \begin{pmatrix} 24 \\ 01 \end{pmatrix} = \begin{matrix} Y \\ B \end{matrix}.$$

$$\begin{pmatrix} 03 & 02 \\ 05 & 07 \end{pmatrix} \times \begin{pmatrix} 18 \\ 04 \end{pmatrix} \text{mod } 26 = \begin{pmatrix} 62 \text{ mod } 26 \\ 118 \text{ mod } 26 \end{pmatrix} = \begin{pmatrix} 10 \\ 4 \end{pmatrix} = \begin{matrix} K \\ O \end{matrix}$$

$$\begin{pmatrix} 03 & 02 \\ 05 & 07 \end{pmatrix} \times \begin{pmatrix} 02 \\ 20 \end{pmatrix} \text{mod } 26 = \begin{pmatrix} 46 \text{ mod } 26 \\ 150 \text{ mod } 26 \end{pmatrix} = \begin{pmatrix} 20 \\ 20 \end{pmatrix} = \begin{matrix} U \\ U \end{matrix}$$

$$\begin{pmatrix} 03 & 02 \\ 05 & 07 \end{pmatrix} \times \begin{pmatrix} 17 \\ 04 \end{pmatrix} \text{mod } 26 = \begin{pmatrix} 59 \text{ mod } 26 \\ 113 \text{ mod } 26 \end{pmatrix} = \begin{pmatrix} 7 \\ 9 \end{pmatrix} = \begin{matrix} H \\ J \end{matrix}.$$

$$\begin{pmatrix} 03 & 02 \\ 05 & 07 \end{pmatrix} \times \begin{pmatrix} 22 \\ 14 \end{pmatrix} \text{mod } 26 = \begin{pmatrix} 16 \text{ mod } 26 \\ 208 \text{ mod } 26 \end{pmatrix} = \begin{pmatrix} 16 \\ 00 \end{pmatrix} = \begin{matrix} Q \\ A \end{matrix}.$$

$$\begin{pmatrix} 03 & 02 \\ 05 & 07 \end{pmatrix} \times \begin{pmatrix} 17 \\ 11 \end{pmatrix} \text{mod } 26 = \begin{pmatrix} 73 \text{ mod } 26 \\ 162 \text{ mod } 26 \end{pmatrix} = \begin{pmatrix} 21 \\ 6 \end{pmatrix} = \begin{matrix} V \\ G \end{matrix}$$

$$\begin{pmatrix} 03 & 02 \\ 05 & 07 \end{pmatrix} \times \begin{pmatrix} 03 \\ 25 \end{pmatrix} \text{mod } 26 = \begin{pmatrix} 59 \text{ mod } 26 \\ 190 \text{ mod } 26 \end{pmatrix} = \begin{pmatrix} 7 \\ 8 \end{pmatrix} = \begin{matrix} H \\ I \end{matrix}.$$

The result is "WIXHTDYBANYBKOUUHJQAVGHI".