PRIYADARSHINI COLLEGE OF ENGINEERING
(Recognised by A.I.C.T.E., New Delhi & Govt. of Maharashtra, Affiliated to
R.T.M.Nagpur University)Near CRPF Campus, Hingna Road,
Nagpur-440 019, Maharashtra (India)
Phone : 07104 – 236381, 237307, Fax : 07104 – 237681,

Practical No. 5

Aim:- To implement Columnar Cipher transposition Techniques.

Theory:

Given a plain-text message and a numeric key, cipher/de-cipher the given text using Columnar Transposition Cipher. The Columnar Transposition Cipher is a form of transposition cipher just like Rail Fence Cipher. Columnar Transposition involves writing the plaintext out in rows, and then reading the ciphertext off in columns one by one.

Steps to be Included:

In a transposition cipher, the order of the alphabets is re-arranged to obtain the cipher-text.

1. The message is written out in rows of a fixed length, and then read out again column by column, and the columns are chosen in some scrambled order.
2. Width of the rows and the permutation of the columns are usually defined by a keyword.
3. For example, the word HACK is of length 4 (so the rows are of length 4), and the permutation is defined by the alphabetical order of the letters in the keyword. In this case, the order would be "3 1 2 4".
4. Any spare spaces are filled with nulls or left blank or placed by a character (Example: _).
5. Finally, the message is read off in columns, in the order specified by the keyword.

Examples:

Columnar Transposition method
Given : Key- 4312567
Plain text: attack postponed until two am xyz

4	3	1	2	5	6	7
a	t	t	a	c	k	p
o	s	t	p	o	n	e
d	u	n	t	i	l	t
w	o	a	m	x	y	z

Columns : 1 2 3 4 5 6 7
Cipher text: ttnaaptmtsuoaodwcoixknlypetz

Conclusion: Columnar cipher implemented Sucessfully .

Viva Questions:

1. Columnar cipher falls under the category of?
2. Which cipher is formed by applying columnar transposition cipher twice ?