A.I.S.S.M.S
INSTITUTE OF INFORMATION TECHNOLOGY
Kennedy Road, Near R.T.O., Pune - 411 001.

* Laboratory Practice II (Information Security) - Experiment Number - 2.

Name:- Kaustubh Shrikant Kabra.
Class:- Third Year Engineering.
Div:- A
ERP Number:- 38
Department:- Computer Department
College:- AISSMS's IOIT.

Title:-

Transposition Techniques.

Aim:-

Write a Java/C/C++/Python program to perform encryption and decryption using the method of Transposition Techniques.

Objective:-

Perform encryption and decryption using Transposition method.

Theory:-

Transposition technique is an encryption method which is achieved by performing perputation over the plain text. Mapping plain text into cipher text using transposition technique is called Transposition cipher.

1. Rail Fence Transposition
2. Columnar Transposition
3. Improved Columnar Transposition
4. Book cipher/Running Key cipher.

A.I.S.S.M.S
INSTITUTE OF INFORMATION TECHNOLOGY
Kennedy Road, Near R.T.O., Pune - 411 001.

- Column Transposition Technique:-

The columnar transposition cipher is more complex as compared to the rail fence. The steps to obtain cipher text using this technique are as follows:

Algorithm:-

Step 1- The plain text is written in the rectangular matrix of the initially defined size in a row by row pattern.

Step 2- To obtain the cipher text read the text written in a rectangular matrix column by column. But you have to permute the order of column before reading it column by column. The obtained message is the cipher text message.

To understand the columnar transposition let us take example:

Plain Text :- meet tomorrow

Now put the plain text in the rectangle of a predefined size. for our example, the predefined size of the rectangle would be 3×4. As you can see in the image below the plain text

3	1	4	2
M	E	E	T
T	O	M	O
R	R	O	W

← Permuted column order.

Now, to obtain the cipher text we have to read the plain text column by column as the sequence of permuted column order. So, the cipher text obtained by the columnar transposition technique in this example:

Cipher text: Mtreoremotow

Similar to the rail fence cipher, the columnar cipher can be easily broken. The cryptanalyst only has to try few permutation and combination over the order of column to obtain the permuted order of column and the get the original message & more sophisticated technique was required to strengthen the encryption.

Conclusion:-

Thus we applied transposition technique to encrypt and decrypt data.