Bharatiya Vidya Bhavan's
SARDAR PATEL INSTITUTE OF TECHNOLOGY
(Autonomous Institute Affiliated to University of Mumbai)
Munshi Nagar, Andheri (W), Mumbai – 400 058.

Experiment No. 2

Aim – Implement transposition techniques

Problem Definition – To implement all transposition encryption techniques namely Rail Fence, Row-Column and Double Row-Column Ciphering Transposition Techniques. Then, perform ethical hacking on all transportation encryption techniques.

Transportation techniques – There is a class of symmetric encryption cryptosystem where it uses systematic shuffling of plain text characters or bits by altering their positions, called as transportation encryption techniques. The positions of the characters present in the plaintext are rearranged or shifted to form the ciphertext. It makes use of some kind of permutation function to achieve the encryption purpose.

Rail Fence Transposition cipher technique is the simplest transposition cipher technique. In the rail fence cipher, the plain-text is written downwards and diagonally on successive rails of an imaginary fence. When we reach the bottom rail, we traverse upwards moving diagonally, after reaching the top rail, the direction is changed again. Thus the alphabets of the message are written in a zig-zag manner. After each alphabet has been written, the individual rows are combined to obtain the cipher-text.

Columnar Transposition (Row-Column Transposition) involves writing the plaintext out in rows, and then reading the ciphertext off in columns one by one. It works as follows. 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. Width of the rows and the permutation of the columns are usually defined by a keyword.

```
Key:       4 3 1 2 5 6 7
Plaintext: 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
```

Useful Links – The useful links of transportation ciphers namely Rail Fence and Row-Column Ciphering Transposition Techniques are as follows:

1. Rail Fence Technique https://www.youtube.com/watch?v=knE4G8DGLoY
2. Row Column Transposition Ciphering Technique https://www.youtube.com/watch?v=cPQXaYUMOjQ

Note – These videos are not sufficient for theoretical details and students need to refer text and reference books.

Input – There are two tasks of the experiment. The first task of this experiment is to implement all transportation techniques. At the time of implementation, you may visit virtual laboratory designed IIIT Hyderbad and use plain-cipher text pair in the simulation section. Each member of a group has to independently implement all algorithms. Each group members have to decide symmetric keys for respective encryption and decryption and these keys have to be kept secret. Each group member has to also create a few pairs of plan-cipher texts and then handover to a member in the same group without sharing secret key. The second task of this experiment is to implement brute-force attack on all transportation techniques. Each member of a group has to independently implement all brute-force attack on all transportation techniques. Each group member has to take plan-cipher pairs from the member in the same group.

Submission and Output –

1) Part 1 – Implementation of all transportation encryption techniques along with plain-cipher text pairs, key etc in text file. All these should be in one folder named substitution-techniques-<your UID>
2) Part 2 – Implementation brute-force attack on all transportation encryption techniques along with plain-cipher text pairs received from group members and key found. All these should be in one folder named substitution-techniques-attack-<your UID>
3) Part 3 – Plot relative frequency of occurrence of letters (Fig. 2.6 Page 69) as given the textbook "Cryptography and Network Security" by William Stallings. Submit all parts in single zipped file on the CSS Moodle page.