**Course – Cryptography and System Security (CSS)**

|  |  |
| --- | --- |
| **UID** | 2021300038 |
| **Name** | Atharva Gite |
| **Class and Batch** | BE Computer Engineering - Batch VIII |
| **Date** | 5/08/2024 |
| **Lab #** | 2 |
| **Aim** | Implement different transportation techniques. |
| **Problem Definition** | To implement all transportation encryption techniques namely Rail Fence, Row-Column and Double Row-Column Ciphering Transposition Techniques. Then, perform ethical hacking on all transportation encryption techniques. |
| **Theory** | 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. |
| **Output** | **Part 1**  **Rail Cipher:**    **Row Column Cipher:**    **Double Row Column Cipher:**    **Part 2**  **Rail Cipher Brute:**    **Row Column Cipher Attack:**      **Double Row Column Cipher Attack:** |