Pre Lab:-

1. What is a transposition cipher?
A transposition cipher rearranges the positions of the letters in the plaintext according to a certain system, without altering the actual letters themselves.

2. What are the applications of the rail-fence cipher?
The rail-fence cipher is used for simple encryption in educational contexts and for basic obfuscation of text in puzzles or games.

3. Brief description of columnar transposition cipher.
In the columnar transposition cipher, the plaintext is written in rows and then read off in columns based on a key, rearranging the letters to form the ciphertext.

4. Columnar transposition cipher is also known as _____.
A row-column transposition cipher.

5. Difference between substitution and transposition techniques?
Substitution replaces the letters with other letters or symbols, while transposition rearranges the existing letters according to a pattern or key.

VIVA:-

1. What is the Rail Fence transposition technique, and how does it work?
The Rail Fence cipher is a transposition technique where plaintext is written diagonally across multiple rails (rows), then read horizontally to create the ciphertext.

2. Describe the process of encrypting a message using the Rail Fence cipher.
To encrypt, write the message in a zigzag pattern across the specified number of rails and then read the letters row by row, combining them to form the ciphertext.

3. Explain the steps involved in decrypting a message encrypted with the Rail Fence cipher.
To decrypt, determine the number of rails and fill the zigzag pattern row by row, then read the message vertically following the original zigzag path.

4. What are some practical applications of the Rail Fence cipher in modern cryptography?
While not commonly used for strong encryption, the Rail Fence cipher may be used in teaching basic cryptography concepts, games, and simple obfuscation of data.

5. Compare the Rail Fence cipher with other transposition ciphers in terms of security and efficiency.
The Rail Fence cipher is simple and efficient but less secure than other transposition ciphers like the Columnar cipher, which can be more resistant to frequency analysis due to its complex rearrangement of letters.