Pre Lab:-

1. What is the columnar transposition technique, and how does it differ from substitution ciphers?
The columnar transposition cipher rearranges the letters of the plaintext in columns based on a key, while substitution ciphers replace letters with other symbols or letters.

2. Explain the process of encrypting a message using the columnar transposition cipher.
Write the plaintext in rows based on the key length, then rearrange the columns according to the key order and read the ciphertext column by column.

3. How does the key affect the encryption and decryption processes in the columnar transposition cipher?
The key determines the order in which the columns are rearranged during encryption and how they should be reordered during decryption.

4. Describe the steps involved in decrypting a message encrypted with the columnar transposition cipher.
Recreate the column grid using the key, fill the ciphertext column by column, and read off the plaintext row by row.

5. Discuss the role of the column order key in the security of the columnar transposition cipher.
The security relies on the complexity of the key; a longer or randomized key increases the difficulty of guessing the correct column arrangement.

VIVA:-

1. Can you illustrate the encryption and decryption processes of a message using the columnar transposition cipher with a specific key?
For the message "HELLO WORLD" and key "3214", write the text in a grid. Rearrange the columns based on the key order for encryption. To decrypt, fill the columns using the key and read row by row.

2. Compare the security strengths and weaknesses of the columnar transposition cipher with other classical ciphers.
The columnar cipher offers better security than simple substitution ciphers by mixing up letters. However, it is vulnerable to frequency analysis and pattern recognition compared to more complex transposition methods.

3. What are some practical applications of the columnar transposition cipher in modern cryptography?
It's mainly used in educational cryptography exercises, puzzles, or for basic obfuscation. It serves to illustrate fundamental cryptographic principles in training.

4. How does the columnar transposition cipher handle spaces, punctuation, and non-alphabetic characters in the plaintext?
Spaces and punctuation can be included directly in the ciphertext grid or omitted based on implementation, but they may complicate the decryption process.

5. What are some potential attacks or vulnerabilities of the columnar transposition cipher, and how can they be mitigated?
The cipher is vulnerable to frequency analysis and ciphertext-only attacks. Using a longer, randomized key and combining it with other encryption methods can increase security.