Introduction

Classical ciphers are foundation of modern cryptography. offering simplest yet effective way to secure info. Columnar & Rail fence cipher fall under the category of transposition ciphers, where the positions of characters are shifted according to certain system but characters remain unchanged.

Columnar Transposition Cipher

In this technique, plaintext is written in rows under a key, & columns are read in a specified order to form cipher text. The security depends on the keys complexity but its relatively easy to break with enough ciphertext.

Rail fence

It arranges the plaintext in a zigzag pattern across multiple lines, or "rails". The cipher text is formed by reading sequentically from each rail. Its simpler but less secure than columnar cipher.

Conclusion:

Both ciphers highlight the basic principles of transposition encryption. They are historically significant but not secure by modern standards, offering insights into the need of more complex cryptographic methods.