Name	Atharva Tamhankar
UID no.	2022300127
Experiment No.	2

AIM:	**Experiment Report: Implementation of Transposition Techniques**
Program 1	
OBJECTIVE:	This experiment aimed to implement and understand three classical cryptographic transposition techniques: Rail Fence Cipher, Columnar Transposition Cipher, and Double Transposition Cipher. Each algorithm was implemented with both encryption and decryption functionality in a menu-driven C++ program.
IMPLEMENTATION OVERVIEW:	**1. Rail Fence Cipher** The Rail Fence cipher arranges plaintext characters in a zigzag pattern across multiple rails and reads them row by row. The implementation uses a vector of strings to represent rails and employs a direction flag to simulate the zigzag movement. The decryption process first calculates the length of each rail, fills them with ciphertext, and then reads back in the zigzag pattern. **Key Learning**: The algorithm's complexity lies in correctly simulating the zigzag pattern and calculating rail lengths during decryption. **2. Columnar Transposition Cipher** This cipher arranges plaintext in a matrix where columns are defined by a keyword. The matrix is read column by column in alphabetical order of the key characters. The implementation creates a 2D matrix, fills it row by row, sorts the key to determine column reading order, and extracts ciphertext column by column. **Key Learning**: Proper handling of key sorting and matrix padding is

	crucial for correct encryption/decryption. **3. Double Transposition Cipher** This technique applies columnar transposition twice using two different keys, significantly increasing security. The implementation simply chains two columnar transposition operations, with decryption performed in reverse order. **Key Learning**: Layered encryption techniques provide exponentially increased security compared to single-layer approaches.
LEARNING OUTCOME:	# Learning Outcomes 1. **Permutation vs Substitution**: Transposition ciphers preserve character frequency but scramble positions, making them vulnerable to specific cryptanalytic techniques. 2. **Key Management**: The security of key-based ciphers heavily depends on key secrecy and randomness. 3. **Implementation Complexity**: While conceptually simple, correct implementation requires careful attention to edge cases, matrix operations, and algorithm flow. 4. **Historical Context**: These classical ciphers demonstrate foundational cryptographic principles that evolved into modern encryption standards.
CONCLUSION:	This experiment provided hands-on experience with classical cryptographic techniques, highlighting the evolution from simple character rearrangement to complex modern encryption. The implementation reinforced understanding of algorithm design, matrix operations, and the importance of systematic testing with various input scenarios. While these ciphers are cryptographically weak by modern standards, they serve as excellent educational tools for understanding fundamental encryption principles.