HELP FILE

Aim: The Idea was to create a cipher that uses the concept of transposition and shifting together. In the technique shifting is followed by substitution.

Problem Definition: The techniques of transposition available nowadays are easily crack able by brute force. Hence in order to eliminate this and increase the complexity the technique of shifting has been incorporated in which cipher is shifted by some random numbers followed by matrix transposition. This is useful for short length ciphers or short messages.

Inputs: Small messages presentable in matrix form.

Steps:

1. User should enter rows and columns according to his designed matrix
2. The user would then be required to enter the input in comma separated manner
3. The user should then enter some row number of random numbers through which each row should be shifted
4. Then user should enter column number of random numbers between the number of columns
5. Click on the encrypt message to see the procedure
6. Similarly click on the decryption to see the decryption process from bottom to top manner.

Observations:

- Works for any length m*n matrix
- Difficult to decrypt as random numbers are difficult to guess
- Good for small messages

Results: A combination of shift and transposition method which is secure and involves very complicated steps has been created. This method is difficult to crack and therefore, it is very useful to encrypt small messages.