CEF 350: SECURITY AND CRYPTOSYSTEMS

Name: Djeutio Quoimon Anderson Roy

Matricule: FE21A169

Implementation of Columnar Transposition cipher

The columnar transposition algorithm is a type of encryption technique that involves rearranging the letters of a message according to a specific pattern, which is determined by a keyword or phrase. Here's a brief explanation of how it works:

Algorithm

1. Firstly, the message entered, then the key is taken in 2 parts:
   - The number of columns
   - The order of the columns
2. Each character of the message is gotten and stored in a matrix according to number of columns i.e. row by column
3. A new message matrix is then sorted in the order in which the user wishes to encrypt his text
4. Then, the message is read column by column based on the order of the user
5. This same process is used to decrypt the message. The difference is that the matrix is sorted according to rows i.e. column by row
6. Then the message is read row by row.

Working principle