SSN College of Engineering,
Department of Computer Science and Engineering
CS6711 Security Laboratory

Exercise 3a:

To implement the transposition techniques: Rail fence Cipher

Programming Language: Java

Hints:

Encryption Procedure for Rail fence Cipher:

1. Read the plain text message
2. Read the key value (The key for the rail fence cipher is just the number of rails / levels)
3. Write the letters of the plaintext diagonally down to the right until you reach the number of rows specified by the key.
    - Then bounce back up diagonally until you hit the first row again. This continues until the end of the plaintext.
4. To generate the cipher text, read off along the rows one by one.
5. Display the cipher text.

Decryption Procedure for Rail fence Cipher:

1. Use the cipher text as input and number of rails as key value
2. Break up the cipher text letters into equal groups for each rail.
3. To retrieve the plaintext text from cipher text, read off the message vertically.
4. Display the plain text.

Exercise 3b:

To implement the transposition techniques: Row & Column Ciphers

Programming Language: Java

Hints:

Encryption Procedure for Row & Column Cipher:

1. Read the plain text message
2. Write the plaintext in row by row forming a matrix / grid of *m X n.*
3. Read the key value (a number with permuted digits ranging from*1* to number of columns in the plaintext matrix)
4. Use the key as column headers
5. Generate the cipher text with respect to the order of the column headers.
6. Display the cipher text.

Decryption Procedure for Row & Column Cipher:

1. Use the cipher text as input
2. The number of rows and columns of the cipher text matrix be now *n X m*
3. Write the cipher text row by row in *n* rows
4. Let the row headers be the permuted key values of 1 to n
    - If encryption key is 4 3 1 2 5 6 7
    - Decryption key will be 3 4 2 1 5 6 7
5. Take the letters in the order of key from the first column to retrieve the plain text. Repeat extracting letters in the other columns according to the key.
6. Display the plain text.