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

Exercise 1:

To implement the substitution techniques: Caesar Cipher and Playfair Cipher

Programming Language: Java

Hints:

Encryption Procedure for Caesar Cipher:

1. Read the plain text message
2. Read the key value (displacement)
3. To generate the cipher text , replace each letter of plaintext by a letter at the position specified by the key value down the alphabetical stream.
4. Display the cipher text.

Decryption Procedure for Caesar Cipher:

1. Use the cipher text as input
2. Use the same key value as displacement
3. To retrieve the plaintext text from cipher text, replace a letter of cipher text by the letter at the position specified by the key value in the reverse alphabetical stream.
4. Display the plain text.

Encryption Procedure for Playfair Cipher:

1. Read the plain text message
2. Read the key value (a string without any repetition letters)
3. Construct a 5 X 5 matrix and fill in the key text in row wise manner.
4. Fill in the remaining cells of the matrix with the rest of the alphabets sans the letters of the key.
5. Split the plain text into two letter words without repetition.
6. If a pair has a repeated letter, insert filler like 'X'
7. If both letters fall in the same row, replace each with letter to right (wrapping back to start from end)
8. If both letters fall in the same column, replace each with the letter below it (wrapping to top from bottom)
9. Otherwise each letter is replaced by the letter in the same row and in the column of the other letter of the pair
10. Display the cipher text.

Decryption Procedure for Playfair Cipher:

1. Use the cipher text as input
2. Use the same key value
3. To retrieve the plaintext text from cipher text, split the plain text into two letter words without repetition.
4. Repeat the steps 7 to 9 of encryption to generate the plaintext
5. Display the plain text.