Lab Report

CSE436, Computer and Network Security

Name:Mohammed Said Mohammed Said ID:15P6048

Assignment No: (1) Experiment Title: Implementing Ciphers

Date: 10 /17 /2019

Caesar Function:

This function takes two parameters the first one is the plain text and the second one is the key.

First, I change all of the plain text in the lower case and without spaces then I iterate on the plain text to get the index of the letter then I add the key to that index, then I put the encrypted message in empty variable.

Hill Function:

This function takes as input the plain text and the key and creates an integer matrix for the text for the indices of each letter and it also depends on the dimension of the key matrix 2x2 or 3x3 and then I multiply the key matrix with the text matrix with matrix multiplication and calculate the size of the result matrix and put the result of the multiplication in it and then translate the integer results to letter based on the indices of the letters.

Play Fair Function:

This function takes two parameters the first one is the plain text and the second one is the key. First, I replace any 'j' with 'I' in the plain text, then I check the size of the plain text if it odd number I add 'x' to the plain text and I also check if there is any two consecutive letters have the same value, so I will add 'x' between them.

Second, I make an empty array to put the key in without repeated letters then I add the rest of the alphabet without the letters that already exists in the key.

Third, I made a function that gets me the position of the letter in the matrix, then I have three condition

The first one is to check if position of the two consecutive letters are in the same row then I will replace each letter with one to the right and if the letter is in the most right it will take the first letter in the row in other words it will move in a circular way. The second condition is that the position of letters is in the same column so they will be replaced with the letter under them and also will move in a circular way. The last condition is that the position of the letters are not in the same row or column, so I will replace them with the one that meets in the same row and column.

Vigenere Function:

This function takes three parameters the first one is the plain text, the second one is the key, and the third one is for the mode if it is true so will work in auto mode, if it is false so will work in the repetitive mode. First, I change all of the plain text in the lower case and without spaces then if we are in the repetitive mode I repeat the key until it is the same size of the plain text, then I iterate on the plain text to get the index of the letter then I add the key to that index, then I put the encrypted message in empty variable.

Vernam Function:

This function is same as Vigenere , the difference is that the key is generated randomly.