****

**Assignment Answer**

**CSE 436, Computer and Networks Security**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name: | Marina Gamal Ibrahim | ID: | 15P6047 |  |

Assignment No: ( 1 )

Date: 17 / 10 / 2019

………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………

I implemented the 5 ciphers using python programming language.  
The first Cipher is the Caesar Cipher, the Caesar function takes the Plain text and the key and removes the white spaces for the text and using the function rotate which I implemented I get the ASCII code for each letter and add the key on it and subtract the ASCII of the first letter A and then apply the mod 26 and add the ASCII of the letter A in the end to enable the rotation. And in the end pass this ASCII code to another built in function that returns the corresponding letter.

The second Cipher is the Playfair cipher which also takes the Plain text and the string key and removes all the spaces and replaces each J with an I, and then it divides the text to pairs of 2 and checks if there is a letter repeated in the pair I insert ‘X’ in the middle and if there a single letter in the end I also insert ‘X’. Next I create the 5x5 matrix from the key which does not have any repeated characters and start matching the text to the matrix and extracting the ciphered text based on the 3 rules below:

1. If both letters fall in the same row, replace each with letter to right (wrapping back to start from end.)
2. If both letters fall in the same column, replace each with the letter below it (wrapping to top from bottom.)
3. Otherwise, each letter is replaced by the letter in the same row and in the column of the other letter of the pair.

The Third Cipher is the Hill cipher, its function also takes the Plain text and the key and creates a matrix for the text based on the corresponding index to each letter based on the length if the hill matrix (key) whether it is 2x2 or 3x3 and then I multiply the Key matrix with the text matrix and then take the final matrix which contains the indexes of the ciphered text and change each to its corresponding letter.

The fourth Cipher is the Vigenere cipher, which again takes the Plain text and the key together with a third argument which is the mode, True for the auto mode which takes the key and concatenate the plain text after it until the length if the key becomes equal to the length of the text, or False for the repetitive mode which repeats the key until the length if the key becomes equal to the length of the text. After preparing the key I get the index of each letter in the key and add it on the corresponding letter in the text using the same rotate function used in the Caesar cipher which gets the corresponding ciphered letter and handles the rotation using the mod operation.  
  
Finally, the fifth Cipher, Vernam cipher, this cipher also takes the Plain text and the key which was given to us in the assignment pdf and which is equal in length to the input plain text and again removes all the spaces and uses the rotate function, after adding the index of each letter in the key to the corresponding letter in the text, which returns the ciphered text after handling the rotation. In general Vernam cipher uses completely random keys that are the same length of the text but here we take as an input the key which we will use to test with.  
  
Attached is the .py containing all the function and the main and the .exe in which the user enters the plain text and key for each cipher and gets the ciphered text. Also the text files for the outputs for each cipher based on the input files are attached.