Lab Assignment-1
Classical Encryption Techniques
Due: 27th January, 2019
Total Mark: 30

Problem 1 (Total Mark=10)

Write a program in Python that implements the Vigenere polyalphabetic cipher for English text. Your cipher should distinguish lowercase and uppercase letters (i.e. a letter should be encrypted differently based on if it is uppercase or lowercase). In your cipher, the encryption key, plaintext and the ciphertext should be composed of lowercase and uppercase letters. Your program should read the input from a file called ‘input.txt’ and write to a file called ‘output.txt’. It should read the encryption key from a file called ‘key.txt’. Your program should perform the following operations:

(a) Remove unnecessary characters except A - Z, a - z from the English text in ‘input.txt’.

(b) Encode the message using the keyphrase in ‘key.txt’.

(c) Convert the ciphertext produced in step(b) into a message consists of words with 5 characters and write it into ‘output.txt’.

(d) Decode the ciphertext in ‘output.txt’ into the original message.

Problem 2 (Total Mark = 20)

Now take a ciphertext file ‘output.txt’ generated from Problem 1 and try to generate the original message without using the encryption key in ‘key.txt’. Your program should perform the following operations:

(a) Print the predicted length of the key. The output may contain more than one value.

(b) The original message or the predicted message based on our algorithm.

(c) Execute the program on each of the ciphertext generated from Problem 1 and compare how close your result to the original message and the key.

(d) Mark on explanation.

Hint: Encrypt an arbitrary large message in Problem 1 to generate a ciphertext that is sufficiently large enough to help you to predict the original message.