

## **Assignment: 1- Caesar Cipher**

**Date of Assignment: 08 August 2017**

**Date of Submission: 14 August 2017 Time: 5:30 pm**

$$e(x) = (x + k) \pmod{26}$$

1. Accept the value of "k" i.e the amount to shift (for example 3 as discussed in the class) as an input.
2. Read in a message from a file. The message will consist of one or more lines.
3. Convert the message characters as ASCII code.
4. Encode each letter by shifting it the right by "k". Discard all the punctuation marks, digits, blanks, and anything else from the input string.
5. Print the final encoded message in blocks of five letters and ten blocks per line. The last line may be shorter than five blocks, and the last block may be shorter than five letters.

## **Cryptanalysis**

1. Write a program for the cryptanalysis of the same without knowing the value of "k".
2. Your program should take one by one value of "k" and store the output as step 5.