CSCI 2916 Lab 3 – Week 3

Lab: Encryption and Decryption – Caesar Cipher

In cryptography, a **Caesar cipher**, also known as **Caesar's cipher**, the **shift cipher**, **Caesar's code** or **Caesar shift**, is one of the simplest and most widely known encryption techniques. It is a type of substitution cipher in which each letter in the plaintext is replaced by a letter some fixed number of positions down the alphabet. For example, with a right shift of 2, A would be replaced with C. With a left shift of 3, D would be replaced by A, E would become B, and so on. The method is named after Julius Caesar, who used it in his private correspondence.

The encryption step performed by a Caesar cipher is often incorporated as part of more complex schemes, such as the Vigenère cipher, and still has modern application in the ROT13 system. As with all single-alphabet substitution ciphers, the Caesar cipher is easily broken and in modern practice offers essentially no communication security.

So, today we will be writing 1 program:

1. The first program will encrypt a message entered by the user using a key which will generate the cipher. You will ask the user to enter a message he/she would like to encrypt and then ask them for a key (basically how many shifts) and the program should output the encrypted message. For example, (user input is in *italics*, computer prompts are in **bold**):
   Enter a message to Encrypt:
   Zebras are extremely Great!
   Key:
   3
   Encrypted Message = Cheudv duh hawuhphob Juhdw!

Note: Ensure if a space is entered as in between Zebras, are, extremely, and Great! that the space remains in the encryption. Also, the ! or any other special character should stay in the encryption.

Extra Credit: Create a program encrypting with the Vigenère cipher.

BEFORE YOU START WRITING CODE . . . On the back of this paper, sketch out:

- How will you calculate the characters (shifting to next letter (based on the key)
- How will you deal with letters lower in the alphabet. For example, if you encrypt the letter Z how will you rotate back to A (based on the key entered)?

Guidelines for a good program:

- The program works, following the dialog and rules above.
- The code is clear and understandable:
  - Properly indented
  - Representative variable names
  - Blank lines separate logical sections of code
  - Appropriate comments included
  - Preamble documentation is included
  - Review program assignment rubric

References: https://www.techopedia.com/definition/6311/caesar-cipher
https://en.wikipedia.org/wiki/Vigenère_cipher