CECS 564
Computer Project #1
Binary Vigenere Crypto System

The purpose of this project is to give students some experience with Vigenere crypto algorithm of binary data. You are to implement in matlab, C, C++, C#, or java routines to encrypt, decrypt, and attack the following crypto:

$$Y_i = (X_i + k_{i\%m}) \% 256$$
$$X_i = (Y_i - k_{i\%m}) \% 256$$

Where $\{Xi ; i = 0 : n\text{-}1 \}$ is the input plain n bytes sequence, $\{k_i ; i = 0 : m\text{-}1\}$ is the keyword of length m characters, and $\{Yi; i = 0 : n\text{-}1\}$ is the output cipher n byte sequence.

To test your routines you need to encrypt a *.jpg* image file and decrypt the resulting file. Exchange the encrypted files with your lab partner, and then run your attack routine to find out your partner's secret keyword and decrypt his/her encrypted file.

Your report should include answers to the following questions:

1. What is the effect of Vigenere encryption on the data statistics such as mode, mean, median, standard deviation and entropy?
2. What is the effect of cascading Vigenere crypto system on the security of the system?

Due: 02/16/2017