X. Xiao

CSE 545: Software Security
Assignment #2

For all the coding problems, please upload your source code and take a screen shot on inputs and outputs of your program. Also please provide instructions on how to run your code, and write a PDF to provide answers and the steps on how you use the outputs from your code to solve the problems. You can use any programming language you like, but we suggest you use Java, C++ and Python.

1. Please implement a Caesar Cipher for characters from 'A' to 'Z' (20 points).

2. Please implement a statistical attack for Caesar Cipher by computing Correlation: $\varphi(i) | i = [0,25]$ based on slides L7 pages 16-19. Use your implemented attack to infer the key and the plain text for the following cipher texts (30 points):
   a. XTKYBFWJXJHZWNYD
   b. KCECMKS

3. Please implement a variant of Vigenère cipher (20 points):
   a. Key length can be from 1-3
   b. Each character in the key must be upper case letters (i.e., 'A'-'Z')
   c. Each character in the cipher text can be any character from the ASCII table (https://en.wikipedia.org/wiki/ASCII)

4. Please implement an exhaustive search algorithm to attack a simpler version of the Vigenère cipher built at question 3 (key length can be 1-3, and cipher text must use upper case letters). Use your implemented attack to infer the key for the following plaintext and cipher text pairs. You need to provide **screenshots to show the input and the output of your code**, and **an output text file to show the keys and the total number of keys** in your algorithm search. (30 points):

Plain Text	**Cipher Text**
ARIZONASTATEUNIVERSITY	EUCDRHEVNEWYYQCZHLWLNC
COMPUTERSCIENCE	GRGTXNIUMGLYRFY