SY201

Name(s): ____________________

Alpha(s): ____________________

Assignment Type:	Lab	Collaboration Policy:	Default
Assignment Title:	Lab 7	Submit Project Name:	lab7
Electronic submission due: _________ Paper submission due: NO PAPER SUBMISSION Submission instructions: http://courses.cyber.usna.edu/SY201/calendar.php?load=policy			

1. Assignment Overview

In this assignment you will build a program that performs encryption and decryption

2. Background Research

a. The Caesar cipher is one of the most well- known encryption techniques. Also known as the shift cipher, it is a substitution cipher in which each letter in the original message (plaintext) is replaced by a different letter which is a fixed number of places down/up the alphabet. Review the Caesar shift that you learned about last year (https://www.usna.edu/CyberDept/sy110/calendar.php?type=class&event=24)

b. Consider the plaintext alphabet being a single string consisting of uppercase English letters as below, shown with each letter's associated index, e.g., M's index is 13.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	13	13	14	15	16	17	18	19	20	21	22	23	24	25

c. Then, using a shift of 23, the cipher alphabet is

X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

d. Using the cipher alphabet, the string "LAZY" is encrypted as:

- The "L" is found at index 11 in the plaintext alphabet. The letter in the shifted alphabet is I
- The "A" is found at index 0 in the plaintext alphabet. The letter in the shifted alphabet is X
- The "Z" is found at index 25 in the plaintext alphabet. The letter in the shifted alphabet is W
- The "Y" is found at index 24 in the plaintext alphabet. The letter in the shifted alphabet is V

Thus, the string "LAZY" becomes the string "IXWV"

e. You will also need to understand the Vigenere cipher as well (https://www.usna.edu/CyberDept/sy110/calendar.php?type=class&event=24). The demo is extremely helpful in understanding how the encryption process works (https://www.usna.edu/CyberDept/sy110/calendar.php?key=c4a8a41190f468461a1c06317bf2701f23afcbb8&type=resources&event=27).

3. Specification - modify the file lab7.py to add the following functions and **includes comments adjacent to each function that describe the function's purpose and use**:

   a. Write your alpha and section number in a comment at the top of your program

   b. Write any sources of discussion/collaboration in a comment at the top of your program

   c. Write a function encrypt_caesar that:
      i. Takes two arguments: (1) a string to encrypt and (2) an integer (key)
      ii. Assume: the string is all uppercase
      iii. Assume: the key is between 0-25
      iv. Note: only letters should be encrypted, all other characters should be unmodified
      v. Returns the result of encrypting the first argument using the Caesar cipher with the second argument as the key

   d. Write a function decrypt_caesar that:
      i. Takes two arguments: (1) a string to decrypt and (2) an integer (key)
      ii. Follows the same rules as encrypt_caesar
      iii. Returns the result of decrypting the first argument using the Caesar cipher with the second argument as the key

   e. Write a function count_freq that:
      i. Takes one argument: (1) a string
      ii. Returns a dictionary where the keys are the strings 'A' through 'Z' and the values are the number of occurrences of those letters in the argument

   f. Write a function encrypt_vigenere that:
      i. Takes two arguments: (1) a string to encrypt and (2) a string (key)
      ii. Assume: the string is all uppercase
      iii. Note: only letters should be encrypted, all other characters should be unmodified
      iv. Returns the result of encrypting the first argument using the Vigenere cipher with the second argument as the key

   g. Write a function decrypt_vigenere that:
      i. Takes two arguments: (1) a string to encrypt and (2) a string (key)
      ii. Follows the same rules as encrypt_vigenere
      iii. Returns the result of decrypting the first argument using the Vigenere cipher with the second argument as the key

h. Write a function named main that (in this order):

  i. Takes no arguments

  ii. This function should run FOREVER unless the user takes advantage of the below "(3) Quit" option (or the program is forcibly quit)

  iii. Precisely prints out the following:

```
Options
(1) Caesar Cipher
(2) Vigenere Cipher
(3) Quit
```

  iv. Prompts the user for a numerical selection using "Selection: "

  v. If the user chooses option three (user input: 3), your program should ask for no additional input and generate no additional output

  vi. If the user chooses option one (user input: 1), your program should:

    1. Precisely print out the following:

```
Options
(1) Encrypt
(2) Decrypt
(3) Frequency Analysis
```

    2. Prompt the user for a numerical selection using "Selection: "

    3. If the user chooses option one (user input: 1), your program should:

      a. Prompt the user for some plaintext using "Plaintext: "

      b. Prompt the user for a key using "Key: "

      c. Encrypt the plaintext

      d. Print out the result as "Ciphertext: [CIPHERTEXT]"

    4. If the user chooses option two (user input: 2), your program should:

      a. Prompt the user for some ciphertext using "Ciphertext: "

      b. Prompt the user for a key using "Key: "

      c. Decrypt the ciphertext

      d. Print out the result as "Plaintext: [PLAINTEXT]"

    5. If the user chooses option three (user input: 3), your program should:

      a. Prompt the user for some ciphertext using "Ciphertext: "

      b. Print out "The most likely key is [KEY] which yields [PLAINTEXT]" where plaintext is the result of decrypting the ciphertext with the most likely key

  vii. If the user chooses an option two (user input: 2), your program should:

    1. Precisely print out the following:

```
Options
(1) Encrypt
(2) Decrypt
```

    2. Prompt the user for a numerical selection using "Selection: "

    3. If the user chooses option one (user input: 1), your program should:

      a. Prompt the user for some plaintext using "Plaintext: "

      b. Prompt the user for a key using "Key: "

   c. Encrypt the plaintext
   d. Print out the result as "Ciphertext: [CIPHERTEXT]"

4. If the user chooses option two (user input: 2), your program should:
   a. Prompt the user for some plaintext using "Ciphertext: "
   b. Prompt the user for a key using "Key: "
   c. Decrypt the ciphertext
   d. Print out the result as "Plaintext: [PLAINTEXT]"