**EXPERT ENCRYPTION**

***Description***

My goal is to create a program that runs encryption/decryption of various entries, like the cipher project earlier in the year. This time around, I want the program to run multiple different ciphers, including much more advanced ones, like the Vigenere cipher and the one-time pad (which hide letter frequencies). These ciphers require keys while encrypting/decrypting that change your phrase in different ways which make them harder to crack (see Cipher section below)

The program will start at a menu allowing you to choose whether you want to encrypt, decrypt, or quit. Choosing one of the first two, the program will then ask you which cipher you’d like to use from a list of ciphers. Any ciphers requiring a key will ask you to enter the phrase to be encrypted or decrypted, and the key used to do so. Any other ciphers will just ask for your phrase/letter jumble. The program would then show you the results and send you back to the main menu (or ask you if you’d like to go again). If time allows, I would like to make this into a GUI for ease of use.

**Ciphers to be used:**

* Vigenere cipher: Uses a sequence of Caesar ciphers based on a keyword to encrypt your message, each with different shift values. The keyword must be shorter than the plaintext (and the program will ensure that it is), and is repeated until the number of letters in the keyword matches the plaintext. Example: plaintext = helloworld, key = code, the key to enter into the program would = codecodeco
* One time pad: Much like the Vigenere, the OTP uses modular addition. In this case, the user enters plaintext and a random key of equal length. With mod 26 addition (or subtraction in the case of decryption), the program generates the coded message. If done correctly, this type of code is virtually unbreakable since the coded message could easily translate to many different things. The program will allow entry of a random key, or generate one for the user (and tell him/her what it is)

**Possible other ciphers:**

* Caesar cipher: Alphabet is shifted x amount, user enters shift number and phrase
* Morse code: dashes and dots, just for fun.
* Columnar transposition: phrase written out in rows, determined by number of letters in key word, key word reads columns off by alphabetic order of letters in key word
* A1Z26 cipher: numbers equal letter position
* Atbash: letters = alphabet in reverse
* Combined: A1Z26, atbash, then Caesar cipher in one
* Hex, binary, or octal: looks like jibberish to anyone who doesn’t know it

***Users***

Anyone who needs phrases encoded or decoded

People who want to have fun

***Problem to solve***

Easily encrypt and decrypt messages rather than doing it manually by hand/researching how to encrypt/decrypt them

***Ways to accomplish final product***

The first way I would write it would be just using functions or classes to define the various ciphers, as well as the different menu options. The main function would be in a while loop until keepGoing = False, which only happens when the user selects the quit option.

The program will make sure the user can only enter certain menu choices, or else it will ask what they want to do again. Each cipher would also be written in a way that the user can only achieve one result (i.e. key must be correct, A1Z26 numbers and morse code must have spaces between each letter, can’t enter wrong symbols for each particular cipher). Most ciphers will also have a check for spaces and case.

The alternate way with less clutter would be to write each cipher in separate files and transfer them in as classes. While easier to read, this way is more confusing to me at the moment.

If I have enough time, I would like to make this as a GUI, where the initial options would be posed as buttons. Once a button is clicked, the GUI would change and ask the user which cipher to use (again by selecting a button, possibly a radio dial then they hit OK button). The GUI will present a space to enter the user’s plaintext/ciphertext, a key (if needed), and a read-only results box. Buttons to “translate”, “reset”, “main menu”, and “quit” will be at the bottom.

Sample Script

*Please choose what you would like to do:*

1. *Encode*
2. *Decode*
3. *Quit*

1

*Please choose the cipher/converter you would like to use:*

1. Vigenere
2. One Time Pad
3. Caesar
4. Morse Code
5. Binary
6. Octal
7. Hex
8. Back to Main Menu

1

*First please enter your plaintext:*

This is for my final project

*Now enter your key:*

Python

*Here is the endoded ciphertext:*

*XXXXXXXXXXXXXXXXXXXXXX*

*Would you like to encode/decode something else? (y/n)*

N

*OK! Have fun doing top secret shenanigans.*

**GUI**

Quit

Menu

Reset

Encode

Enter plaintext \*entry\*

CIPHER 1

Enter Key \*entry box\*

Results \*Read-only\*

btnCipher 2

btnCipher 3

btnCipher 4

btnBack to menu

btnCipher 1

btnQuit

btnDecode

btnEncode

lblENCRYPTION!