Inquiry Question

Could you use your Python skills to encrypt and decrypt messages using the Roman Caesar cipher?

Name: _____ Date: _____

General Instructions

The Caesar cipher is an encryption technique which can transform plain, readable text into jumbled and encrypted cipher text. The method is named after the Roman emperor Julius Caesar, who used it to communicate privately.

To encrypt a message, shift each letter to a different letter in the alphabet. The shift amount is called the “secret key”, and is how we know how to decrypt the ciphertext. For example, if we use a shift of 2, then A would be replaced by C, and D would be replaced by F.

Using lists, strings, input, output, loops, functions, and other skills you have learned, write your own implementation of the Caesar cipher encryption tool. Your program should be able to encrypt and decrypt messages using a secret key (shift value).

Materials you'll need:

- Pencil
- Computer

Project submission:

Submit the completed pages of this project as well as the .py code file for your encryption program.

Design Specifications

- ❑ Ask the user if they would like to encrypt or decrypt a message
- ❑ If the user enters invalid input, continue prompting them until they enter a valid mode
- ❑ Allow the user to specify a secret key (shift) value
- ❑ Accept both positive and negative secret keys, as well as secret keys greater than 26 (number of letters in the alphabet) (*Hint: modulo operator*)
- ❑ Correctly encrypt a string of plain text, and output the cipher text
- ❑ Correctly decrypt a string of cipher text, and output the plain text
- ❑ Symbols and spaces should not be encrypted or decrypted but should remain in the message
- ❑ When encrypting and decrypting, always output the message in all capital letters
- ❑ You must create and use at least 3 functions

Bonus Options

- ❑ Add the ability to encrypt or decrypt an entire text file

- ❏ Generate a random shift value, and output this secret key to the user when encrypting messages

- ❏ [HARD] Write program mode which will "break" the cipher and decrypt a message without being given the secret key.

Hints and Resources

Here is a short example of how your program might look when you run it in the console.

```
>>> %Run caesar_cipher.py
 Would you like to encrypt (E) or decrypt (D)? G
 Invalid mode, please enter 'E' to encrypt, or 'D' to decrypt.
 Would you like to encrypt (E) or decrypt (D)? E
 Enter your message to encrypt: We attack at dawn!
 You entered: 'WE ATTACK AT DAWN!'
 Enter a secret key: -7
 Encryption complete
 The cipher text is 'PX TMMTVD TM WTPG!'
 All done, exiting...
```

Hint: you can determine the index of an element within a list using the **index()** method.

For example:

ALPHABET = "ABCDEFGHIJKLMNOPQRSTUVWXYZ"

print(ALPHABET.index("C"))

Below is some sample input and output so you can test the accuracy of your program.

PLAIN TEXT

THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG

CIPHER TEXT (secret key = 2)

VJG SWKEM DTQYP HQZ LWORU QXGT VJG NCBA FQI

PLAIN TEXT

WE ATTACK AT DAWN!

CIPHER TEXT (secret key = -7)

PX TMMTVD TM WTPG!

PLAIN TEXT

AS LONG AS WE DON'T HAVE MAGIC, THEY WILL NEVER TREAT US WITH RESPECT. THEY NEED TO KNOW WE CAN HIT THEM BACK. IF THEY BURN OUR HOMES, WE BURN THEIRS, TOO.

CIPHER TEXT (secret key = 14)

OG ZCBU OG KS RCB'H VOJS AOUWQ, HVSM KWZZ BSJSF HFSOH IG KWHV FSGDSQH. HVSM BSSR HC YBCK KS QOB VWH HVSA POQY. WT HVSM PIFB CIF VCASG, KS PIFB HVSWFG, HCC.

Questions

Is the Caesar cipher still used for web encryption? Why or why not?

Did you run into any difficulties while coding this project? How did you solve any problems?

Can the Caesar cipher be broken? If so, how would you go about trying to decrypt a message without knowing the secret key?

Can you think of any way to make the Caesar cipher more secure? How would you add this to your program?