Computer Science I — Bill Griffith PhD

HW5 12 pts — **Due 11:59 PM Sunday October 6**

Vigenère Cipher

The Vigenère Cipher is a polyalphabetic substitution cipher. The method was originally described by Giovan Battista Bellaso in his 1553 book La cifra del. Sig. Giovan Battista Bellaso; however, the scheme was later misattributed to Blaise de Vigenère in the 19th century, and is now widely known as the Vigenère cipher. The Vigenère Cipher was considered le chiffre ind hiffrable (French for the unbreakable cipher) for 300 years, until in 1863 Friedrich Kasiski published a successful attack on the Vigenère cipher. Charles Babbage had, however, already developed the same test in 1854.

The Algorithm: The 'key' for a vigenere cipher is a key word or phrase. e.g. 'PYTHONISEXTRA'. The Vigenere Cipher uses the following tableau (the 'tabula recta') to encipher the plaintext:

```
    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
    -----------------------------------------------------
A   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
B   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 A
C   C D E F G H I J K L M N O P Q R S T U V W X Y Z A B
D   D E F G H I J K L M N O P Q R S T U V W X Y Z A B C
E   E F G H I J K L M N O P Q R S T U V W X Y Z A B C D
F   F G H I J K L M N O P Q R S T U V W X Y Z A B C D E
G   G H I J K L M N O P Q R S T U V W X Y Z A B C D E F
H   H I J K L M N O P Q R S T U V W X Y Z A B C D E F G
I   I J K L M N O P Q R S T U V W X Y Z A B C D E F G H
J   J K L M N O P Q R S T U V W X Y Z A B C D E F G H I
K   K L M N O P Q R S T U V W X Y Z A B C D E F G H I J
L   L M N O P Q R S T U V W X Y Z A B C D E F G H I J K
M   M N O P Q R S T U V W X Y Z A B C D E F G H I J K L
N   N O P Q R S T U V W X Y Z A B C D E F G H I J K L M
O   O P Q R S T U V W X Y Z A B C D E F G H I J K L M N
P   P Q R S T U V W X Y Z A B C D E F G H I J K L M N O
Q   Q R S T U V W X Y Z A B C D E F G H I J K L M N O P
R   R S T U V W X Y Z A B C D E F G H I J K L M N O P Q
S   S T U V W X Y Z A B C D E F G H I J K L M N O P Q R
T   T U V W X Y Z A B C D E F G H I J K L M N O P Q R S
U   U V W X Y Z A B C D E F G H I J K L M N O P Q R S T
V   V W X Y Z A B C D E F G H I J K L M N O P Q R S T U
W   W 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
X   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
Y   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 X
Z   Z 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
```

To encipher a message, repeat the keyword above the plaintext:
PYTHONISEXTRAPYTHONISEXT
IJUSTLOVECOMPUTERSCIENCE

Now we take the letter we will be encoding, 'I', and find it on the first column on the tableau. Then, we move along the 'I' row of the tableau until we come to the column with the 'P' at the top (The 'P' is the keyword letter for the first 'I'), the intersection is our ciphertext character, 'X'.

So, the ciphertext for the above plaintext is:

XHNZHYWNIZHDPJRXYGPQWRZX

We can look at the algorithm this way:

Encryption
The the plaintext(P) and key(K) are added modulo 26.
Ei = (Pi + Ki) mod 26

Decryption
Di = (Ei - Ki + 26) mod 26

You task is to write a Python program that will implement this algorithm. The user will be asked to input a string of characters (including special characters) containing an unencrypted message. Then the program will accept the **key** that will be used to encode the message. You **must** first create a function named **cleanup**, which will accept the original input as a parameter, remove the special characters and spaces and **return** a string of UPPER CASE characters containing a message to be encrypted using the Vigenère Cipher.

Next the main section of the program will call a function named **encrypt** taking the cleaned message string as a parameter. The function will then print out the original message and the encoded message and return that message to the main section.

Lastly, the main section will call a function named **decrypt**, which will accept the encoded message as a parameter, decode it, and print out what should be the original message. No return required.

The main section will simply print a closing message: "Encryption/decryption complete".

A Sample Run Follows:

This program uses the Vigenère Cipher to encrypt and decrypt messages

Enter a message to be encrypted and then decrypted: *(IJ&u^s66T:lo*(v5ECom*(pu*tE5RSci^&en^c@e**
Enter the encryption key: PYTHONISEXTRA

The cleaned message is: IJUSTLOVECOMPUTERSCIENCE
The encrypted message is: XHNZHYWNIZHDPJRXYGPQWRZX
The decrypted message is: IJUSTLOVECOMPUTERSCIENCE
Encryption/Decryption Complete