Character Encoding Practice

1 Name your Jupyter Notebook as:

`TASK1_<your name>_<centre number>_<index number>.ipynb`

The task is to implement a Vigenère cypher encryption algorithm.

Vigenère cypher is a method of encrypting alphabetic plaintext using multiple substitution alphabets. A Vigenère table or square that is used to encrypt each character is shown below:

Plaintext

Key	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

A ciphertext can be obtained by determining the character contained within the intersection between the column belonging to the plaintext and the row belonging to the key.

For example, if a character in the plaintext is M, and the key is E, then the ciphertext of that character is Q, which is the intersection between column M and row E.

By taking the first column (column A) to be column 0, the first row (row A) to be row 0, and the characters A to Z to be in alphabetical sequence from position 0 (A) to 25 (Z), we can also interpret the Vigenère square as follows:

- Plaintext M is in column 12.
- Key E is in row 4.
- Ciphertext is character in position 12 + 4 = 16 i.e. Q.
- If the ciphertext goes beyond position 25, i.e. Z, it cycles back to position 0 i.e. A.

When a passage in plaintext needs to be encrypted, a keyword containing more than one letter can be written repeatedly under the characters of the passage to derive the ciphered characters of the encrypted passage.

For example, if the plaintext is “COMPUTING” and the keyword is “GREAT”, we may follow the steps below to encrypt the plaintext:

Plaintext	C	O	M	P	U	T	I	N	G
Position	2	14	12	15	20	19	8	13	6

Key	G	R	E	A	T	G	R	E	A
Position	6	17	4	0	19	6	17	4	0

Ciphertext	I	F	Q	P	N	Z	Z	R	G
Position	8	5	16	15	13	25	25	17	6

For this task, assume that only uppercase English letters (A – Z) will be used for both the plaintext and ciphertext .

For each of the sub-tasks, add a comment statement, at the beginning of the code using the hash symbol ‘#’, to indicate the sub-task the program code belongs to, for example:

```
In [1]:    # Task 1.1
           Program code

           Output:
```

Task 1.1

Write a function `substitution(char, key)` that:

- takes in an uppercase letter of the plaintext, `char`, and a character of the key which is also an uppercase letter, `key`
- returns the encrypted letter. [5]

Task 1.2

Write program code to:

- read in 2 uppercase letters from the user, which is a letter for the plaintext and a letter for the key
- call your function from **Task 1.1** with these letters
- output its encrypted letter. [2]

Test your program **two times**, with the following test data:

- `char = 'A', key = 'P'`
- `char = 'Y', key = 'C'` [2]

Task 1.3

Write a function `vigenere_cipher(plaintext, keyword)` that:

- takes in a string `plaintext`, which consists of uppercase letters
- takes in a string `keyword`, which consists of uppercase letters
- uses Vigenère cypher to encrypt `plaintext` using `keyword`
- uses the function from **Task 1.1** to encrypt each letter
- return the encrypted string, ciphertext. [4]

Test your function using the following data:

- `plaintext = 'HELLOWORLD', key = 'PYTHON'` [1]

Task 1.4

The text file `plaintext.txt` contains a message that needs to be encrypted using Vigenère cypher and then stored in a text file named `ciphertext.txt`

Write program code to:

- read the data from the text file `plaintext.txt`
- remove all non-alphabetical characters from the data and convert all the alphabets to uppercase letters
- read in a keyword from the user, ensuring that the user input is a valid keyword consisting of at least 2 alphabetical characters
- use your function from **Task 1.3** to encrypt the plaintext
- store the encrypted message, ciphertext in the text file `ciphertext.txt` [5]

Test your program with `plaintext.txt`

Show the contents of `ciphertext.txt` after you have run the program. [1]

Save your Jupyter Notebook for Task 1.