Background

The Vigenère Cypher was first described by Bellaso in 1553. Centuries later it was incorrectly attributed to Vigenère (a contemporary of Bellaso) and for some reason that is the name that has stuck.

The Vigenère Cypher is an improvement on the much older Caesar Cypher, in which each letter of a message (or "plaintext") is replaced by the letter that is offset from the original letter by a fixed amount.

Example: In a Caesar Cypher with offset 3, each “A” in the plaintext is replaced with “D”, each “B” with “E”, and so on. The alphabet is considered to wrap-around, so each “X” in the plaintext is replaced with “A”, etc. The paintext “MYDOGHASFLEAS” would be encrypted as “PBGRJKDVIOHDV”.

We call the offset number the *key* of the cypher. To use the cypher, the sender and recipient both need to know the key.

The problem with the Caesar Cypher is that it is trivially easy to break - every instance of a common letter in English text, such as “E” and “T”, will be replaced by the same letter. So finding the most common letters in the encrypted text gives strong indications of the letters of the plaintext.

The Vignère Cypher addresses this weakness by applying multiple Caesar Cyphers to the plaintext. It is based on 26 Caesar Cyphers, represented by the rows of this table:

	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

Note: we do not expect you to type this table into your program by hand. Consider how to create the first row using a loop, and then how to create all the other rows by applying slicing operations to the first row.

Instead of the key being a single number, the key is a word. The keyword can be of any length and can contain repeated letters. To perform the encryption, we place repeated copies of the keyword under the plaintext. Each letter of the plaintext is encrypted using the row of the table corresponding to the letter of the keyword that is under it.

Example:
Suppose the plaintext is originally “Blue blue windows behind the stars.” and the given key is “moose”. First we convert everything to upper case and eliminate spaces and punctuation, giving “BLUEBLUEWINDOWSBEHINDTHESTARS” and “MOOSE”. We line the plaintext and keyword copies up like this:

```
BLUEBLUEWINDOWSBEHINDTHESTARS
MOOSEMOOSEMOOSEMOOSEMOOSEMOOS
```

To encrypt the first “B”, we go to row “M” of the table and find the letter in the column for “B”, which is “N”. For the “L” and “U” we use row “O”, getting “Z” and “I”. For the “E” we use row “S”, getting “W”. So, the first “BLUE” is encrypted as “NZIW”.

You can see that the second “BLUE” will have a different encryption because it lines up with the keyword letters “EMOO” whereas the first “BLUE” lines up with “MOOS”.

The Scenario

You have been hired by a start-up called *Renaissance Technologies*. The company’s mission is to re-introduce 16th century technology to the modern world. Many of your colleagues are working on re-inventing the spinning wheel and the astrolabe. You have been assigned a solo project: implementing state-of-the-art 16th century data security.

Your Assignment

You are required to write a computer program that will prompt the user for some text and a keyword, and then display the Vignère encrypted form of the text on the screen.

You may assume:

1. The plaintext will only contain letters, numbers, spaces and punctuation symbols. It will not contain letters with accents or characters that cannot be printed. Recall, that you must remove punctuation prior to generating the cypher
2. The keyword will contain only letters.
3. The plaintext and keyword may contain a mix of uppercase and lowercase letters

Requirements

1. There is a link to a python outline of a solution on the same page as this assignment file. You are not required to follow the outline, but you must include the initial docstring as listed below.. You may use a language other than python so long as:
    a. Your program compiles
    b. The language is a reasonable first coding language (eg. C, Java). Languages such as SQL or Haskell are not appropriate.

    c. If in doubt, just use Python
2. You will be graded out of 100 with the following breakdown:
    a. 70 marks for correctness (your code accurately yields the required cyphertext)
    b. 30 marks programming style (have you followed reasonable protocol, did you implement your loops correctly, etc.)
3. Your submission must include **a program file**, and a **comment** in the dropbox:
    a. The program must compile without any modifications
    b. The comment must include the following informations:
        i. The language you have chosen
        ii. A copy and paste of your code
        iii. A copy and paste of your testing output

        Note: it is recommended that you save this comment in a text file, before copying it into the textbox.

STYLE GUIDE:
https://sites.cs.queensu.ca/courses/cisc121/cisc_121_python_3_style_guide.html

All assignment programs must begin with the following docstring::

```
"""
    CISC-121 2022F

    Name:   <Your name here>
    Student Number: <Your student number here>
    Email:  <Your email here>
    Date: 2022-XX-XX

    I confirm that this assignment solution is my own work and
    conforms to Queen's standards of Academic Integrity
"""
```