The Vigenère Cypher

Robin Dawes

September 12, 2021

In this assignment you are tasked with implementing a version of data encryption which was believed to be unbreakable for many years.

.

Background

The Vigenère Cypher. 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.
So the plaintext "MYDOGHASFLEAS" would be encrypted as "PBGRJKDVIOHDV".

We will only work with plaintext that is all capital letters, and contains no spaces or punctuation.

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 Vigenère 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

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".

How do we go to row "M" when all indices in Python are integers? We use the built-in **ord()** function! See class notes for more information.

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.

The Scenario

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

Your Assignment

You are required to write a Python 3 program that will prompt the user for some text and a keyword, and then display the Vigenère encrypted form of the text on the screen.

Where to Start

Here is a link to a Python outline of your solution. `https://courses.caslab.queensu.ca/d/sites/default/files/2021-09/Assignment%201%20Shell.py__0.txt`

You need to write all the parts that say "You write this". You may add other steps if you wish.

Programming Style

See `https://sites.cs.queensu.ca/courses/cisc121/cisc_121_python_3_style_guide.php` for guidelines on appropriate programming style for CISC-121 assignments. There is also a link to this document on the Assignments page on our course website.

How You Will Be Graded

The assignment will be marked out of 100. 70% of the grade will be for correctness and 30% of the grade will be for programming style.

The grader will read your code and will run your program to test its correctness.

What to Submit

For this assignment, you are required to upload (on onQ) a single file called Assignment_1.py.