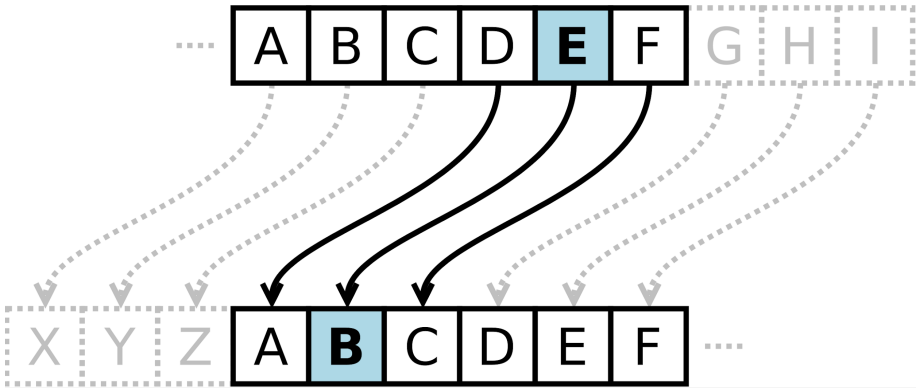
Challenge #3: Vigenère Cipher

Bachelor in Informatics and Computing Engineering
Programming Fundamentals
Instance: 2022/2023

1. Introduction

The *Caesar Cipher* is one of oldest known ciphers used to encrypt secret messages: each letter from A to Z is substituted by another shifted by a fixed distance k. For example, for the left shift of 3, the substitution is:

Plain	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
Cipher	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



To encrypt an entire message, we simply substitute each letter of the alphabet by its shifted one; for example:

Plaintext: `THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG`
Ciphertext: `QEB NRFZH YOLTK CLU GRJMP LSBO QEB IXWV ALD`

To decrypt the message, one simply has to perform a right shift of 3, or equivalently, perform a left-shift of 23 (because there are 26 letters and 26-3= 23).

The Caesar cipher is an example of a *mono-alphabetical* substitution cipher because each letter in the plaintext is replaced by another fixed one in the ciphertext. And because there are only 26 keys (i.e. number of possible shifts), it is easy to decrypt any ciphertext by trial and error, so this is a very insecure cipher.

A variation of the Caesar cipher that greatly increases the number of possible keys and makes it a little bit more secure is called the *Vigenère cipher.* The idea is to encrypt the

plaintext using a distinct shift for each letter according to a keyword previously exchanged between the communicating parties.

Suppose the plaintext to encrypt is “ATTACK AT DAWN” and the keyword is “LEMON”. We write the keyword repeated as often as necessary below the plaintext. Each letter of the keyword now defines a (right) shift from 0 to 25:

Plaintext:	`ATTACKATDAWN`
Key:	`LEMONLEMONLE`
Ciphertext:	`LXFOPVEFRNHR`

The first letter A is shifted by L (= 11); the second letter T is shifted by E (= 4); the third letter T is shifted by M (= 12) and so forth. Note that the two occurrences of letter T in the plaintext become different letters in the ciphertext (X, F). This property makes the Vigenère cipher *poly-alphabetical*.

2. Objective

Write a Python program that asks for a plaintext and keyword and outputs the ciphertext encrypted by the Vigenère cipher. Your program should ignore all characters other than letters and treat uppercase and lowercase letters as equivalent (for example by converting the entire plaintext to uppercase).
Instead of writing a separate program to decrypt the ciphertext given the key, can you think of a way of using the same program to handle both encryption and decryption?

3. References

- Wikipedia article on the Caesar cipher
- Wikipedia article on the Vigenère cipher

The end.