CSE108 – Computer Programming Laboratory
Spring 2022, Lab 6

Task: Write a complete C program to encrypt and decrypt messages by using Vigenère Cipher described below. (The key, plaintext, keystream and ciphertext mentioned below are all char arrays.)

Vigenère Cipher uses **a key** to encrypt a message. This key might be shorter/longer than **the plaintext** which is desired to be encrypted. The size of the key and the plaintext should be equalized either deleting some characters of the key (starting with the last character) or repeating the key again and again till its size reaches the size of the plaintext. The final version of the key is named **keystream**. Once you have plaintext and the key stream you should use the following alphabet table to encrypt the plaintext. The encrypted text is called **the ciphertext.**

PLAIN TEXT

KEYSTREAM	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

How to obtain the alphabet table?

You are allowed to write only the first row of the table (you should use English alphabet, which means you should create a 2D array with a size of 26x26) manually. The other rows should be generated in a loop by using the first row. PS: the blackboxes above are not the parts of the array, they are just used to make it easier to see the table better.

How to encrypt?
Once you have the plaintext and the keystream, you should use the alphabet table to encrypt a message. Whatever you see at the intersection of the keystream letter and the plaintext letter, is the ciphertext letter. All of these letters' indexes are the same. I.e. if you are trying to get the first letter of the ciphertext, you should use the first letter of the plaintext and the first letter of the keystream.

How to decrypt?
Likewise, you should decrypt the ciphertext letter by letter. You should search the array and find the plaintext letter which generates the corresponding ciphertext letter when it intersects with the corresponding keystream letter.

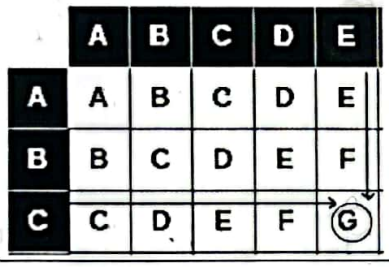
Encrypting example:

Input	Output
Plaintext: ENUMERATED	Keystream: CBACBACBAC
Key: CBA	Ciphertext: GOUOFRCUEF

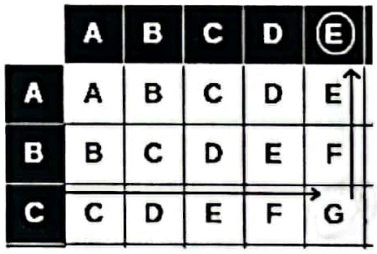
Decrypting example:

Input	Ouput
Ciphertext: GOUOFRCUEF	Keystream: CBACBACBAC
Key: CBA	Plaintext: ENUMERATED

Encrypting the first letter:
(use the first letter of the keystream which is 'C', and check what it produces with the plaintext's first letter which is 'E'. The result is 'G')



Decrypting the first letter:
(use the first letter of the ciphertext which is 'G', and check which plaintext letter produces 'G' by using the first letter of the keystream which is 'C'. The result is 'E'.)



The program should generate the 2D array and print it (10 points).
After that, the program should implement encryption (35 points) and decryption (35 points) respectively.
There should be a makefile (10 points) and comments (10 points).
For encryption; the program should ask for a plaintext (10 chars) & a key (3 chars) and print the generated keystream (10 chars) & ciphertext (10 chars).
For decryption: the program should ask for a ciphertext (10 chars) & key (3 chars) and print the keystream (10 chars) & plaintext (10 chars).
Do not use %s operator in any part of your code.
Use char c = getchar (); to read chars instead of scanf (if you use scanf, it will not work as desired)
Using pointers is not allowed. Using libraries other than stdio.h is not allowed.
The program should be able to generate a ciphertext by using a key, and then turn back to the same plaintext by using the same key.
The program should have
- a function to print the table
- a function to encrypt a single letter
- a function to decrypt a single letter

***Expected output** for encryption and decryption, you should print the table too, as you saw on the picture above (only white boxes).*

```
*** ENCRYPTION ***

Plaintext: ENUMERATED
Key: CBA
Keystream: CBACBACBAC
Ciphertext: GOUOFRCUEF

*** DECRYPTION ***

Ciphertext: GOUOFRCUEF
Key: CBA
Keystream: CBACBACBAC
Ciphertext: ENUMERATED
```