

DESIGN PROBLEM

A shift cipher¹, also known as a Caesar cipher, is a simple encryption technique where each letter of a message is replaced by another letter some number of positions down in the alphabet. For example, if $N=3$ (assuming a left shift) then the cipher looks as in the table and the word `Hello` becomes `Ebiil`.

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

This cipher can be applied to text multiple times to further complicate the encryption. For example, applying $N=3$ twice in a row results in `Hello` becoming `Byffi`. Or using $N=3$ and then $N=7$ results in `Hello` becoming `Xubbe`. Or using $N=3$, then $N=7$, and then $N=4$ results in `Hello` becoming `Tqxxa`.

Using a design pattern discussed in class, write a small program that implements the use of a shift cipher to encrypt a string. The encryption can be applied multiple times to the message.

¹ See https://en.wikipedia.org/wiki/Caesar_cipher