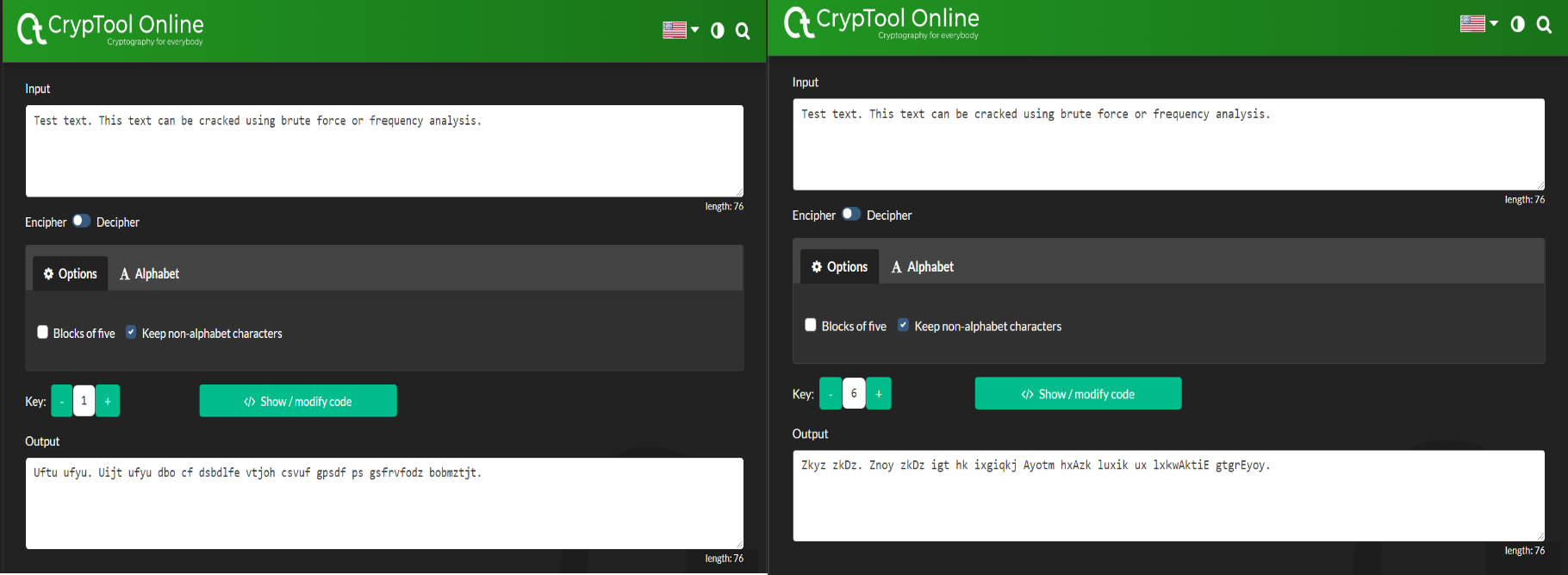
Cryptography and Network Security Tutorial Task – 1

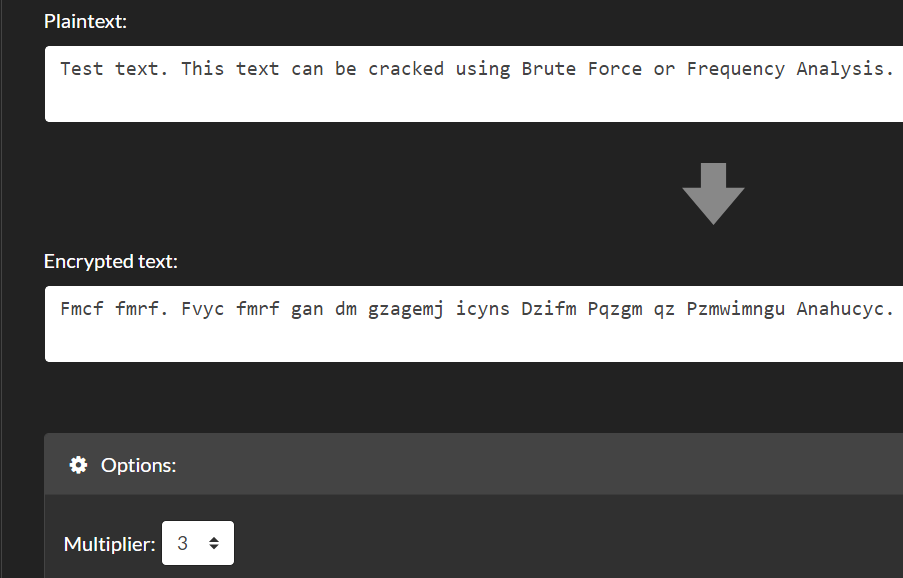
Amogh Karhadkar 1BM18CS014

There are many ciphers available to try at Cryptool such as Caesar, RSA, Enigma(The one that Germans used during World War 2), Multiplicative, and many more. Each has its advantages and disadvantages.

The Caesar cipher is named after the Roman military and political leader Gaius Julius Caesar. This cipher uses a key(integer) which is used to encrypt(convert plaintext to ciphertext) and decrypt(convert ciphertext to plaintext) messages. Below is one example.

The 1st image has key = 1 and the 2nd one has key = 6. If key = 0 then plaintext would be the same as ciphertext. The Caesar cipher is vulnerable to Brute Force and Frequency Analysis. As the images show it is a one-to-one cipher, which means if A is mapped to X then whenever there is A in the text there will be X. This fact can be used to the advantage and Caesar cipher can be cracked.

Multiplicative cipher needs an integer as a key. Each character in the message is multiplied with this key. Then is modded by the number of letters in the keyspace. This is the process of encryption. For decryption, the inverse has to be found to get the original text back. This is also a one-to-one cipher.

Here Multiplier chosen is 3. If the multiplier would have been 1 then plaintext would be equal to ciphertext.

Even though this cipher seems to be more complex than the Caesar cipher, it is not more secure. It is less secure than the Caesar cipher because the number of possible keys is smaller.

As a part of the task, Enigma was also explored. It uses wheels where each wheel is a permutation of the letters. There can be any number of wheels. The

Enigma cipher is a complex cipher developed by Germans during the reign of Hitler.

There are many more ciphers to be explored and to be learned about. These were the few that interested me.