CNS Tutorial Task 1 - CrypTool

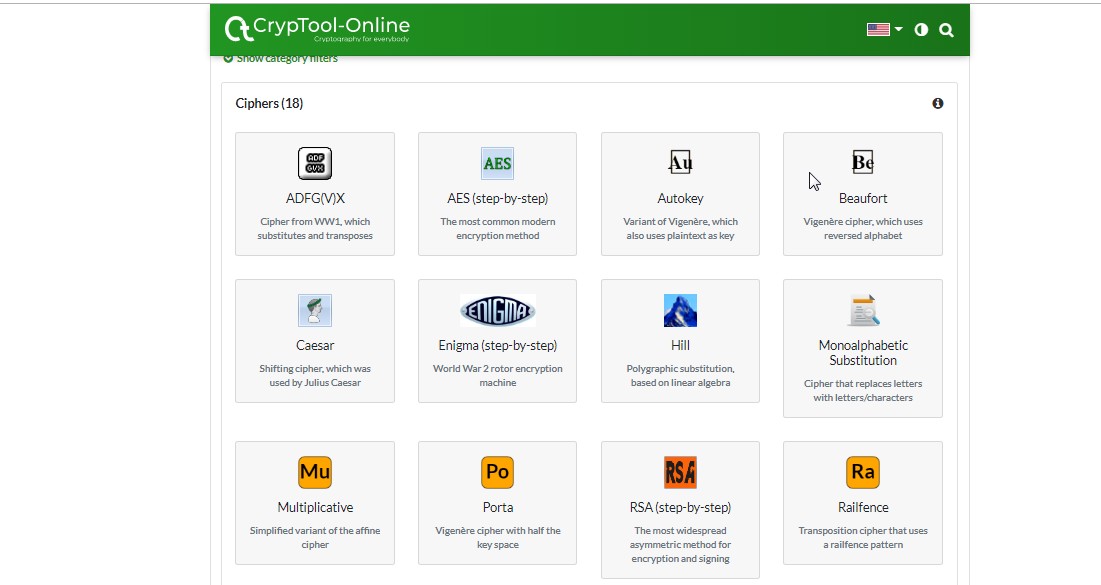
**Name: ARBAZ AHMED**

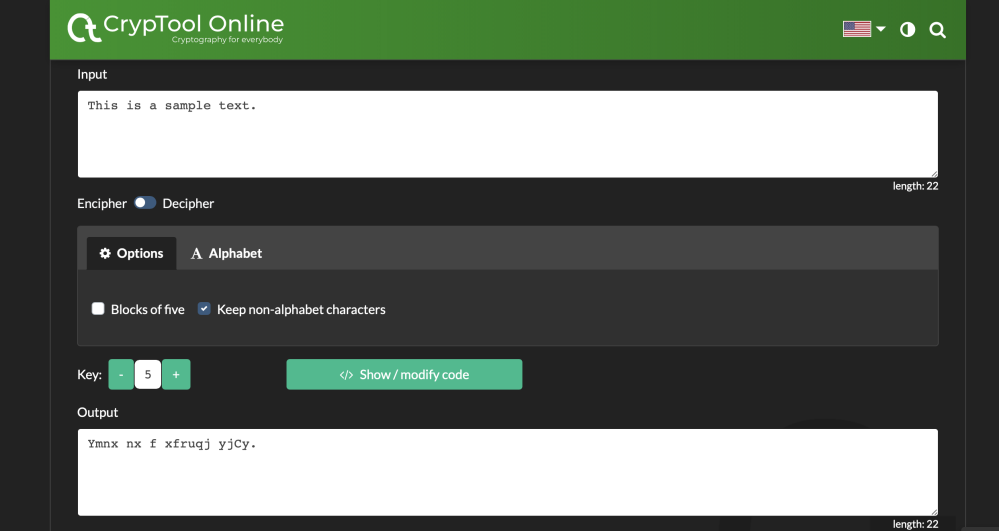
**USN: 1BM19CS401**

**The Caesar Cipher technique is one of the earliest and simplest method of encryption technique. It’s simply a type of substitution cipher, i.e., each letter of a given text is replaced by a letter some fixed number of positions down the alphabet. For example with a shift of 1, A would be replaced by B, B would become C, and so on. The method is apparently named after Julius Caesar, who apparently used it to communicate with his officials.**

Ciphers are algorithms that are used for encryption and decryption of plaintext and ciphertext respectively using a secret key. Ciphertext is encrypted text transformed from plaintext using an encryption algorithm. Ciphertext cannot be read until it has been decrypted (i.e.., converted into plaintext) with the secret key.

There are many ciphers available to try at Cryptool such as Caesar, Beaufort. CrypTool helped me visualise different ciphers such as Caesar, Enigma and Beaufort and many more as shown below



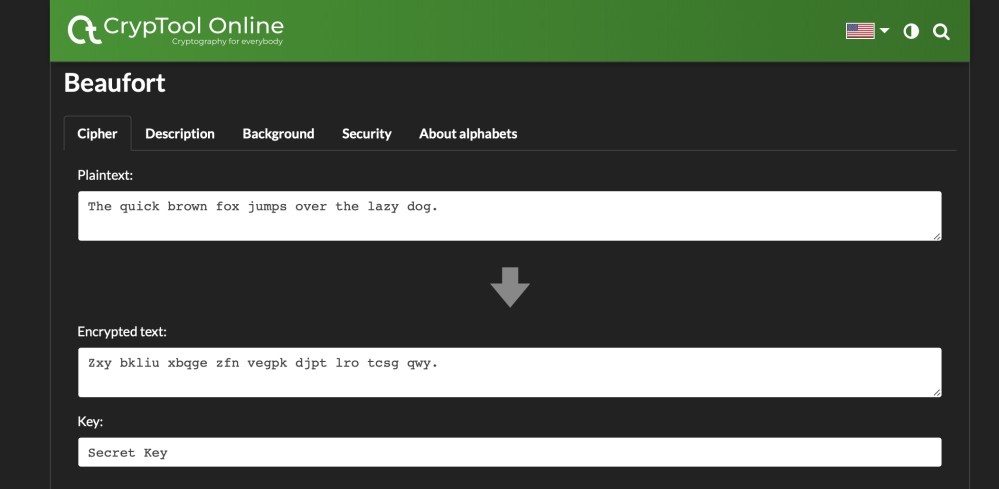


The first image shows the code used to form Caesar cipher and also to decipher it based on the given key value. The Caesar cipher is vulnerable to Brute Force and Frequency.

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. In second image, we can see an example of Caesar Cipher with key = 5.

The other method is Beaufort method, mentioned in images below:



Beautfort description:

