Aim:- Explain the fundamentals concepts of computer security and network security.

Theory:-

What is shift Cipher?

The Caesar Cipher is a type of **shift cipher**. Shift Ciphers work by using the modulo operator to encrypt and decrypt messages. The Shift Cipher has a **key K**, which is an **integer from 0 to 25**. We will only share this key with people that we want to see our message.

How and why shift cipher can be broken?

Since there English text.are only a limited number of possible shifts (25 in English), an attacker can mount a brute force attack by deciphering the message, or part of it, using each possible shift. The correct description will be the one which makes sense as

What is Mono-aplhabetic substitution?

A monoalphabetic substitution is a cipher in which each occurrence of a plaintext symbol is replaced by a corresponding ciphertext symbol to generate ciphertext. The key for such a cipher is a table of the correspondence or a function from which the correspondence is computed.

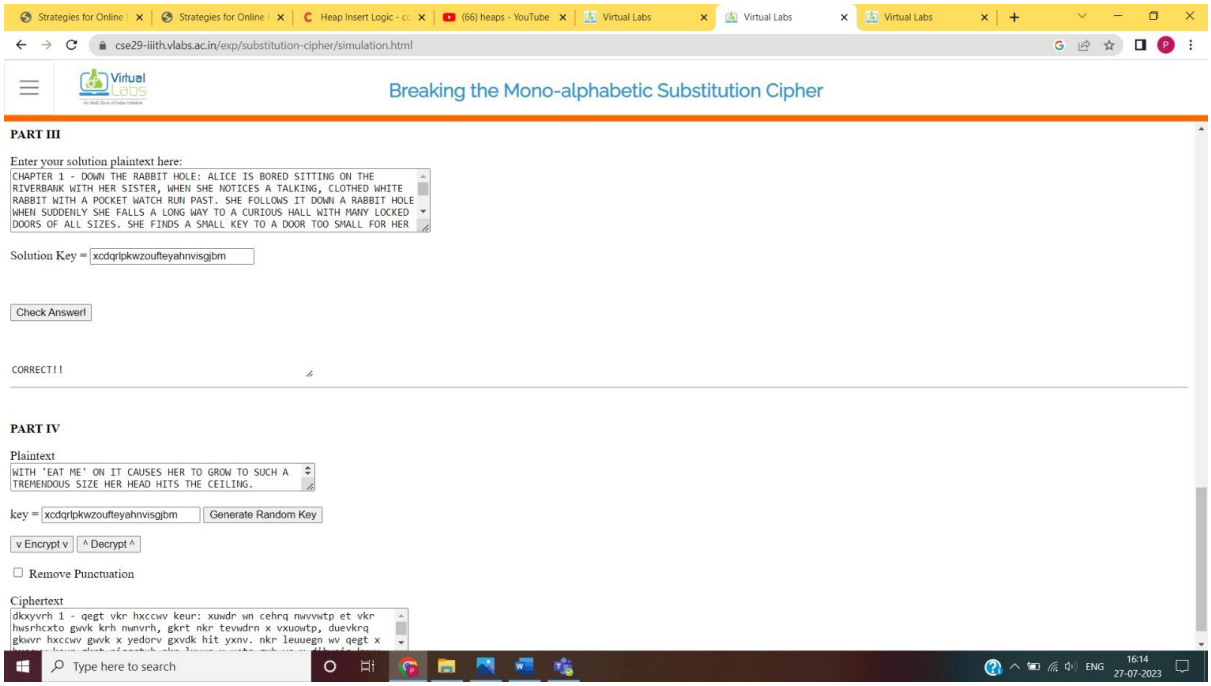
Can it be broken using brute force?

Brute force is the “dumb” approach to breaking a cipher. While it was sufficient in breaking the Caesar cipher, it is not feasible for a monoalphabetic substitution cipher

How can be broken?

A good way to break a monoalphabetic substitution cipher is to perform a frequency analysis of the characters in the ciphertext, and then compare the frequencies obtained with the frequencies of each letter of the alphabet in english plaintext (or any language the original message is assumed to be written in). You then match the character with the highest frequency in the ciphertext with the character with the highest frequency in the english language, and do the same thing with the next most frequent, then with the next until you have a complete mapping between the frequencies of the characters in the ciphertext and the frequencies of the letters in english plaintext.

Output:



Conclusion:-

With help of mono-alphabetic break shift cipher technique we could convert cipher text to plain text.