PRIYADARSHINI COLLEGE OF ENGINEERING
(Recognised by A.I.C.T.E., New Delhi & Govt. of Maharashtra, Affiliated to R.T.M.Nagpur University)Near CRPF Campus, Hingna Road, Nagpur-440 019, Maharashtra (India)
Phone : 07104 - 236381, 237307, Fax : 07104 - 237681,

Practical No. 1

Aim- To implement Caesar Cipher Substitution Techniques.

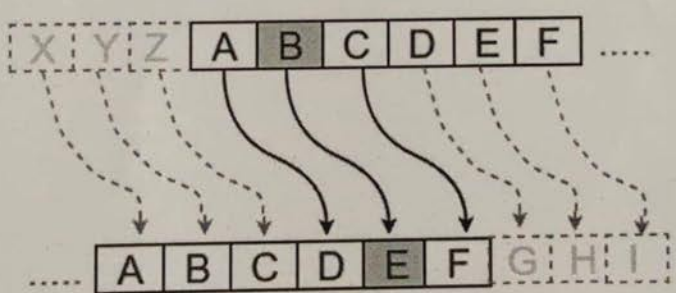
Theory:-

The Caesar Cipher technique is one of the earliest and simplest methods of encryption technique. It's simply a type of substitution cipher, i.e., each letter of a given text is replaced by a letter with a 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.

Thus to cipher a given text we need an integer value, known as a shift which indicates the number of positions each letter of the text has been moved down.
The encryption can be represented using modular arithmetic by first transforming the letters into numbers, according to the scheme, A = 0, B = 1,..., Z = 25. Encryption of a letter by a shift n can be described mathematically as.

$$E_n(x) = (x + n) mod\ 26$$
(Encryption Phase with shift n)

$$D_n(x) = (x - n) mod\ 26$$
(Decryption Phase with shift n)



Algorithm : -

- Traverse the given text one character at a time .
- For each character, transform the given character as per the rule, depending on whether we're encrypting or decrypting the text.
- Return the new string generated.

Example:

Sample Input :
Plain text: Welcome to Computer Technology

Sample Output:
Cipher Text: z h o f r p h wr frpsxwhu whfkqrorjb

Conclusion:
The concept of Ceaser cipher is implemented sucessfully.

Viva Questions:
Q. 1.What is Caesar Cipher?
Q. 2 What is Brute Force Attack?
Q. 3 What is disadvantage of Caesar Cipher ?