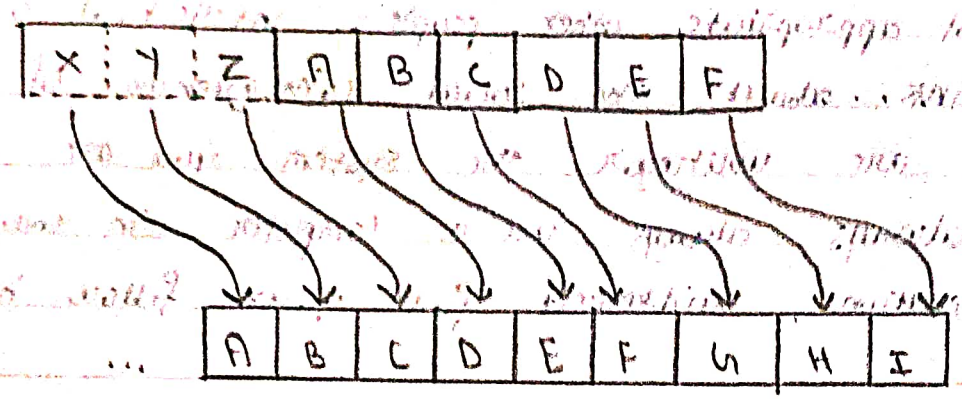
Practical No. 2

Aim: To implement Caesar cipher substitution method.



CHANDAN
PAGE NO.:
DATE :

Practical No. 2

Name of Practical

Aim: To implement caesar cipher substitution Techniques.

Theory:

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 with a fixed no. 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 connect & 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 number, according to the scheme, A = 0, B = 1, ..., Z = 25. Encryption of a letter by a shift n can be described mathematically as,

$$E_n(x) = (x + n) \bmod 26$$

(Encryption phase with shift n)

$$D_n(x) = (x - n) \bmod 26$$

(Decryption phase with shift n)

Teacher's Signature .....

CHANDAN
PAGE NO.:
DATE :

Name of Practical

Algorithms :

- 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 I/p:

plain text : welcome to computer Technology

Sample o/p:

cipher text : zhforph wr frpsxwhu whfkqrorjb

Conclusion :

The concept of caesar cipher is implemented successfully.

Viva Question :

(1) what is caesar cipher?

→ A caesar cipher is a simple method of encoding message.

(2) what is Brute force attack?

→ A brute force attack is a hacking method that uses trial and error to crack passwords, logins credentials and encryption keys.

Teacher's Signature .....

Conclusion:

The concept of Caesar Cipher is implemented successfully.

me of Practical

(3) What is disadvantage of caesar cipher?

→ (1) It can be easily hacked

(2) It provides very little security

(3) By looking at the pattern of letter in it, the entire message can be decrypted.