

Ex. No.: 1

Date:

CAESAR CIPHER

Problem Statement:

Julius Caesar protected his confidential information by encrypting it using a cipher. Caesar's cipher shifts each letter by a number of letters. If the shift takes you past the end of the alphabet, just rotate back to the front of the alphabet. In the case of a rotation by 3, w, x, y, and z would map to z, a, b and c.

Original alphabet: abcdefghijklmnopqrstuvwxyz

Alphabet rotated +3: defghijklmnopqrstuvwxyzabc

Aim:

To implement encryption and decryption in Caesar Cipher technique.

Algorithm:

1. Declare two arrays to store plaintext and ciphertext
2. Prompt the user to enter plaintext
3. Loop till the end-of line marker comes
 - a. get one plaintext character & put the same in plaintext[] array and increment i
 - b. apply caesar 3 key shift cipher on the character and store in ciphertext[] array and increment x.
4. Print the ciphertext

Program Code:

```
#include <stdio.h>
```

```
int main()
```

```
{
```

```
    char plaintext[100]={0}, ciphertext[100]={0};
```

```
    int c;
```

```
    printf("Plaintext:");
```

```
    while((c=getchar()) != '\n')
```

```
    {
```

```
        static int x=0, i=0;
```

```
        plaintext[i++]=(char)c;
```

```
        ciphertext[x++]=(char)(c+3);
```

```
    }
```

```
    printf("Cipher text:");
```

```
    printf("%s\n",ciphertext);
```

```
    return 0;
```

}

Output:

```
venom -p venom --list          vi ceasarc.c
root@fedora:/home/sudhashreemadhu# gcc ceasarc.c
root@fedora:/home/sudhashreemadhu# vi ceasarc.c
root@fedora:/home/sudhashreemadhu# ./a.out
Enter a message to encrypt: sudhashree
Enter the key: 3
Encrypted message: vxgkdvkuhhroot@fedora:/home/sudhashreemadhu# vi ceasarc.c
```

Result: