PRACTICAL-1

AIM: IMPLEMENT CAESAR CIPHER ENCRYPTION-DECRYPTION ALGORITHM.

EXPLANATION:

- 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.
- Thus to cipher a given text we need an integer value, known as shift which indicates the number of position each letter of the text has been moved down.

EXPRESSION:

$E_n(X)=(X+N) \bmod 26$

$D_n(X)=(X-N) \bmod 26$

Where n=key and x=text.

CODE:

```
#include<stdio.h>
#include<conio.h>
#include<string.h>
void encryption(char [],int);
void decryption(char [],int);
void encryption(char msg[],int key){
 printf("\nCipher Text is:");
 int i;
 for(i=0;i<strlen(msg);i++)
 {
    if(isupper(msg[i]))
```

```
        {msg[i]=((msg[i]+key-65)%26)+65;}
     else
       {msg[i]=((msg[i]+key-97)%26)+97;}
 }
 puts(msg);
}
void decryption(char cipher_text[],int key){
  printf("\nDecrypted Text is:");
  int i;
  for(i=0;i<strlen(cipher_text);i++)
  {
    if(isupper(cipher_text[i]))
       {cipher_text[i]=((cipher_text[i]-key-65)%26)+65;}
  else
       {cipher_text[i]=((cipher_text[i]-key-97)%26)+97;}
  }
  puts(cipher_text);
}
int main(){
 char msg[30];
 int key;
 clrscr();
 printf("Enter plain text:");
 gets(msg);
printf("Enter key:");
 scanf("%d",&key);
 encryption(msg,key);
decryption(msg,key);
 getch();
```

```
return 0;
}
```

OUTPUT:

```
Enter plain text:demo
Enter key:3

Cipher text is:ghpr

Decrypted text is:demo
```