EX. NO: 1(A)

IMPLEMENTATION OF CAESAR CIPHER

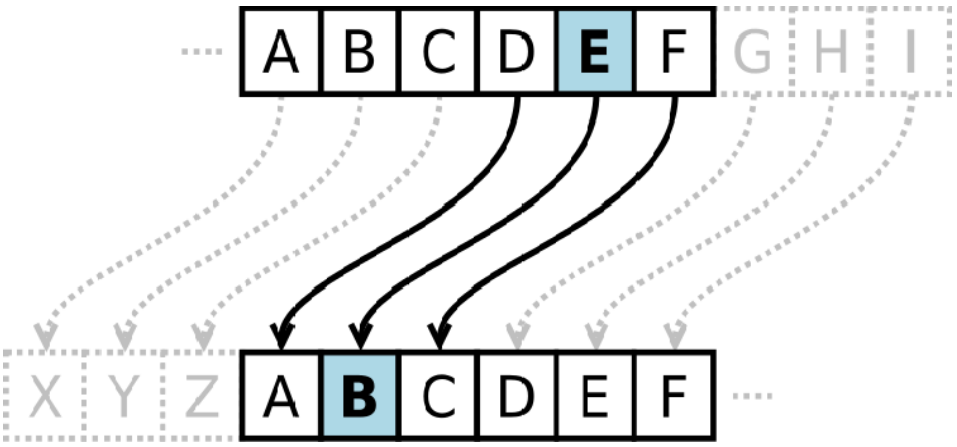
AIM:

To implement the simple substitution technique named Caesar cipher using C language.

DESCRIPTION:

To encrypt a message with a Caesar cipher, each letter in the message is changed using a simple rule: shift by three. Each letter is replaced by the letter three letters ahead in the alphabet. A becomes D, B becomes E, and so on. For the last letters, we can think of the alphabet as a circle and "wrap around". W becomes Z, X becomes A, Y becomes B, and Z becomes C. To change a message back, each letter is replaced by the one three before it.

EXAMPLE:



ALGORITHM:

STEP-1: Read the plain text from the user.

STEP-2: Read the key value from the user.

STEP-3: If the key is positive then encrypt the text by adding the key with each character in the plain text.

STEP-4: Else subtract the key from the plain text.

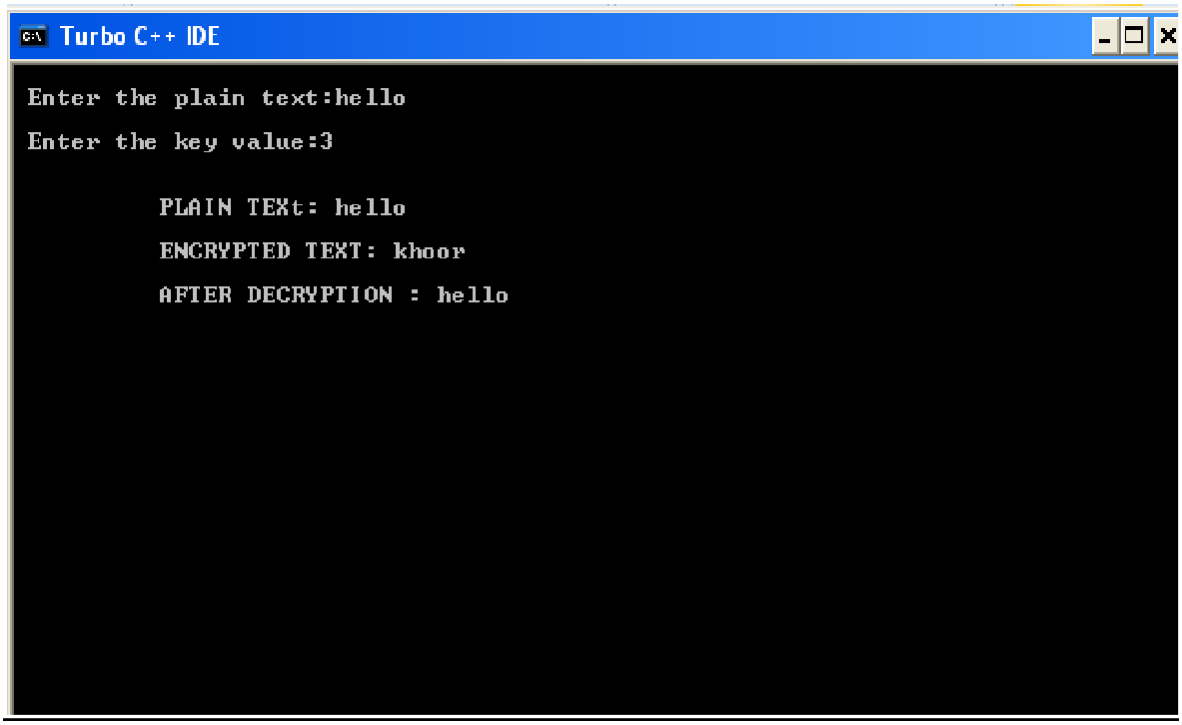
STEP-5: Display the cipher text obtained above.

PROGRAM: (Caesar Cipher)

```
#include <stdio.h>
#include <string.h>
#include<conio.h>
#include <ctype.h>
void main()
```

```
{
 char plain[10], cipher[10];
 int key,i,length;
 int result;
 clrscr();
 printf("\n Enter the plain text:");
 scanf("%s", plain);
 printf("\n Enter the key value:");
 scanf("%d", &key);
 printf("\n \n \t  PLAIN TEXt: %s",plain);
 printf("\n \n \t  ENCRYPTED TEXT: ");
 for(i = 0, length = strlen(plain); i < length;  i++)
     {
     cipher[i]=plain[i] + key;
     if (isupper(plain[i]) && (cipher[i] > 'Z'))
     cipher[i] = cipher[i] - 26;
     if (islower(plain[i]) && (cipher[i] > 'z'))
     cipher[i] = cipher[i] - 26;
     printf("%c", cipher[i]);
     }
     printf("\n \n \t  AFTER DECRYPTION : ");
 for(i=0;i<length;i++)
     {
      plain[i]=cipher[i]-key;
     if(isupper(cipher[i])&&(plain[i]<'A'))
     plain[i]=plain[i]+26;
     if(islower(cipher[i])&&(plain[i]<'a'))
     plain[i]=plain[i]+26;
     printf("%c",plain[i]);
 }
getch();
}
```

OUTPUT:



VIVA QUESTIONS:

1. Crack the following plaintext TRVJRI TZGYVIJ RIV HLZKV VRJP KF TIRTB
2. What encryption key was used?
3. Make you own cipher text using the Caesar cipher.
4. Can you crack other people's ciphertexts?
5. What key do we need to make "CAESAR" become "MKOCKB"?
6. What key do we need to make "CIPHER" become "SYFXUH"?
7. Use the Caesar cipher to encrypt your first name

How can we find the decryption key from the encryption key?

RESULT:

Thus the implementation of Caesar cipher had been executed successfully.