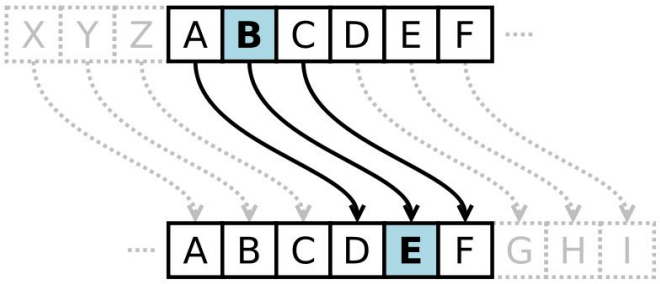
Experiment 1

Aim: Write a program to implement Caesar Cipher encryption and decryption.

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



Mathematically,

Encryption = $En = (x+k) \ mod \ 26$

Decryption = $Dn = (x+ k-1) \ mod \ 26$

Where x is the input alphabet ASCII representation and k the key, k-1 is the additive inverse of k.

Source Code:

```
import java.util.Scanner;
public class CaesarCipher
{
   public static String encryption(String text, int k)
   {
      String result="";
      for (int i=0; i<text.length(); i++)
      {
         if (Character.isUpperCase(text.charAt(i)))
         {
            char ch = (char)(((int)text.charAt(i)+k-65)%26+65);
            result+=ch;
         }
else
         {
```

```
            char ch = (char)(((int)text.charAt(i)+k-97)%26+97);
            result+=ch;
          }
       }
       return result;
    }
    public static String decryption(String text, int k)
    {
       String result=encryption(text, 26-k);
       return result;
    }
    public static void main(String[] args)
    { Scanner myObj = new Scanner(System.in);
       System.out.println("Enter the input text:");
       String text = myObj.nextLine();
       System.out.println("Enter the key to shift:");
       int k= myObj.nextInt();
       String encrypt=encryption(text, k).toString();
       System.out.println("Text          : " + text);
       System.out.println("Shift         : " + k);
       System.out.println("Encrypted Text: " + encrypt);
       System.out.println("Decrypted Text: " + decryption(encrypt,k));
    }
}
```

Output:

```
C:\Users\Admin\Desktop\college\7th Semester\Information and network security (INS)\Lab\Programs>java CaesarCipher
Enter the input text:
InformationAndSecurityLAb
Enter the key to shift:
3
Text          : InformationAndSecurityLAb
Shift         : 3
Encrypted Text: LqirupdwlrqDqgVhfxulwbODe
Decrypted Text: InformationAndSecurityLAb

C:\Users\Admin\Desktop\college\7th Semester\Information and network security (INS)\Lab\Programs>
```

Learning Outcomes:

The Caesar cipher offers essentially no communication security and it can be easily broken.