VISHNU
UNIVERSAL LEARNING
Estd. 2012

BVRIT H
BVRIT HYDERABAD College of
Engineering for Women (UGC-Autonomous)

PPS Lab Activity

Department of CSE Certified that this is a Bonafide Record of the word done by:

R. Bhanu Sri – 23WH1A05D0

G. Snikitha – 23WH1A05D2

M. Lohitha – 23WH1A05H5

G. Rishika – 23WH1A05H9

Of Class CSE C of Year 1 of Semester 1 in PPS Laboratory

Date: ***Signature***

Problem Statement:

Project 10: Caesar Cipher in Cryptography

The Caesar cipher is a simple encryption technique that was used by Julius Caesar to send secret messages to his allies. It works by shifting the letters in the plaintext message by a certain number of positions, known as the “shift” or “key”.

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 a 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 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 numbers, according to the scheme, A = 0, B = 1…, Z = 25. Encryption of a letter by a shift n can be described mathematically as.

For example, if the shift is 3, then the letter A would be replaced by the letter D, B would become E, C would become F, and so on. The alphabet is wrapped around so that after Z, it starts back at A.

Here is an example of how to use the Caesar cipher to encrypt the message “HELLO” with a
shift of 3:

Write down the plaintext message: HELLO

Choose a shift value. In this case, we will use a shift of 3.

Replace each letter in the plaintext message with the letter that is three positions to the right
in the alphabet.

H becomes K (shift 3 from H)
E becomes H (shift 3 from E)
L becomes O (shift 3 from L)
L becomes O (shift 3 from L)
O becomes R (shift 3 from O)

4.The encrypted message is now “KHOOR”.

To decrypt the message, you simply need to shift each letter back by the same number of
positions. In this case, you would shift each letter in “KHOOR” back by 3 positions to get the
original message, “HELLO”.

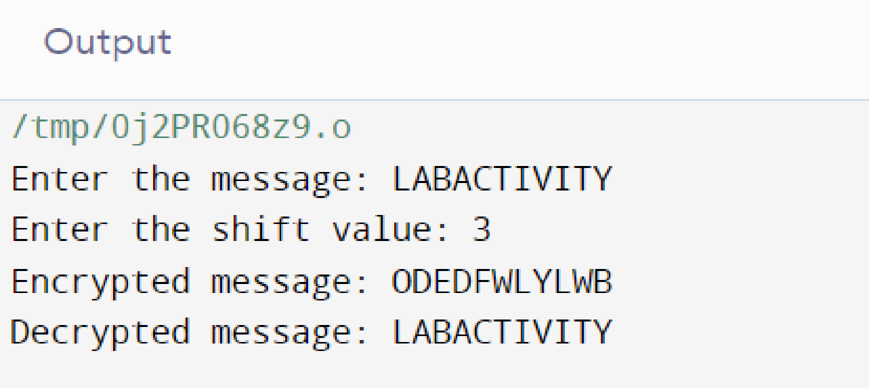
Text: ABCDEFGHIJKLMNOPQRSTUVWXYZ
Shift: 23
Cipher: XYZABCDEFGHIJKLMNOPQRSTUVW

Text: ATTACKATONCE
Shift: 4
Cipher: EXXEGOEXSRGI

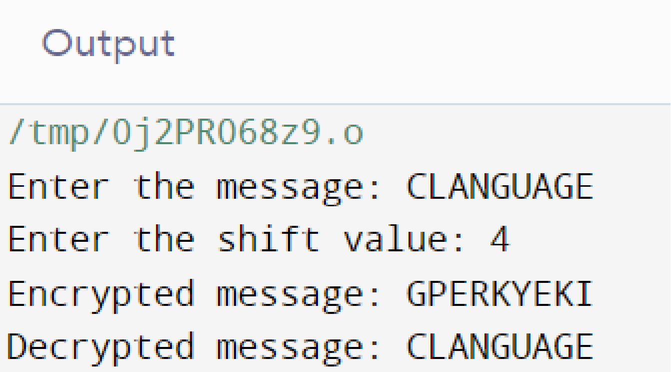
Source Code:

```
#include <stdio.h>
void encrypt(char message[], int shift)
{
   for (int i = 0; message[i] != '\0'; ++i)
   {
      if (message[i] >= 'A' && message[i] <= 'Z')
      {
         message[i] = (message[i] - 'A' + shift) % 26 + 'A';
      }
   }
}
void decrypt(char message[], int shift)
{
   for (int i = 0; message[i] != '\0'; ++i)
   {
      if (message[i] >= 'A' && message[i] <= 'Z')
      {
         message[i] = (message[i] - 'A' - shift + 26) % 26 + 'A';
      }
   }
}
int main()
{
   char message[100];
   int shift;
   // Input message from the user
   printf("Enter the message: ");
   scanf("%s", message);
   // Input shift value from the user
   printf("Enter the shift value: ");
   scanf("%d", &shift);
   // Encrypt the message
   encrypt(message, shift);
   printf("Encrypted message: %s\n", message);
   // Decrypt the message
   decrypt(message, shift);
   printf("Decrypted message: %s\n", message);
   return 0;     }
```

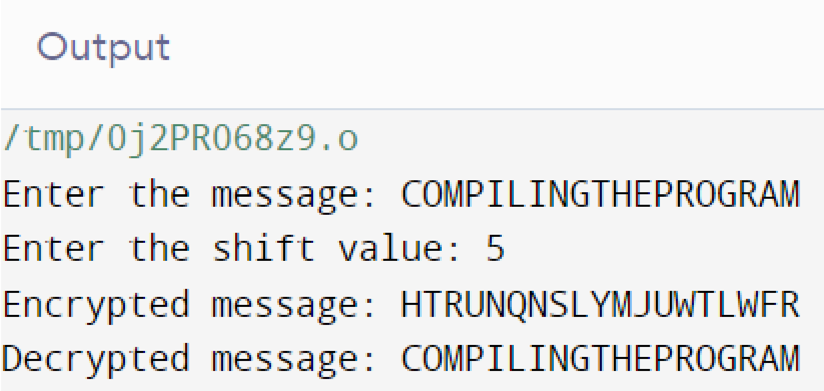
Output:



```
/tmp/0j2PR068z9.o
Enter the message: LABACTIVITY
Enter the shift value: 3
Encrypted message: ODEDFWLYLWB
Decrypted message: LABACTIVITY
```



```
/tmp/0j2PR068z9.o
Enter the message: CLANGUAGE
Enter the shift value: 4
Encrypted message: GPERKYEKI
Decrypted message: CLANGUAGE
```



```
/tmp/0j2PR068z9.o
Enter the message: COMPILINGTHEPROGRAM
Enter the shift value: 5
Encrypted message: HTRUNQNSLYMJUWTLWFR
Decrypted message: COMPILINGTHEPROGRAM
```