

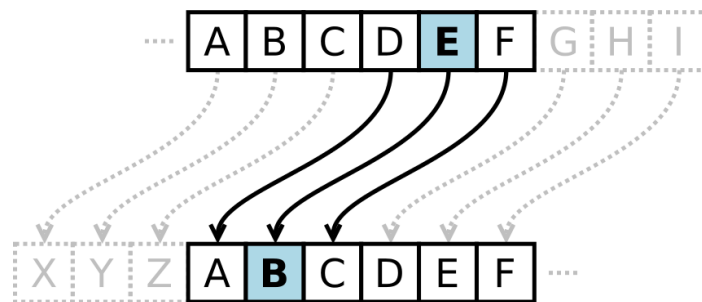
Program – 1

AIM: To implement a program to show encryption and decryption through Caesar Ciphers.

Introduction and Theory

The Caesar Cipher, also known as a shift cipher, is one of the oldest and simplest forms of encrypting a message. It is a type of substitution cipher where each letter in the original message (which in cryptography is called the plaintext) is replaced with a letter corresponding to a certain number of letters shifted up or down in the alphabet.

For each letter of the alphabet, you would take its position in the alphabet, say 3 for the letter 'C', and shift it by the key number. If we had a key of +3, that 'C' would be shifted down to an 'F' - and that same process would be applied to every letter in the plaintext.



Mathematically,

$$\text{Encryption} = E_n = (x + k) \bmod 26$$

$$\text{Decryption} = D_n = (x + k^{-1}) \bmod 26$$

Where x is the input alphabets ASCII representation and k the key, k^{-1} is the additive inverse of k.

Algorithm

```
1 encrypt (P, key)
2   encrypted = ""
3   for i in P
4     encrypted.append( (i + key) % 26 )
5   return encrypted

1 decrypt (E, key)
2   decrypted = ""
3   for i in E
4     decrypted.append( (i - key) % 26 )
5   return decrypted
```

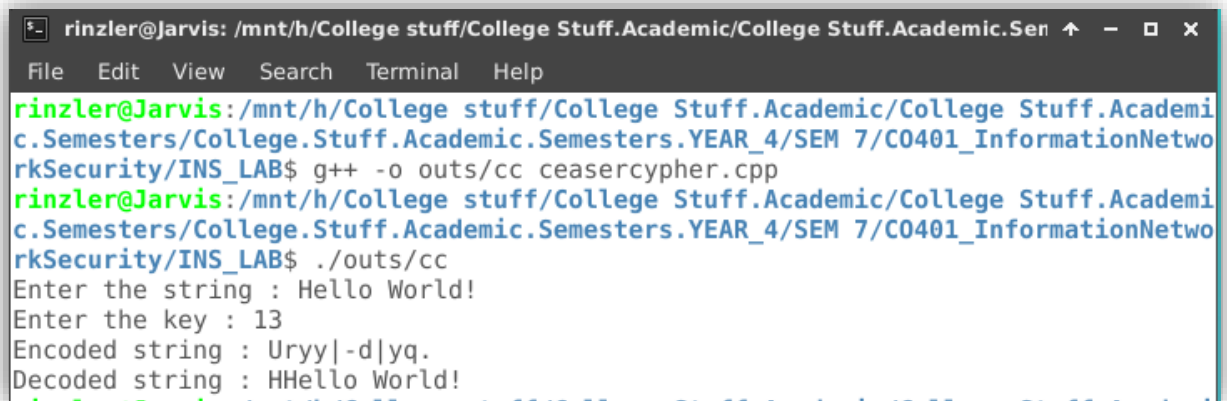
Program – 1

Code

```
1  #include <iostream>
2  #include <cstring>
3
4  std::string encoder(std::string P, int key)
5  {
6      std::string result = "";
7
8      for (int i = 0; i < P.length(); i++)
9      {
10         if (isupper(P[i]))
11             result += char(int(P[i] + key - 65) % 256 + 65);
12         else
13             result += char(int(P[i] + key - 97) % 256 + 97);
14     }
15     return result;
16 }
17
18 std::string decoder(std::string C, int key)
19 {
20     std::string result = "";
21
22     for (int i = 0; i < C.length(); i++)
23     {
24         if (isupper(C[i]))
25             result += char(int(C[i] - key - 65) % 256 + 65);
26
27             result += char(int(C[i] - key - 97) % 256 + 97);
28     }
29     return result;
30 }
31
32 int main()
33 {
34     std::string input, encoded, decoded;
35     int key;
36     std::cout << "Enter the string : ";
37     std::getline(std::cin, input);
38     std::cout << "Enter the key : ";
39     std::cin >> key;
40     encoded = encoder(input, key);
41     std::cout << "Encoded string : " << encoded << std::endl;
42     decoded = decoder(encoded, key);
43     std::cout << "Decoded string : " << decoded << std::endl;
44     return 0;
45 }
```

Program – 1

Results and Outputs:



```
rinzler@Jarvis: /mnt/h/College stuff/College Stuff.Academic/College Stuff.Academic.Semesters/College.Stuff.Academic.Semesters.YEAR_4/SEM 7/C0401_InformationNetworkSecurity/INS_LAB$ g++ -o outs/cc ceasercypher.cpp
rinzler@Jarvis: /mnt/h/College stuff/College Stuff.Academic/College Stuff.Academic.Semesters/College.Stuff.Academic.Semesters.YEAR_4/SEM 7/C0401_InformationNetworkSecurity/INS_LAB$ ./outs/cc
Enter the string : Hello World!
Enter the key : 13
Encoded string : Uryy|-d|yq.
Decoded string : HHHello World!
```

Findings and Learnings:

1. The Caesar cipher is a simple substitution cipher where the characters are shifted by some key value.
2. The cipher is cyclic in its behavior, thus allowing the same encryption procedure to be used to decrypt the text by only finding the inverse of the key in the mod.