Program – 2

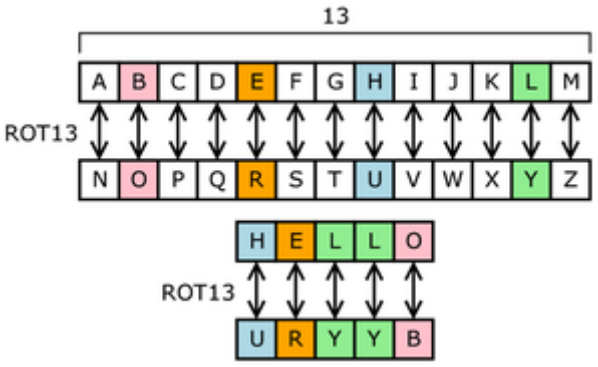
AIM: To implement a program to show encryption and decryption through Mono-Alphabetic ciphers.

Introduction and Theory

A monoalphabetic cipher is any cipher in which the letters of the plaintext are mapped to ciphertext letters based on a single alphabet key. Substitution ciphers work by replacing each letter of the plaintext with another letter. For this reason, a monoalphabetic cipher is also called a simple substitution cipher.

It relies on a fixed replacement structure, meaning the substitution is fixed for each letter of the alphabet. Thus, if the letter “a” is encoded as letter “Q”, then every time the letter “a” appears in the plaintext, it’s replaced with the letter “Q”.

There are many different monoalphabetic substitution ciphers, actually infinitely many, as each letter can be encrypted to any symbol, not just another letter.



Algorithm

```
encrypt (P, key)
  encrypted = ""
  for i in P
    encrypted.append(key[i])
  return encrypted
```

```
decrypt (E, key)
  decrypted = ""
  for i in E
    decrypted.append( key-1[i] )
  return decrypted
```

Program – 2

Code

```cpp
#include <iostream>
#include <cstring>

int enc_array[] = {9, 5, 25, 11, 8, 16, 19, 12, 6, 10, 18, 15, 20,
14, 7, 2, 4, 21, 23, 17, 3, 22, 24, 0, 1, 13};
int dec_array[26];

std::string Encrypt(std::string str, int n)
{
        std::string ans = "";
        for (int i = 0; i < n; i++)
        {
                ans += char('a' + enc_array[str[i] - 'a']);
        }
        return ans;
}

std::string Decrypt(std::string str, int n)
{
        std::string ans = "";
        for (int i = 0; i < n; i++)
        {
                ans += char('a' + dec_array[str[i] - 'a']);
        }
        return ans;
}

int main()
{
        for (int i = 0; i < 26; ++i)
        {
                dec_array[enc_array[i]] = i;
        }
        std::string input, enc, dec;
    std::cout << "Enter the string : ";
    std::getline(std::cin, input);
    enc = Encrypt(input, input.length());
    std::cout << "Encoded string : " << enc << std::endl;
    dec = Decrypt(enc, enc.length());
    std::cout << "Decoded string : " << dec << std::endl;
    for (int i = 0; i < 26; ++i)
        {
                std::cout << enc_array[i] << ' ' ;
        }
        std::cout << std::endl;
        for (int i = 0; i < 26; ++i)
        {
                std::cout << dec_array[i] << ' ' ;
        }
        std::cout << std::endl;
    return 0;
}
```

Program – 2

Results and Outputs:

```
(Ml_Py3) rinzler@Jarvis:/mnt/h/College stuff/College Stuff.Academic/College Stuf
f.Academic.Semesters/College.Stuff.Academic.Semesters.YEAR_4/SEM 7/CO401_Informa
tionNetworkSecurity/INS_LAB$ ./outs/monoc
Enter the string : hello
Encoded string : mipph
Decoded string : hello
9 5 25 11 8 16 19 12 6 10 18 15 20 14 7 2 4 21 23 17 3 22 24 0 1 13
23 24 15 20 16 1 8 14 4 0 9 3 7 25 13 11 5 19 10 6 12 17 21 18 22 2
(Ml_Py3) rinzler@Jarvis:/mnt/h/College stuff/College Stuff.Academic/College Stuf
f.Academic.Semesters/College.Stuff.Academic.Semesters.YEAR_4/SEM 7/CO401_Informa
tionNetworkSecurity/INS_LAB$
```

Findings and Learnings:

1. We have implemented Monoalphabetic ciphers