**Assignment No 1**

**Name-Aniket Tatoba Mane**

**PRN-2020BTECS00020**

**Batch-B7**

**Subject - CNS LAB**

**Aim**: To implement Caesar cipher

**Theory**: The Caesar cipher is a simple and widely known substitution cipher technique used for encryption. It was named after Julius Caesar, who is historically believed to have used this method to encode his private correspondence. The Caesar cipher is a basic encryption technique where each letter in a message is shifted a fixed number of positions

//2020BTECS00020

#include <bits/stdc++.h>

using namespace std;

char shift\_char(char c, int shift, char op)

{

    if (isalpha(c) && op == 'e')

    {

        char base = islower(c) ? 'a' : 'A';

        return char((c - base + shift) % 26 + base);

    }

    else if (isalpha(c) && op == 'd')

    {

        char base = islower(c) ? 'a' : 'A';

        return char((c - base - shift + 26) % 26 + base);

    }

    return c;

}

string encrypt\_text(string text, int key)

{

    string encrypted = "";

    for (char c : text)

    {

        encrypted += shift\_char(c, key, 'e');

    }

    return encrypted;

}

string decrypt\_text(string text, int key)

{

    string decrypted = "";

    for (char c : text)

    {

        decrypted += shift\_char(c, key, 'd');

    }

    return decrypted;

}

int main(int argc, char const \*argv[])

{

    int choice, key;

    string text;

    cout << "Enter choice: ";

    cout << endl

         << "1. Encrypt | 2. Decrypt" << endl;

    cin >> choice;

    cin.get();

    if (choice == 1)

    {

        cout << "enter text: ";

        getline(cin, text);

        cout << "Enter key: ";

        cin >> key;

        string result = encrypt\_text(text, key);

        cout << "encrypted text: " << result << endl;

    }

    else if (choice == 2)

    {

        cout << "enter encrypted text: ";

        getline(cin, text);

        cout << "Enter key: ";

        cin >> key;

        string result = decrypt\_text(text, key);

        cout << "decrypted text: " << result << endl;

    }

    else

    {

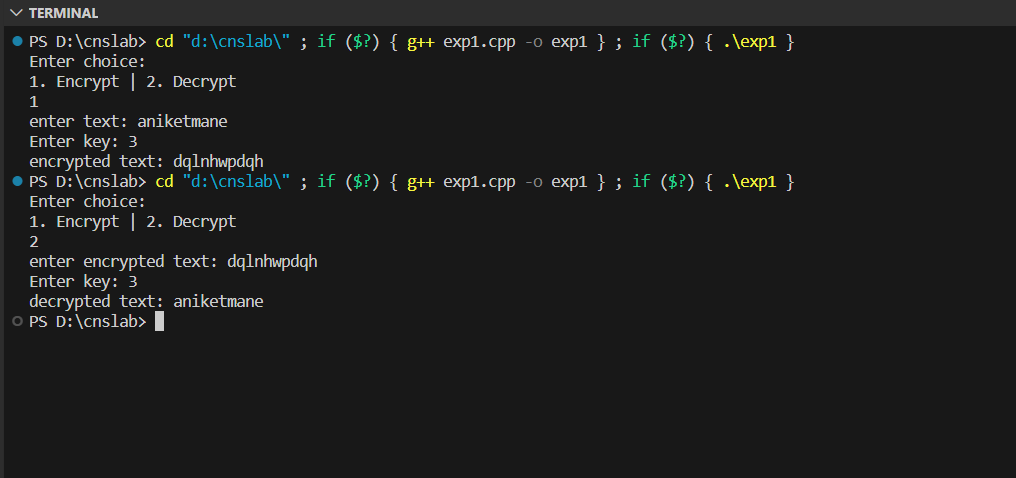
        cout << "not a valid choice!" << endl;

    }

    return 0;

}

Output:



**Limitations:**

The Caesar cipher is a simple and historically significant encryption technique that is based on shifting letters in the alphabet by a fixed number of positions. While it was effective in its time, it has several limitations that make it unsuitable for most modern encryption needs:

Lack of Security: The Caesar cipher is highly vulnerable to even the most basic cryptanalysis techniques. With only 26 possible keys (assuming an English alphabet), it can be easily cracked through brute force by trying all possible key values.

Predictable Patterns: The Caesar cipher shifts letters by a fixed amount, which means that the same letter will always be replaced with the same letter when the same key is used. This predictability allows attackers to identify common patterns and perform frequency analysis, making it easier to decrypt the message.

Limited Key Space: As mentioned earlier, the Caesar cipher has a limited key space because it only has 26 possible keys for the English alphabet. This makes it very susceptible to brute force attacks, where an attacker can quickly try all possible keys.