# Charotar University of Science & Technology (CHARUSAT)

# Devang Patel Institute of Advance Technology & Research (DEPSTAR)

# Information Security (CE348)
# Practical Solution

**Semester:6th** **Academic Year: 2022-23**

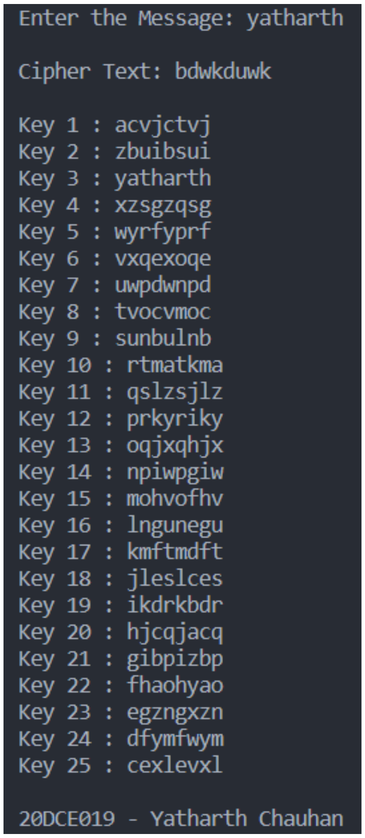
| Sr No | Aim |
|---|---|
| **1.** | **Aim:** The "Caesar Box," or "Caesar Cipher," is one of the earliest known ciphers. Developed around 100 BC, it was used by Julius Caesar to send secret messages to his generals in the field. In the event that one of his messages got intercepted, his opponent could not read them. This obviously gave him a great strategic advantage. Caesar shifted each letter of his message few letters to the right to produce what could be called the ciphertext. The ciphertext is what the enemy would see instead of the true message. So, for example, if Caesar's messages were written in the English alphabet, and shift by 3 then each letter "A" in the message would become a "D," the "B's" would become "E's," and the "X's" become "A's." This type of cipher is appropriately called a "shift cipher." Implement the cipher in any programming language of your choice. Perform encryption, decryption. Discuss and try some possible attacks on traditional Caesar cipher. |

**Code:**

```
#include <iostream>
using namespace std;
string encrypt(string msg, int key);
string decrypt(string msg, int key);
void bruteForce(string cipherText);
int main()
{
    string msg;
    int key = 3;
    cout << "Enter the Message: ";
    cin >> msg;
    string cipherText = encrypt(msg, key);
    cout << endl
         << "Cipher Text: " << cipherText << endl
         << endl;
    bruteForce(cipherText);

    cout << "\n20DCE019 - Yatharth Chauhan";
}
string encrypt(string msg, int key)
{
    string text;
    for (int i = 0; i < msg.length(); i++)
        text += 'a' + (msg[i] + key - 'a') % 26;
    return text;
}
string decrypt(string msg, int key)
{
    string text;
    for (int i = 0; i < msg.length(); i++)
        text += 'a' + (msg[i] - key - 'a' + 26) % 26;
    return text;
}
void bruteForce(string cipherText)
{
    for (int key = 1; key < 26; key++)
    {
        string text = decrypt(cipherText, key);
        cout << "Key " << key << " : " << text << endl;
    }
}
```

**Output screenshot:**



```
Enter the Message: yatharth

Cipher Text: bdwkduwk

Key 1 : acvjctvj
Key 2 : zbuibsui
Key 3 : yatharth
Key 4 : xzsgzqsg
Key 5 : wyrfyprf
Key 6 : vxqexoqe
Key 7 : uwpdwnpd
Key 8 : tvocvmoc
Key 9 : sunbulnb
Key 10 : rtmatkma
Key 11 : qslzsjlz
Key 12 : prkyriky
Key 13 : oqjxqhjx
Key 14 : npiwpgiw
Key 15 : mohvofhv
Key 16 : lngunegu
Key 17 : kmftmdft
Key 18 : jleslces
Key 19 : ikdrkbdr
Key 20 : hjcqjacq
Key 21 : gibpizbp
Key 22 : fhaohyao
Key 23 : egzngxzn
Key 24 : dfymfwym
Key 25 : cexlevxl

20DCE019 - Yatharth Chauhan
```

**Conclusions:** In this practical we learnt how to encrypt plain text into cipher text and then decrypt the cipher text into plain text.