Name - Khushi Nitinkumar Patel
PRN - 2020BTECS00037
Batch - B3

Assignment no 1: Implementation of Caesar Cipher

Introduction

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.

Encryption

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.

1. H becomes K (shift 3 from H)
2. E becomes H (shift 3 from E)
3. L becomes O (shift 3 from L)
4. L becomes O (shift 3 from L)
5. O becomes R (shift 3 from O)

The encrypted message is now **"KHOOR".**

Decryption

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".**

Encryption Code:

```cpp
#include <iostream>
using namespace std;

// This function receives text and shift and
// returns the encrypted text
string encrypt(string text, int s)
{
    string result = "";
    // traverse text
    for (int i = 0; i < text.length(); i++) {
        // apply transformation to each character
        // Encrypt Uppercase letters
        if (isupper(text[i]))
            result += char(int(text[i] + s - 65) % 26 + 65);

        // Encrypt Lowercase letters
        else
            result += char(int(text[i] + s - 97) % 26 + 97);
    }
    // Return the resulting string
    return result;
}
// Driver program to test the above function
int main()
{
    string text = "ATTACKATONCE";
    int s = 4;
    cout << "Text : " << text;
    cout << "\nShift: " << s;
    cout << "\nCipher: " << encrypt(text, s);
    return 0;
}
```

Output:

```
PROBLEMS   OUTPUT   TERMINAL

(c) Microsoft Corporation. All rights reserved.

C:\Users\khush\Desktop\acads\7th sem\cnsl>cd "c:\Users\khush\Desktop\acads\7th sem\cnsl\" && g++
sh\Desktop\acads\7th sem\cnsl\"caesar
Text : ATTACKATONCE
Shift: 4
Cipher: EXXEGOEXSRGI
c:\Users\khush\Desktop\acads\7th sem\cnsl>
```

Decryption Code:

```
#include <iostream>
using namespace std;

//This function receives text and shift and returns the encrypted text
string encrypt(string text,int s)
{
    string result="";
    //traverse text
    for(int i=0;i<text.length();i++)
    {
        //apply transformation to each character
        //Encrypt Uppercase letters
        if(isupper(text[i]))
            result+=char(int(text[i]+s-65)%26 +65);
    //Encrypt Lowercase letters
    else
        result+=char(int(text[i]+s-97)%26 +97);
    }
    //Return the resulting string
    return result;
}

//Driver program to test the above function
int main()
{
    string text="EXXEGOEXSRGI";
    int s = 4;


    cout<<"Text :"<<text;
    cout<<"\nShift:" << s;
    s = s%26; // ensuring that s lies between 0-25
    cout<<"\nCipher:"<<encrypt(text, 26-s);
    return 0;
}
```

Output:

```
c:\Users\khush\Desktop\acads\7th sem\cnsl>cd "c:\Users\khush\Desktop\acads\7th sem\cnsl\"
sh\Desktop\acads\7th sem\cnsl\"caesar
Text :EXXEGOEXSRGI
Shift:4
Cipher:ATTACKATONCE
c:\Users\khush\Desktop\acads\7th sem\cnsl>
```