Assignment – 5

Q1. Write a program to encrypt the message "Are you Ready for class" using shift cipher with any key value. Then decrypt the message back to plain text.

A:

Pseudocode and Explanation –

Input – a message string and a key value

First for loop converts all the character values into their respective number notations. Those are then further converted to cypher numbers using (x + key)mod26. All these numbers are stored in the vector – c_text.

Each number of this vector is then converted to their respective alphabetic notations. This is encrypted string which is stored in variable encrypted_text.

This encrypted text is then converted to decrypt numbers using (y-k)mod26. These numbers are then converted to their respective alphabet notation. This is decrypted string which is stored in variable decrypted_text.

Code –

```
#include<bits/stdc++.h>
using namespace std;
int main()
{
    int key;
    string s;
    cout<<"Enter the message: "<<endl;
    cin>>s;
    cout<<"Enter the key value: "<<endl;
    cin>>key;
    // cout<<s;
    vector<int> c_text;

    for(int i=0;i<s.length();i++){
        if(int(s[i])>=65 && int(s[i])<=90){
```

```
            int val = int(s[i]) - 'A';
            int x = (val+key)%26;
            c_text.push_back(x);
        }else{
            int val = int(s[i]) - 'a';
            int x = (val+key)%26;
            c_text.push_back(x);
        }
    }

    // for(int i=0;i<c_text.size();i++){
    //     cout<<c_text[i]<<" ";
    // }

    string encrypted_text="";
    for(int i=0;i<c_text.size();i++){
        encrypted_text+=char(c_text[i]+65);
    }
    cout<<"The encrypted text is: "<<encrypted_text<<endl;

    string decryted_text="";
    for(int i=0;i<c_text.size();i++){
        int val = c_text[i] - key;
        int x;
        if(val<0){
            x = val+26;
        }else{
            x = val;
        }

        decryted_text+=char(x+65);
    }
    cout<<"The decrypted text is: "<<decryted_text<<endl;

}
```

Output –

```
Enter the message:
AreyouReadyforclass
Enter the key value:
11
The encrypted text is: LCPJZFCPLOJQZCNWLDD
The decrypted text is: AREYOUREADYFORCLASS
PS C:\Users\arinr\Desktop\Crypto_Lab\Lab_5>
```

Q2. Write a program to find the key value of the given cipher text (JBCRCLQRWCRVNBJENBWRWN).

A:

Pseudocode and Explanation –

We check for all the values of key from 1 to 25. As we get all the decrypted string, We try to extract the most meaningful string.

Code –

```
#include<bits/stdc++.h>
using namespace std;
int main()
{
    string cipher_text = "JBCRCLQRWCRVNBJENBWRWN";
    // string cipher_text = "HPHTWWXPPELXTOYTRSE";

    vector<int> c_text;
    for(int i=0;i<cipher_text.length();i++){
        int val = int(cipher_text[i] - 65);
        cout<<val<<" ";
        c_text.push_back(val);
    }

    for(int i=1;i<=25;i++){
        int key = i;

        string decryted_text="";
        for(int i=0;i<c_text.size();i++){
            int val = c_text[i] - key;
            int x;
            if(val<0){
                x = val+26;
            }else{
                x = val;
            }

            decryted_text+=char(x+65);
        }
        cout<<"The decrypted text for key "<<key<<" is:
"<<decryted_text<<endl;
    }

    // key = 9
```

```
    // A stich in nine saves time

}
```

Output –

```
PS C:\Users\arinr\Desktop\Crypto_Lab\Lab_5> cd "c:\Users\a
inr\Desktop\Crypto_Lab\Lab_5\" ; if ($?) { g++ Q2.cpp -o Q
 } ; if ($?) { .\Q2 }
The decrypted text for key 1 is: IABQBKPQVBQUMAIDMAVQVM
The decrypted text for key 2 is: HZAPAJOPUAPTLZHCLZUPUL
The decrypted text for key 3 is: GYZOZINOTZOSKYGBKYTOTK
The decrypted text for key 4 is: FXYNYHMNSYNRJXFAJXSNSJ
The decrypted text for key 5 is: EWXMXGLMRXMQIWEZIWRMRI
The decrypted text for key 6 is: DVWLWFKLQWLPHVDYHVQLQH
The decrypted text for key 7 is: CUVKVEJKPVKOGUCXGUPKPG
The decrypted text for key 8 is: BTUJUDIJOUJNFTBWFTOJOF
The decrypted text for key 9 is: ASTITCHINTIMESAVESNINE
The decrypted text for key 10 is: ZRSHSBGHMSHLDRZUDRMHMD
The decrypted text for key 11 is: YQRGRAFGLRGKCQYTCQLGLC
The decrypted text for key 12 is: XPQFQZEFKQFJBPXSBPKFKB
The decrypted text for key 13 is: WOPEPYDEJPEIAOWRAOJEJA
The decrypted text for key 14 is: VNODOXCDIODHZNVQZNIDIZ
The decrypted text for key 15 is: UMNCNWBCHNCGYMUPYMHCHY
The decrypted text for key 16 is: TLMBMVABGMBFXLTOXLGBGX
The decrypted text for key 17 is: SKLALUZAFLAEWKSNWKFAFW
The decrypted text for key 18 is: RJKZKTYZEKZDVJRMVJEZEV
The decrypted text for key 19 is: QIJYJSXYDJYCUIQLUIDYDU
The decrypted text for key 20 is: PHIXIRWXCIXBTHPKTHCXCT
The decrypted text for key 21 is: OGHWHQVWBHWASGOJSGBWBS
The decrypted text for key 22 is: NFGVGPUVAGVZRFNIRFAVAR
The decrypted text for key 23 is: MEFUFOTUZFUYQEMHQEZUZQ
The decrypted text for key 24 is: LDETENSTYETXPDLGPDYTYP
The decrypted text for key 25 is: KCDSDMRSXDSWOCKFOCXSXO
PS C:\Users\arinr\Desktop\Crypto_Lab\Lab_5>
```

The string that is most meaningful is for key value 9 i.e. “A stich in nine saves time”.

Q3. Implement Substitution Cipher.

A: *Pseudocode and Explanation –*

Firstly, we took the user input of the characters that he wants to replace with. The string is encrypted now using that vector of replaced characters.

Code –

```cpp
#include<bits/stdc++.h>
using namespace std;
int main()
{
    string s;
    cout<<"Enter the string: "<<endl;
    cin>>s;

    vector<char> subst;
    for(int i=0;i<26;i++){
        char ch;
        cout<<"Enter the letter that will be replaced with
"<<char(65+i)<<endl;
        cin>>ch;
        subst.push_back(ch);
    }
    // B C D E F G H I J K L M N O P Q R S T U V W X Y Z A

    string encrypted;
    for(int i=0;i<s.length();i++){
        int val = int(s[i]-65);
        encrypted+=subst[val];
    }

    cout<<encrypted;
}
```

Output –

```
PS C:\Users\arinr\Desktop\Crypto_Lab\Lab_5> cd "c:\Users\arinr\Desktop\Crypto_Lab\Lab_5\" ; if ($?) { g++ Q3.cpp -o Q3 } ; if ($?) {
.\Q3 }
Enter the string:
MYNAMEISARIN
Enter the replacement of each character starting from A:
B C D E F G H I J K L M N O P Q R S T U V W X Y Z A
Encrypted String: NZOBNFJTBSJO
PS C:\Users\arinr\Desktop\Crypto_Lab\Lab_5>
```

Q4. Implement the first question for input: “I TRANSFERRED RS2034 TO YOU”

A: *Pseudocode and Explanation –*

Firstly, I made a vector c_text that includes all the numbers and characters. In the next loop, using the same concept we will encrypt it using (x+key)modn.

Code –

```
#include<bits/stdc++.h>
using namespace std;
int main()
{
    int key;
    string s;
    cout<<"Enter the message: "<<endl;
    cin>>s;
    cout<<"Enter the key value: "<<endl;
    cin>>key;
    // cout<<s;
    vector<char> c_text={'0','1','2','3','4','5','6','7','8','9','A','B','C',
'D', 'E', 'F', 'G', 'H', 'I', 'J', 'K', 'L', 'M', 'N', 'O', 'P', 'Q', 'R',
'S', 'T', 'U' ,'V', 'W', 'X', 'Y', 'Z'};

    string encrypted_text="";
    for(int i=0;i<s.length();i++){
        char ch = s[i];
        int val;
        for(int j=0;j<c_text.size();j++){
            if(ch == c_text[j]){
                val = j;
            }
        }
        int x = (val+key)%36;
        char cp = c_text[x];
        encrypted_text.push_back(cp);
    }

    cout<<encrypted_text;

}
```

Output –

```
Enter the message:
ITRANSFERREDRS2034TOYOU
Enter the key value:
3
LWUDQVIHUUHGUV5367WR1RX
PS C:\Users\arinr\Desktop\Crypto_Lab\Lab_5>
```