**Information and Network Security**

**2CSDE54**

**Practical 1**

1. Perform encryption, decryption using the following substitution techniques
2. Caeser cipher
3. ROT-13

**CAESER CIPHER**

#include <bits/stdc++.h>

using namespace std;

string cc\_encrypt(string text, int key)

{

    char c;

    for (int i = 0; i < text.length(); i++)

    {

        c = text[i];

        if (isalpha(c))

        {

            if (islower(c))

            {

                c = (c - 'a' + key) % 26 + 'a';

            }

            if (isupper(c))

            {

                c = (c - 'A' + key) % 26 + 'A';

            }

        }

        text[i] = c;

    }

    return text;

}

string cc\_decrypt(string text, int key)

{

    char c;

    for (int i = 0; i < text.length(); i++)

    {

        c = text[i];

        if (isalpha(c))

        {

            if (islower(c))

            {

                c = (c - 'a' - key + 26) % 26 + 'a';

            }

            if (isupper(c))

            {

                c = (c - 'A' - key + 26) % 26 + 'A';

            }

        }

        text[i] = c;

    }

    return text;

}

int main()

{

    FILE \*ptr;

    fstream f;

    char ch;

    string s = "";

    string cipher\_text, plain\_text;

    ptr = fopen("input.txt", "r");

    f.open("output.txt", fstream::out);

    if (NULL == ptr)

    {

        printf("Cannot open\n");

    }

    printf("Plain text: \n");

    while (!feof(ptr))

    {

        ch = fgetc(ptr);

        s += ch;

        printf("%c", ch);

    }

    cout << "\n";

    int key;

    cout << "Enter key: \n";

    cin >> key;

    cout << cc\_encrypt(s, key);

    cipher\_text = cc\_encrypt(s, key);

    cout << "\nEncryption"

         << "\n"

         << "Cipher Text: " << cipher\_text;

    for (int i = 0; i < cipher\_text.length(); i++)

    {

        f << cipher\_text[i];

    }

    plain\_text = cc\_decrypt(cipher\_text, key);

    cout << "\nDecryption"

         << "\n"

         << "Plain Text: " << plain\_text;

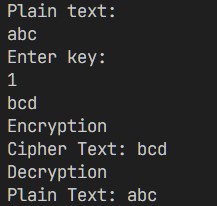
    f.close();

    fclose(ptr);

    return 0;

}

**O/P:**

****

**ROT CIPHER**

#include <bits/stdc++.h>

using namespace std;

string cc\_encrypt(string text, int key)

{

    char c;

    for (int i = 0; i < text.length(); i++)

    {

        c = text[i];

        if (isalpha(c))

        {

            if (islower(c))

            {

                c = (c - 'a' + key) % 26 + 'a';

            }

            if (isupper(c))

            {

                c = (c - 'A' + key) % 26 + 'A';

            }

        }

        text[i] = c;

    }

    return text;

}

string cc\_decrypt(string text, int key)

{

    char c;

    for (int i = 0; i < text.length(); i++)

    {

        c = text[i];

        if (isalpha(c))

        {

            if (islower(c))

            {

                c = (c - 'a' - key + 26) % 26 + 'a';

            }

            if (isupper(c))

            {

                c = (c - 'A' - key + 26) % 26 + 'A';

            }

        }

        text[i] = c;

    }

    return text;

}

int main()

{

    FILE \*ptr;

    fstream f;

    char ch;

    string s = "";

    string cipher\_text, plain\_text;

    ptr = fopen("input.txt", "r");

    f.open("output.txt", fstream::out);

    if (NULL == ptr)

    {

        printf("Cannot open\n");

    }

    printf("Plain text: \n");

    while (!feof(ptr))

    {

        ch = fgetc(ptr);

        s += ch;

        printf("%c", ch);

    }

    cout << "\n";

    int key;

    cout << "Enter key: \n";

    cin >> key;

    cout << cc\_encrypt(s, key);

    cipher\_text = cc\_encrypt(s, key);

    cout << "\nEncryption"

         << "\n"

         << "Cipher Text: " << cipher\_text;

    for (int i = 0; i < cipher\_text.length(); i++)

    {

        f << cipher\_text[i];

    }

    plain\_text = cc\_decrypt(cipher\_text, key);

    cout << "\nDecryption"

         << "\n"

         << "Plain Text: " << plain\_text;

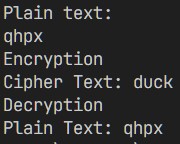
    f.close();

    fclose(ptr);

    return 0;

}

**O/P:**

****

**Questions**

1. Crack the following plaintext TRVJRI TZGYVIJ RIV HLZKV VRJP KF

TIRTB

Ans: Plain text = “CAESAR CIPHERS ARE QUITE EASY TO CRACK” and Key = “R”. “V” and “R” are the most common letters in the ciphertext.

2. What key do we need to make “CAESAR” become “MKOCKB”?

Ans: Key = “K”

3. What key do we need to make “CIPHER” become “SYFXUH”?

Ans: Key = “Q”

4. Use the Caesar cipher to encrypt your first name

Ans: Considering Key = 1,

First Name: AZIM

Last Name: BAJN

5. How can we find the decryption key from the encryption key?

Ans: Encryption and decryption keys occur in pairs.