

**U18CO018**  
**Shekhaliya Shubham**  
**CNS**  
**Lab Assignment 4**

Write a program to implement Vernam cipher

Code:

```
#include <bits/stdc++.h>

using namespace std;

string generateKey(int n) {
    string key = "";

    for(int i = 0;i<n;i++) {
        key += ((rand() % 26) + 'A');
    }

    return key;
}

int hex2Dec(char hex[]) {
    int len = strlen(hex);
    int base = 1;
    int dec = 0;

    for (int i = len - 1; i >= 0; i--) {
        if(hex[i] >= '0' && hex[i] <= '9') {
            dec += (hex[i] - '0') * base;
            base = base * 16;
        } else if (hex[i] >= 'a' && hex[i] <= 'f') {
            dec += (hex[i] - 'a' + 10) * base;
            base = base * 16;
        }
    }
    return dec;
}
```

```

string encrypt(string plainText, string key) {

    string cipherText = "";
    int n = plainText.length();

    char temp[8];

    for(int i = 0; i < n; i++) {
        int d = plainText[i]^key[i];

        itoa(d, temp, 16);

        if(strlen(temp) == 1) {
            cipherText += "0";
        }

        cipherText += temp;
        cipherText += " ";
    }

    return cipherText;
}

```

```

string decrypt(string cipherText, string key) {

    string plainText = "";
    int n = key.length();
    int p = 0;
    char hex[2];

    for(int i = 0; i < n; i++) {
        hex[0] = cipherText[p];
        hex[1] = cipherText[p + 1];
        int d = hex2Dec(hex);
        plainText += (key[i]^d);
        p += 3;
    }

    return plainText;
}

```

```

string readFrom(string filename)
{
    ifstream file;
    string input = "", result = "";
    file.open(filename);
    while (!file.eof())

```

```

    {
        getline(file, input);
        result += input + "\n";
    }
    file.close();
    return result.substr(0, result.length() - 1);
}

void writeTo(string filename, string message)
{
    ofstream file;
    file.open(filename);
    file << message;
    file.close();
}

int main() {

    int ch = 0;
    string key = "";

    while(true) {

        cout<<"1. Encryption\n";
        cout<<"2. Decryption\n";

        cin>>ch;

        if (ch == 1) {

            string plainText = readFrom("input.txt");
            key = generateKey(plainText.length());

            cout<<"PlainText : "<<plainText<<endl<<endl;

            cout<<"Randomly Generated Key : "<<key<<endl<<endl;

            string cipherText = encrypt(plainText, key);
            cout<<"CipherText : "<<cipherText<<endl<<endl;

            writeTo("output.txt", cipherText);

        } else if (ch == 2) {

            string cipherText = readFrom("output.txt");

            cout<<"CipherText : "<<cipherText<<endl<<endl;

```

```

        cout<<"Randomly Generated Key : "<<key<<endl<<endl;

        string plainText = decrypt(cipherText, key);
        cout<<"PlainText : "<<plainText<<endl<<endl;

        writeTo("output1.txt", plainText);

    } else {
        break;
    }
}

return 0;
}

```

Input.txt

hitherehopeyouaredoingwell

Output.txt

38 21 25 2f 2d 27 28 2d 2e 29 29 37 23 33 25 2a 23 2d 3d 2a 38 34 34 3d 2b 2b

```

E:\Asem7\CNS\Assignment4>g++ vernam.cpp
E:\Asem7\CNS\Assignment4>a.exe
1. Encryption
2. Decryption
1
PlainText : hitherehopeyouaredoingwell

Randomly Generated Key : PHQGHUMEAYLNLFDXFIRCVSCXGG

CipherText : 38 21 25 2f 2d 27 28 2d 2e 29 29 37 23 33 25 2a 23 2d 3d 2a 38 34 34 3d 2b 2b

1. Encryption
2. Decryption
2
CipherText : 38 21 25 2f 2d 27 28 2d 2e 29 29 37 23 33 25 2a 23 2d 3d 2a 38 34 34 3d 2b 2b

Randomly Generated Key : PHQGHUMEAYLNLFDXFIRCVSCXGG

PlainText : hitherehopeyouaredoingwell

1. Encryption
2. Decryption
3

```