Nithin S
221IT085

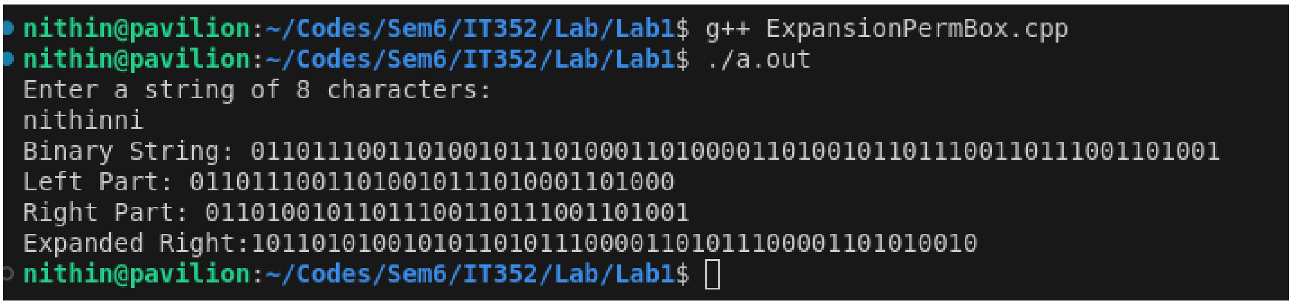
IT352 Lab Assignment 1

Q1. Use any one of the following programming languages Python/Java/C++/C to implement Expansion permutation box of Data Encryption Standard (DES). Your program should take runtime input (alphanumeric) then it should convert into binary then show the output step by step. Print all results (initial binary values block-by-block of 64 bits). Divide 64 bit block into two sub-blocks of 32 bits and apply expansion permutation on right block of 32 bit block. Print all intermediate values and also store them on text file (.txt). Do not use any library directly on your program

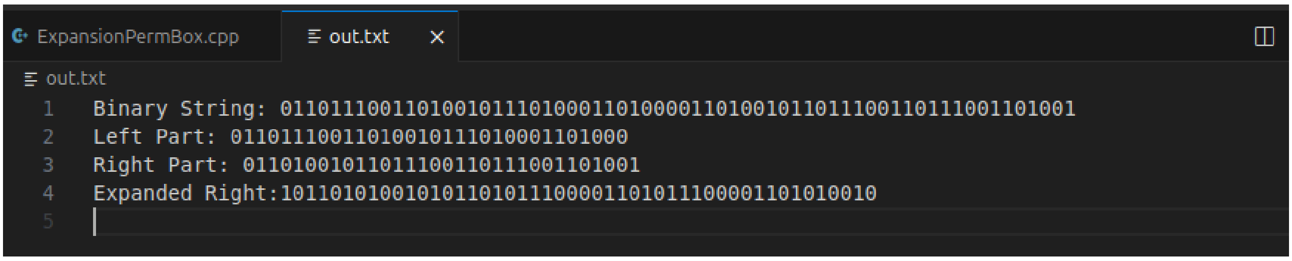
Code

```
#include<bits/stdc++.h>
using namespace std;

const vector<int>E_BOX{
    32,1,2,3,4,5,
    4,5,6,7,8,9,
    8,9,10,11,12,13,
    12,13,14,15,16,17,
    16,17,18,19,20,21,
    20,21,22,23,24,25,
    24,25,26,27,28,29,
    28,29,30,31,32,1
};
ofstream my_file("out.txt");

string convertToBin(string str){
    string res="";
    for(auto it:str){
        res+=bitset<8>(it).to_string();
    }
    my_file<<"Binary String: "<<res<<endl;
    cout<<"Binary String: "<<res<<endl;

    if (res.size() > 64) {
        return res.substr(0, 64);
    } else if (res.size() < 64) {
        return res + string(64 - res.size(), '0');
    }
    return res;
}

string expansion(string str){
    string left=str.substr(0,32);
    string right=str.substr(32,32);
    cout<<"Left Part: "<<left<<endl;
    my_file<<"Left Part: "<<left<<endl;
    cout<<"Right Part: "<<right<<endl;
    my_file<<"Right Part: "<<right<<endl;
    string expandedRight="";
    for(int i:E_BOX){
        expandedRight+=right[i-1];
    }
    return expandedRight;
}

int main(){
    string str;
    cout<<"Enter a string of 8 characters: "<<endl;
    cin>>str;
    string bstr=convertToBin(str);
    string expandedRight=expansion(bstr);
    cout<<"Expanded Right:"<<expandedRight<<endl;
    my_file<<"Expanded Right:"<<expandedRight<<endl;
    return 0;
}
```

Output



```
nithin@pavilion:~/Codes/Sem6/IT352/Lab/Lab1$ g++ ExpansionPermBox.cpp
nithin@pavilion:~/Codes/Sem6/IT352/Lab/Lab1$ ./a.out
Enter a string of 8 characters:
nithinni
Binary String: 0110111001101001011101000110100001101001011011100110111001101001
Left Part: 01101110011010010111010001101000
Right Part: 01101001011011100110111001101001
Expanded Right:101101010010101101011100001101011100001101010010
nithin@pavilion:~/Codes/Sem6/IT352/Lab/Lab1$ 
```



```
Binary String: 0110111001101001011101000110100001101001011011100110111001101001
Left Part: 01101110011010010111010001101000
Right Part: 01101001011011100110111001101001
Expanded Right:101101010010101101011100001101011100001101010010

```