

Program :

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

unsigned int sBox[8][4][16] = {
    {{14,4,13,1,2,15,11,8,3,10,6,12,5,9,0,7},
     {0,15,7,4,14,2,13,1,10,6,12,11,9,5,3,8},
     {4,1,14,8,13,6,2,11,15,12,9,7,3,10,5,0},
     {15,12,8,2,4,9,1,7,5,11,3,14,10,0,6,13}},

    {{15,1,8,14,6,11,3,4,9,7,2,13,12,0,5,10},
     {3,13,4,7,15,2,8,14,12,0,1,10,6,9,11,5},
     {0,14,7,11,10,4,13,1,5,8,12,6,9,3,2,15},
     {13,8,10,1,3,15,4,2,11,6,7,12,0,5,14,9}},

    {{10,0,9,14,6,3,15,5,1,13,12,7,11,4,2,8},
     {13,7,0,9,3,4,6,10,2,8,5,14,12,11,15,1},
     {13,6,4,9,8,15,3,0,11,1,2,12,5,10,14,7},
     {1,10,13,0,6,9,8,7,4,15,14,3,11,5,2,12}},

    {{7,13,14,3,0,6,9,10,1,2,8,5,11,12,4,15},
     {13,8,11,5,6,15,0,3,4,7,2,12,1,10,14,9},
     {10,6,9,0,12,11,7,13,15,1,3,14,5,2,8,4},
     {3,15,0,6,10,1,13,8,9,4,5,11,12,7,2,14}},

    {{2,12,4,1,7,10,11,6,8,5,3,15,13,0,14,9},
     {14,11,2,12,4,7,13,1,5,0,15,10,3,9,8,6},
     {4,2,1,11,10,13,7,8,15,9,12,5,6,3,0,14},
     {11,8,12,7,1,14,2,13,6,15,0,9,10,4,5,3}},

    {{12,1,10,15,9,2,6,8,0,13,3,4,14,7,5,11},
     {10,15,4,2,7,12,9,5,6,1,13,14,0,11,3,8},
     {9,14,15,5,2,8,12,3,7,0,4,10,1,13,11,6},
     {4,3,2,12,9,5,15,10,11,14,1,7,6,0,8,13}},

    {{4,11,2,14,15,0,8,13,3,12,9,7,5,10,6,1},
     {13,0,11,7,4,9,1,10,14,3,5,12,2,15,8,6},
     {1,4,11,13,12,3,7,14,10,15,6,8,0,5,9,2},
     {6,11,13,8,1,4,10,7,9,5,0,15,14,2,3,12}},

    {{13,2,8,4,6,15,11,1,10,9,3,14,5,0,12,7},
     {1,15,13,8,10,3,7,4,12,5,6,11,0,14,9,2},
     {7,11,4,1,9,12,14,2,0,6,10,13,15,3,5,8},
     {2,1,14,7,4,10,8,13,15,12,9,0,3,5,6,11}}
};

int PT[]={
    16, 7 , 20, 21, 29, 12, 28, 17,
    1 , 15, 23, 26, 5 , 18, 31, 10,
```

```

    2 , 8 , 24, 14, 32, 27, 3 , 9 ,
    19, 13, 30, 6 , 22, 11, 4 , 25
};

```

```

string permutate(string str)
{
    string res="";
    for(int i=0;i<32;i++)
        res+=str[PT[i]-1];
    return res;
}

```

```

int binToDec(string bin)
{
    int dec=0,n=bin.length();
    for(int i=0;i<n;i++)
        dec=dec*2+(bin[i]-48);
    return dec;
}

```

```

string decToBin(int dec)
{
    string binrev="",bin="0000";
    int i=4;
    while(dec>0)
    {
        bin[--i]=((dec%2)+48);
        dec/=2;
    }
    return bin;
}

```

```

string fnXor(string a,string b)
{
    string res="";
    for(int i=0;i<32;i++)
        res+=(a[i]==b[i])?'0':'1';
    return res;
}

```

```

int main()
{
    int i,j,row,col,val;
    string inputToSbox, outputOfFn="", rowBin="";
    string L,R,text,temp;
    ifstream fin("inputToSbox.txt");
    fin>>text>>inputToSbox;
    fin.close();
    cout<<"O/p of (i-1)th round (from file) : "<<endl<<text<<endl<<endl;
    cout<<"Input to SBox (from file): "<<inputToSbox<<endl<<endl;

    L=text.substr(0,32);
    R=text.substr(32,32);
}

```

```

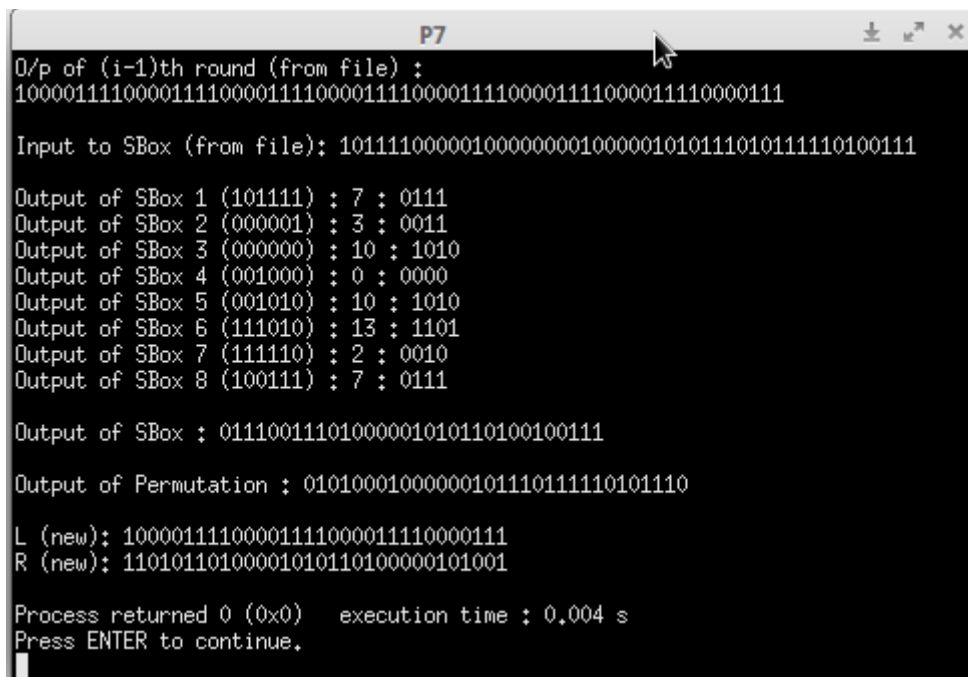
for(i=0;i<48;i+=6)
{
    rowBin=inputToSbox[i];
    rowBin+=inputToSbox[i+5];
    row=binToDec(rowBin);
    col=binToDec(inputToSbox.substr(i+1,4));
    val=sBox[j][row][col];
    outputOfFn+=decToBin(val);
    cout<<"Output of SBox "<<j+1<<" ("<<inputToSbox.substr(i,6)<<") : "<<val<<" :
"<<decToBin(val)<<endl;
    j++;
} cout<<endl;

cout<<"Output of SBox : "<<outputOfFn<<endl<<endl;
outputOfFn=permutate(outputOfFn);
cout<<"Output of Permutation : "<<outputOfFn<<endl<<endl;
temp=R;
R=fnXor(L,outputOfFn);
L=temp;

cout<<"L (new): "<<L<<endl;
cout<<"R (new): "<<R<<endl;
return 0;
}

```

Output :



```

P7
O/p of (i-1)th round (from file) :
1000011110000111100001111000011110000111100001111000011110000111

Input to SBox (from file): 1011100000100000000100000101011101011110100111

Output of SBox 1 (101111) : 7 : 0111
Output of SBox 2 (000001) : 3 : 0011
Output of SBox 3 (000000) : 10 : 1010
Output of SBox 4 (001000) : 0 : 0000
Output of SBox 5 (001010) : 10 : 1010
Output of SBox 6 (111010) : 13 : 1101
Output of SBox 7 (111110) : 2 : 0010
Output of SBox 8 (100111) : 7 : 0111

Output of SBox : 01110011101000001010110100100111

Output of Permutation : 01010001000000101110111110101110

L (new): 10000111100001111000011110000111
R (new): 11010110100001010110100000101001

Process returned 0 (0x0)   execution time : 0.004 s
Press ENTER to continue.

```