

### **Program :**

```
#include <iostream>
#include <bits/stdc++.h>
#include <fstream>
using namespace std;
int expPerm[]={
    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
};

int main()
{
    unsigned long long inputhex;
    string input,key,R,inputToSbox="";
    ifstream fin("keys.txt");
    int i=0,n;

    cout<<"Enter key number : ";cin>>n;
    while( i<n && getline(fin,key) ) { i++; }
    cout<<"Key Taken : "<<key<<endl<<endl;
    fin.close();

    cout<<"Enter input string (hex): "; cin>>hex>>inputhex;
    input= bitset<64>(inputhex).to_string() ;
    cout<<"Binary Representation of input :\n"<<input<<endl;
    R=input.substr(32,32);

    //Apply Expansion Permutation && XOR with key
    for(int i=0;i<48;i++)
        inputToSbox+=(key[i]!=R[expPerm[i]-1])?'1':'0'; //XOR
    cout<<"Input to S-box : "<<inputToSbox<<endl;
    return 0;
}
```

**Output :**

```
P6
Enter key number : 3
Key Taken : 010101011111111100100010100100001011001111110011001

Enter input string (hex): 87878787878787
Binary Representation of input :
100001111100001111100001111100001111100001111100001111100001111

Input to S-box : 100101010000000010000101100000100011001110010110

Process returned 0 (0x0)   execution time : 6.120 s
Press ENTER to continue.
█
```