

### **Program :**

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

int PC1[] = {
    57, 49, 41, 33, 25, 17, 9,
    1, 58, 50, 42, 34, 26, 18,
    10, 2, 59, 51, 43, 35, 27,
    19, 11, 3, 60, 52, 44, 36,
    63, 55, 47, 39, 31, 23, 15,
    7, 62, 54, 46, 38, 30, 22,
    14, 6, 61, 53, 45, 37, 29,
    21, 13, 5, 28, 20, 12, 4};

int PC2[] = {
    14, 17, 11, 24, 1, 5, 3, 28,
    15, 6, 21, 10, 23, 19, 12, 4,
    26, 8, 16, 7, 27, 20, 13, 2,
    41, 52, 31, 37, 47, 55, 30, 40,
    51, 45, 33, 48, 44, 49, 39, 56,
    34, 53, 46, 42, 50, 36, 29, 32};

int shiftTable[] = {1, 1, 2, 2, 2, 2, 2, 2, 1, 2, 2, 2, 2, 2, 2, 1};

string compPC1(string key)
{
    string res="";
    for(int i=0;i<56;i++)
        res+=key[PC1[i]-1];
    return res;
}

string compPC2(string key)
{
    string res="";
    for(int i=0;i<48;i++)
        res+=key[PC2[i]-1];
    return res;
}

int main()
{
    ofstream fout("keys.txt");
    unsigned long long hexkey=0x133457799bbcdff1;
    string C,D;
    cout<<"Enter 64 bit key (in hex) : " ;cin>>hex>>hexkey;
    // Convert hex to bin
    string key=bitset<64>(hexkey).to_string() ;
    // Compute PC1
    key=compPC1(key);
```

```

C=key.substr(0,28) , D=key.substr(28,28);
for(int i=0;i<16;i++)
{
    //Left Shift
    C=C.substr(shiftTable[i],28-shiftTable[i]) + C.substr(0,shiftTable[i]);
    D=D.substr(shiftTable[i],28-shiftTable[i]) + D.substr(0,shiftTable[i]);
    // Compute PC2
    key=compPC2(C+D);
    cout<<"Key "<<i+1<<" : "<<key<<endl;
    fout<<key<<endl;
}
fout.close();
return 0;
}

```

### Output :

```

P5
Enter 64 bit key (in hex) : 133457799bbcdff1
Key 1 : 0001101100000010111011111111000111000001110010
Key 2 : 011110011010111011011001110110111100100111100101
Key 3 : 01010101111111110010001010010000101100111110011001
Key 4 : 011100101010110111010110110110011010100011101
Key 5 : 011111001110110000000111111010110101001110101000
Key 6 : 0110001110100101001111110010100000111101100101111
Key 7 : 11101100100001001011011111101100001100010111100
Key 8 : 11110111100010100011101011000001001110111111011
Key 9 : 111000001101101111101011111011011110011110000001
Key 10 : 101100011111001101000111101110100100011001001111
Key 11 : 001000010101111111010011110111101101001110000110
Key 12 : 011101010111000111110101100101000110011111101001
Key 13 : 100101111100010111010001111110101011101001000001
Key 14 : 01011111010000111011011111100101110011100111010
Key 15 : 101111111001000110001101001111010011111100001010
Key 16 : 11001011001111011000101100001110000101111110101

Process returned 0 (0x0)   execution time : 11.893 s
Press ENTER to continue.

```