

main.cpp

```
1  #include <iostream>
2  #include <string>
3  using namespace std;
4  string round_keys[16];
5  string shift_left_once(string key_chunk){
6      string shifted="";
7      for(int i = 1; i < 28; i++){
8          shifted += key_chunk[i];
9      }
10     shifted += key_chunk[0];
11     return shifted;
12 }
13 string shift_left_twice(string key_chunk){
14     string shifted="";
15     for(int i = 0; i < 2; i++){
16         for(int j = 1; j < 28; j++){
17             shifted += key_chunk[j];
18         }
19         shifted += key_chunk[0];
20         key_chunk= shifted;
21         shifted = "";
22     }
23     return key_chunk;
24 }
25 void generate_keys(string key){
26     int pc1[56] = {
27         57,49,41,33,25,17,9,
28         1,58,50,42,34,26,18,
29         10,2,59,51,43,35,27,
30         19,11,3,60,52,44,36,
31         23,15,7,28,20,12,4,
32     };
33 };
34 int pc2[48] = {
35     14,17,11,24,1,5,
36     3,28,15,6,21,10,
37     23,19,12,4,26,8,
38     16,7,27,20,13,2,
39     41,52,31,37,47,55,
40     30,40,51,45,33,48,
41     44,49,39,56,34,53,
42     46,42,50,36,29,32
43 };
44 };
45 // 1. Compressing the key using the PC1 table
46 string perm_key = "";
47 for(int i = 0; i < 56; i++){
48     perm_key+= key[pc1[i]-1];
49 }
50 // 2. Dividing the result into two equal halves
51 string left= perm_key.substr(0, 28);
52 string right= perm_key.substr(28, 28);
53 // Generating 16 keys
54 for(int i=0; i<16; i++){
55     if(i == 0 || i == 1 || i==8 || i==15 ){
56         left= shift_left_once(left);
57         right= shift_left_once(right);
58     }
59     else{
60         left= shift_left_twice(left);
61         right= shift_left_twice(right);
62     }
63 }
```

```

51 // 2. Dividing the result into two equal halves
52 string left= perm_key.substr(0, 28);
53 string right= perm_key.substr(28, 28);
54 // Generating 16 keys
55 for(int i=0; i<16; i++){
56     if(i == 0 || i == 1 || i==8 || i==15 ){
57         left= shift_left_once(left);
58         right= shift_left_once(right);
59     }
60     else{
61         left= shift_left_twice(left);
62         right= shift_left_twice(right);
63     }
64     string combined_key = left + right;
65     string round_key = "";
66     for(int i = 0; i < 48; i++){
67         round_key += combined_key[pc2[i]-1];
68     }
69     round_keys[i] = round_key;
70     cout<<"Key "<<i+1<<": "<<round_keys[i]<<endl;
71 }
72 }
73 int main(){
74     string key = "10101010111011000010010001100000100111001101101100110011011101
75     "01101100110011011101";
76     cout<<"input key: "<<key<<endl;
77     cout<<"Genrated keys"<<endl;
78     generate_keys(key);
79 }
80

```

OUTPUT:

```

input key: 10101010111011000010010001100000100111001101101100110011011101
Genrated keys
Key 1: 000110010100110011010000011100101101111010001100
Key 2: 010001010110100001011000000110101011110011001110
Key 3: 000001101110110110100100101011001111010110110101
Key 4: 110110100010110100000011001010110110111011100011
Key 5: 011010011010011000101001111111101100100100010011
Key 6: 110000011001010010001110100001110100011101011110
Key 7: 011100001000101011010010110111011011001111000000
Key 8: 001101001111100000100010111100001100011001101101
Key 9: 100001001011101101000100011100111101110011001100
Key 10: 000000100111011001010111000010001011010110111111
Key 11: 011011010101010101100000101011110111110010100101
Key 12: 110000101100000111101001011010100100101111110011
Key 13: 100110011100001100010011100101111100100100011111
Key 14: 001001010001101110001011110001110001011111010000
Key 15: 001100110011000011000101110110011010001101101101
Key 16: 000110000001110001011101011101011100011001101101

```