Program: 6 **S- DES Key Generation**

Date:

**AIM**

**ALGORITHM**

**CODE**

#include <iostream>

using namespace std;

int P10[] = {2, 4, 1, 6, 3, 9, 0, 8, 7, 5};

int P8[]  = {5, 2, 6, 3, 7, 4, 9, 8};

string applyPermutation(string key10, int \*permutation, int length) {

    string result;

    for (int i=0; i<length; i++) {

        result.push\_back(key10[permutation[i]]);

    }

    return result;

}

void mergeTwo(string key1, string key2, string &result) {

    for (char c: key1) {

        result.push\_back(c);

    }

    for (char c: key2) {

        result.push\_back(c);

    }

}

void splitToTwo(string key, string &res1, string &res2) {

    int length = key.length();

    int half = length / 2;

    for (int i=0; i<length; i++) {

        if (i < half)

            res1.push\_back(key[i]);

        else

            res2.push\_back(key[i]);

    }

}

void leftShift(string &key, int count) {

    int l = key.length();

    int i, j;

    char extra[count];

    for (i=0; i<count; i++) {

        extra[i] = key[i];

    }

    for (i=count; i<l; i++) {

        key[i - count] = key[i];

    }

    j = 0;

    for (i=l-count; i<l; i++) {

        key[i] = extra[j];

        j++;

    }

}

int main() {

    string inputKey10;

    cout << "Enter 10 bit input key : ";

    cin >> inputKey10;

    inputKey10 = applyPermutation(inputKey10, P10, 10);

    string LS1res1;

    string LS1res2;

    splitToTwo(inputKey10, LS1res1, LS1res2);

    leftShift(LS1res1, 1);

    leftShift(LS1res2, 1);

    string merged1;

    mergeTwo(LS1res1, LS1res2, merged1);

    merged1 = applyPermutation(merged1, P8, 8);

    cout << "Key 1: "  << merged1 << endl;

    leftShift(LS1res1, 2);

    leftShift(LS1res2, 2);

    string merged2;

    mergeTwo(LS1res1, LS1res2, merged2);

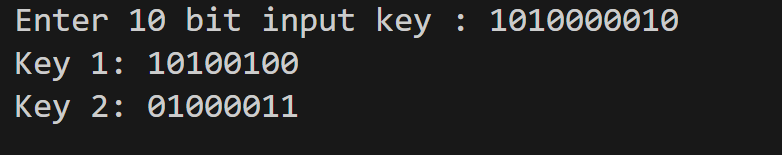
    merged2 = applyPermutation(merged2, P8, 8);

    cout << "Key 2: "  << merged2 << endl;

    return 0;

}

**OUTPUT**

****

**RESULT**

Thus, the program to generate 2 subkeys of 8 bits from a 10 bit input key is executed successfully.