Program-17 des algorithm in c

#include <stdint.h>

#include<stdio.h>

static const int IP[] = { 2, 6, 3, 1, 4, 8, 5, 7 };

static const int IP\_INV[] = { 4, 1, 3, 5, 7, 2, 8, 6 };

static const uint64\_t KEY = 0x133457799BBCDFF1;

static const uint64\_t CIPHERTEXT = 0x0123456789ABCDEF;

uint64\_t permute(uint64\_t input, const int \*table, int size) {

uint64\_t result = 0;

int i;

for (i = 0; i < size; i++) {

result |= ((input >> (64 - table[i])) & 1) << (size - 1 - i);

}

return result;

}

uint64\_t des\_decrypt(uint64\_t ciphertext, uint64\_t key) {

uint64\_t permuted\_ciphertext = permute(ciphertext, IP, 64);

uint64\_t decrypted = permuted\_ciphertext ^ key;

decrypted = permute(decrypted, IP\_INV, 64);

return decrypted;

}

int main() {

uint64\_t decrypted = des\_decrypt(CIPHERTEXT, KEY);

printf("Ciphertext: 0x%016llX\n", CIPHERTEXT);

printf("Decrypted: 0x%016llX\n", decrypted);

return 0;

}

Output:

