CSA5122-CRYPTOGRAPHY FOR NETWORK AND SECURITY

LAB PROGRAMS EXECUTION

7. TRIPLE DES ALGORITHM

#include <stdio.h>

#include <stdint.h>

int IP[64] = {

58,50,42,34,26,18,10,2, 60,52,44,36,28,20,12,4,

62,54,46,38,30,22,14,6, 64,56,48,40,32,24,16,8,

57,49,41,33,25,17,9,1, 59,51,43,35,27,19,11,3,

61,53,45,37,29,21,13,5, 63,55,47,39,31,23,15,7

};

int FP[64] = {

40,8,48,16,56,24,64,32, 39,7,47,15,55,23,63,31,

38,6,46,14,54,22,62,30, 37,5,45,13,53,21,61,29,

36,4,44,12,52,20,60,28, 35,3,43,11,51,19,59,27,

34,2,42,10,50,18,58,26, 33,1,41,9,49,17,57,25

};

uint64\_t permute(uint64\_t in, int\* table) {

uint64\_t out = 0;

for (int i = 0; i < 64; i++) {

out <<= 1;

out |= (in >> (64 - table[i])) & 1;

}

return out;

}

uint64\_t des(uint64\_t block, uint64\_t key) {

block = permute(block, IP);

uint32\_t L = block >> 32, R = block & 0xFFFFFFFF, temp;

for (int i = 0; i < 16; i++) {

temp = R;

R = L ^ (R ^ (uint32\_t)(key & 0xFFFFFFFF));

L = temp;

}

return permute(((uint64\_t)R << 32) | L, FP);

}

uint64\_t triple\_des(uint64\_t blk, uint64\_t k1, uint64\_t k2, uint64\_t k3, int dec) {

return dec ?

des(des(des(blk, k3), k2), k1) :

des(des(des(blk, k1), k2), k3);

}

int main() {

int choice;

uint64\_t msg, k1, k2, k3;

printf("Triple DES (3DES)\n1. Encrypt\n2. Decrypt\nChoose: ");

scanf("%d", &choice);

printf("Enter 16-digit hex message: ");

scanf("%llx", &msg);

printf("Enter 16-digit hex key1: ");

scanf("%llx", &k1);

printf("Enter 16-digit hex key2: ");

scanf("%llx", &k2);

printf("Enter 16-digit hex key3: ");

scanf("%llx", &k3);

uint64\_t res = triple\_des(msg, k1, k2, k3, choice == 2);

printf("%s: %016llX\n", choice == 1 ? "Encrypted" : "Decrypted", res);

return 0;

}

