Министерство образования и науки Украины

Харьковский национальный университет радиоэлектроники

Кафедра БИТ

Отчет

По лабораторной работе по MК

Тема «Освоение алгоритма построения таблиц разности и таблиц линейных

аппроксимаций для подстановок современных шифров»

Выполнили: Проверил:

ст.гр БИКСм-18-1 Руженцев В. И.

До Тхао

Харьков 2018

**1 Цель работы.**

На примере таблицы подстановки шифра rijndael (или любого другого современного шифра) освоить методику построения таблиц разностей и таблиц линейных аппроксимаций для нелинейных подстановок (S блоков) шифра.

**2 Код программа**

#include <iostream>

#include <bitset>

#include <stdio.h>

using namespace std;

typedef unsigned int uint;

typedef unsigned char uchar;

#define M 8

#define SIZE (1<<M)

const uchar Sbox[256] = {

0x63, 0x7c, 0x77, 0x7b, 0xf2, 0x6b, 0x6f, 0xc5, 0x30, 0x01, 0x67, 0x2b, 0xfe, 0xd7, 0xab, 0x76,

0xca, 0x82, 0xc9, 0x7d, 0xfa, 0x59, 0x47, 0xf0, 0xad, 0xd4, 0xa2, 0xaf, 0x9c, 0xa4, 0x72, 0xc0,

0xb7, 0xfd, 0x93, 0x26, 0x36, 0x3f, 0xf7, 0xcc, 0x34, 0xa5, 0xe5, 0xf1, 0x71, 0xd8, 0x31, 0x15,

0x04, 0xc7, 0x23, 0xc3, 0x18, 0x96, 0x05, 0x9a, 0x07, 0x12, 0x80, 0xe2, 0xeb, 0x27, 0xb2, 0x75,

0x09, 0x83, 0x2c, 0x1a, 0x1b, 0x6e, 0x5a, 0xa0, 0x52, 0x3b, 0xd6, 0xb3, 0x29, 0xe3, 0x2f, 0x84,

0x53, 0xd1, 0x00, 0xed, 0x20, 0xfc, 0xb1, 0x5b, 0x6a, 0xcb, 0xbe, 0x39, 0x4a, 0x4c, 0x58, 0xcf,

0xd0, 0xef, 0xaa, 0xfb, 0x43, 0x4d, 0x33, 0x85, 0x45, 0xf9, 0x02, 0x7f, 0x50, 0x3c, 0x9f, 0xa8,

0x51, 0xa3, 0x40, 0x8f, 0x92, 0x9d, 0x38, 0xf5, 0xbc, 0xb6, 0xda, 0x21, 0x10, 0xff, 0xf3, 0xd2,

0xcd, 0x0c, 0x13, 0xec, 0x5f, 0x97, 0x44, 0x17, 0xc4, 0xa7, 0x7e, 0x3d, 0x64, 0x5d, 0x19, 0x73,

0x60, 0x81, 0x4f, 0xdc, 0x22, 0x2a, 0x90, 0x88, 0x46, 0xee, 0xb8, 0x14, 0xde, 0x5e, 0x0b, 0xdb,

0xe0, 0x32, 0x3a, 0x0a, 0x49, 0x06, 0x24, 0x5c, 0xc2, 0xd3, 0xac, 0x62, 0x91, 0x95, 0xe4, 0x79,

0xe7, 0xc8, 0x37, 0x6d, 0x8d, 0xd5, 0x4e, 0xa9, 0x6c, 0x56, 0xf4, 0xea, 0x65, 0x7a, 0xae, 0x08,

0xba, 0x78, 0x25, 0x2e, 0x1c, 0xa6, 0xb4, 0xc6, 0xe8, 0xdd, 0x74, 0x1f, 0x4b, 0xbd, 0x8b, 0x8a,

0x70, 0x3e, 0xb5, 0x66, 0x48, 0x03, 0xf6, 0x0e, 0x61, 0x35, 0x57, 0xb9, 0x86, 0xc1, 0x1d, 0x9e,

0xe1, 0xf8, 0x98, 0x11, 0x69, 0xd9, 0x8e, 0x94, 0x9b, 0x1e, 0x87, 0xe9, 0xce, 0x55, 0x28, 0xdf,

0x8c, 0xa1, 0x89, 0x0d, 0xbf, 0xe6, 0x42, 0x68, 0x41, 0x99, 0x2d, 0x0f, 0xb0, 0x54, 0xbb, 0x16,

};

uchar popcount(uchar n) {

return std::bitset<CHAR\_BIT \* sizeof n>(n).count();

}

//es[a][b] = #{c in GF(2\*\*m) | S(c xor a) xor S(c) = b}

float DiffCryptAnalys(int es[SIZE][SIZE])

{

uint a, b, c, max = 0;

es[0][0] = SIZE;

for (a = 1; a < SIZE; a++) {

for (c = 0; c < SIZE; c++) {

b = Sbox[a ^ c] ^ Sbox[c];

es[a][b] += 1;

max = (max < es[a][b]) ? es[a][b] : max;

}

}

cout << "maxes = " << max << endl;

return (float)max / SIZE;

}

//cs[a][b] = #{x in GF(2\*\*m) | (W(x & a) + W(S(x) & b)) mod 2 == 0} - 2\*\*(m-1)

float LineCryptAnalys(int cs[SIZE][SIZE])

{

uint a, b, x, tmp;

int max = -(SIZE >> 1);

cs[0][0] = SIZE >> 1;

for (a = 1; a < SIZE; a++) {

for (b = 1; b < SIZE; b++) {

cs[a][b] -= SIZE >> 1;

for (x = 0; x < SIZE; x++) {

tmp = popcount(x & a) + popcount(Sbox[x] & b);

if (!(tmp & 1)) cs[a][b]++;

max = (max < cs[a][b]) ? cs[a][b] : max;

}

}

}

cout << "maxcs = " << max << endl;

return (float)max\*max / (1 << (2 \* (M - 1)));

}

void printTable(int es[SIZE][SIZE])

{

const int sub = 16;

for (int i = sub, a; i <= SIZE; i += sub) {

for (int j = sub, b = 0; j <= SIZE; j += sub) {

printf(" |");

for (b = j - sub; b < j; b++) printf(" %2X", b);

cout << endl;

printf("\_\_\_|");

for (b = j - sub; b < j; b++) printf("\_\_\_");

cout << endl;

for (a = i - sub; a < i; a++) {

printf("%2X |", a);

for (b = j - sub; b < j; b++)

printf(" %2d", es[a][b]);

cout << endl;

}

cout << endl;

}

cout << endl << endl;

}

}

int main()

{

int es[SIZE][SIZE] = { 0 };

int cs[SIZE][SIZE] = { 0 };

float pDmax, pLmax;

pDmax = DiffCryptAnalys(es);

pLmax = LineCryptAnalys(cs);

//printTable(es);

//printTable(cs);

printf("pDmax = %f\n", pDmax);

printf("pLmax = %f\n", pLmax);

system("pause");

return 0;

}

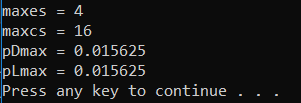
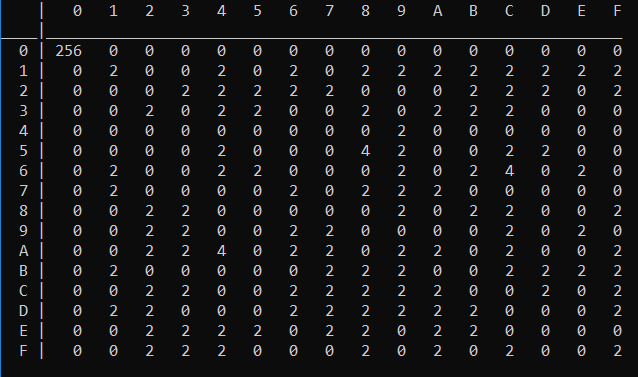
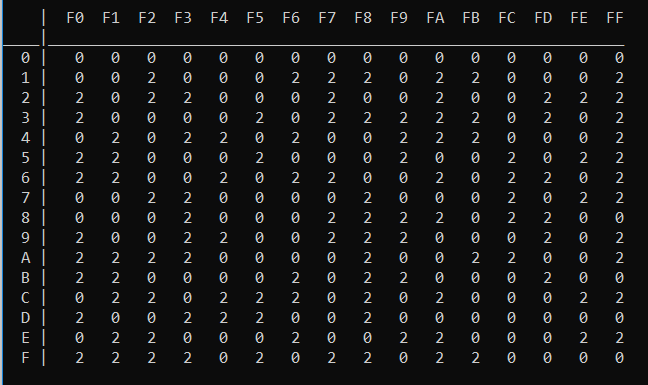


Таблица разности S-блока:

 .... 

................................................................................

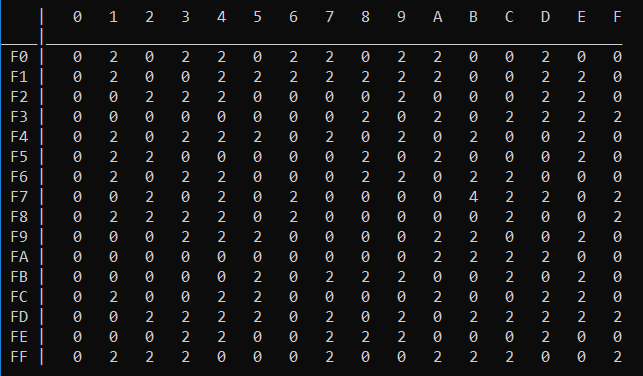
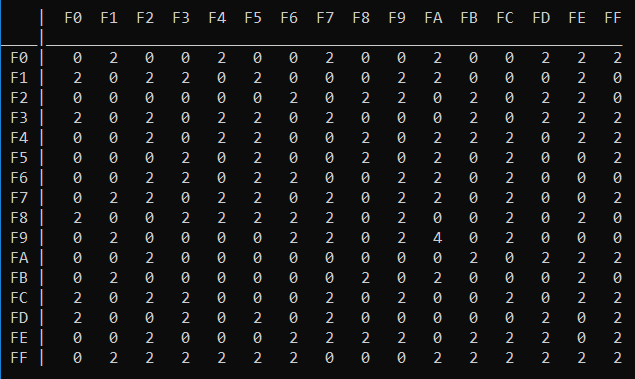
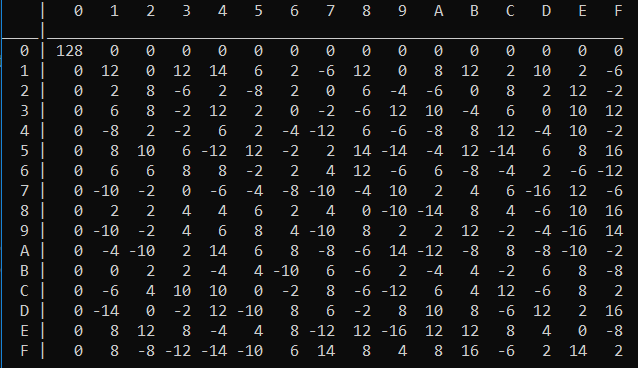
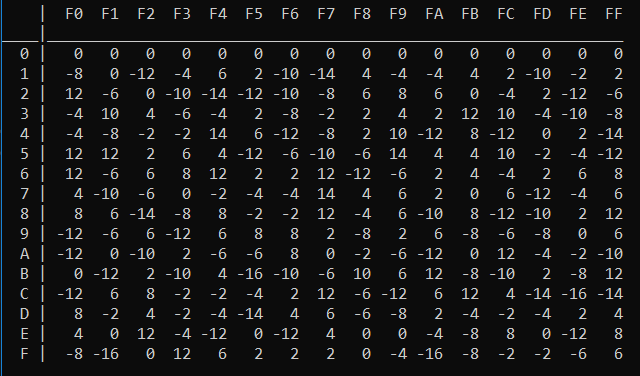
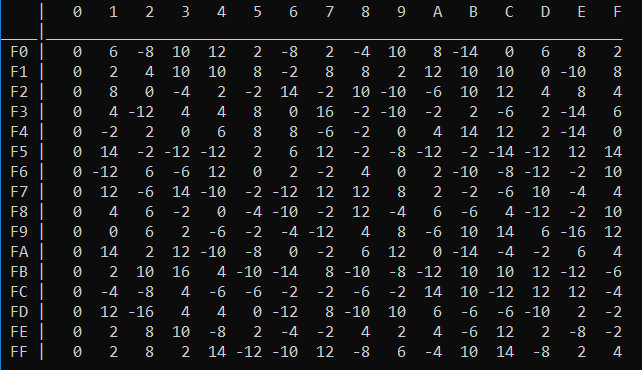
 ... 

Таблица линейных апроксімацій:

 ... 

...................................................................................

 ... 