

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТІРЛІГІ
ӘЛ-ФАРАБИ АТЫНДАҒЫ ҚАЗАҚ ҰЛТТЫҚ УНИВЕРСИТЕТІ
МЕХАНИКО-МАТЕМАТИКА ФАКУЛЬТЕТІ
АҚПАРАТТЫҚ ЖҮЙЕЛЕР КАФЕДРАСЫ

ДИПЛОМДЫҚ ЖҰМЫС

ТАҚЫРЫБЫ:

БЛОКТЫҚ ШИФРЛАР ҮШІН ДИФФЕРЕНЦИАЛДЫҚ
КРИПТОТАЛДАУ ТӘСІЛДЕРІМЕН ОРНЫҚТЫЛЫҚТЫ ЗЕРТТЕУ

Орындаған: Әбдәлімова А.Е

Топ: АЖ 13 – 2в

Ғылыми жетекшісі: Мусиралиева Ш.Ж
ф.-м.ғ.к., АЖ кафедрасының доцент қ.а.

МАҚСАТЫ

2

Дипломдық жұмыстың мақсаты:

- блоктік шифрлі алгоритмдерді дифференциалдық криптоталдау әдісі арқылы зерттеу;
- алгоритмге криптоталдау жасайтын және жасырын кілтті табатын программаны жүзеге асыру.

ҒЫЛЫМИ ЖАҢАЛЫҒЫ

3

Дипломдық жұмыстың ғылыми жаңалығы:

- блоктық шифрлау алгоритмдерінің құрамына кіретін криптографиялық әдістер қарастырылды;
- дифференциалдық криптоталдау әдісіне негізделген мәтінді шифрлау мен дешифрлау кезінде қолданылатын кілтті іздеу программасы жасалды.

БЛОКТИК ШИФРЛАР

Блоктық шифрлеу кезінде бастапқы мәтіннің ұзындығы тұрақты бекітілген блоктарға бөлінеді. Блоктың мәтіндері бір-біріне қатыссыз бөлек-бөлек шифрланады. Шифрлау үшін барлық блоктарға бір ғана кілт қолданылады. Шифрлаудің үш тәсілі бар, олар: ауыстыру, орын алмастыру, құрастырма шифрлар.

КРИПТОТАЛДАУ

Криптоталдау (грек тілінен аударғанда *kryptos* – «жасырын» және *analein* – «әлсірету немесе құтылу») деп ашық мәтінді кілтке қолжетімділіксіз қалыпқа келтіру ғылымын айтады. Криптоталдаудың даму тарихы ұзақ ғасырларды қамтыса да, нағыз қарқынды даму кезеңі компьютерлік дәуірдің келуімен басталды деп айтуға болады.

ДИФФЕРЕНЦИАЛДЫҚ КРИПТОТАЛДАУ

6

Дифференциалдық криптоталдау әдісін 1990 жылы израильдік зерттеушілер Эли Бихам және Ади Шамир ойлап тапты. Дифференциалдық криптоталдау – бұл криптожүйелердің белгілі бір класстарын бұзу тәсілі болып табылады. Дифференциалдық криптоталдау әдісінің негізі ашық мәтін мен шифрмәтін арасындағы дифференциалдық айырымды қолданудан тұрады.

ПРОГРАММАНЫ ҚҰРУ ЖӘНЕ ОНЫ СИПАТТАУ

7

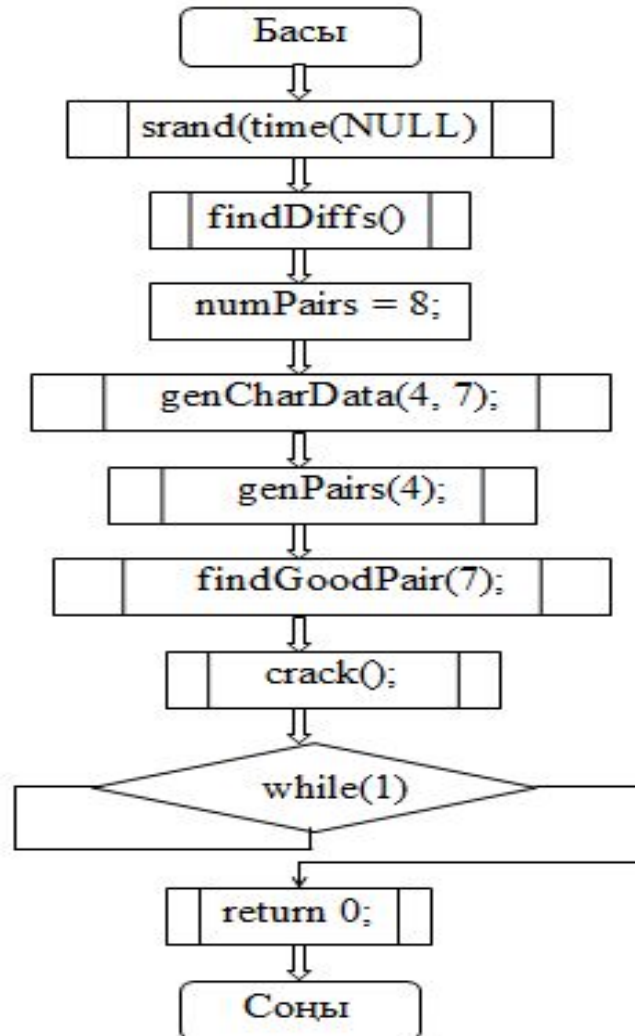
Программа C тілінде жазылған. Программаны құру кезінде қолданылған бағдарламалар:

- DEV-C++;
- C++ Builder.

Программа таңдалған сипаттамға (4□7) барлық мүмкін кіріс мәндерін/шығыс мәндерін көрсететін және аз уақыт ішінде кілтті қалпына келтіретін дифференциалды сипаттамаларды есептеп береді.

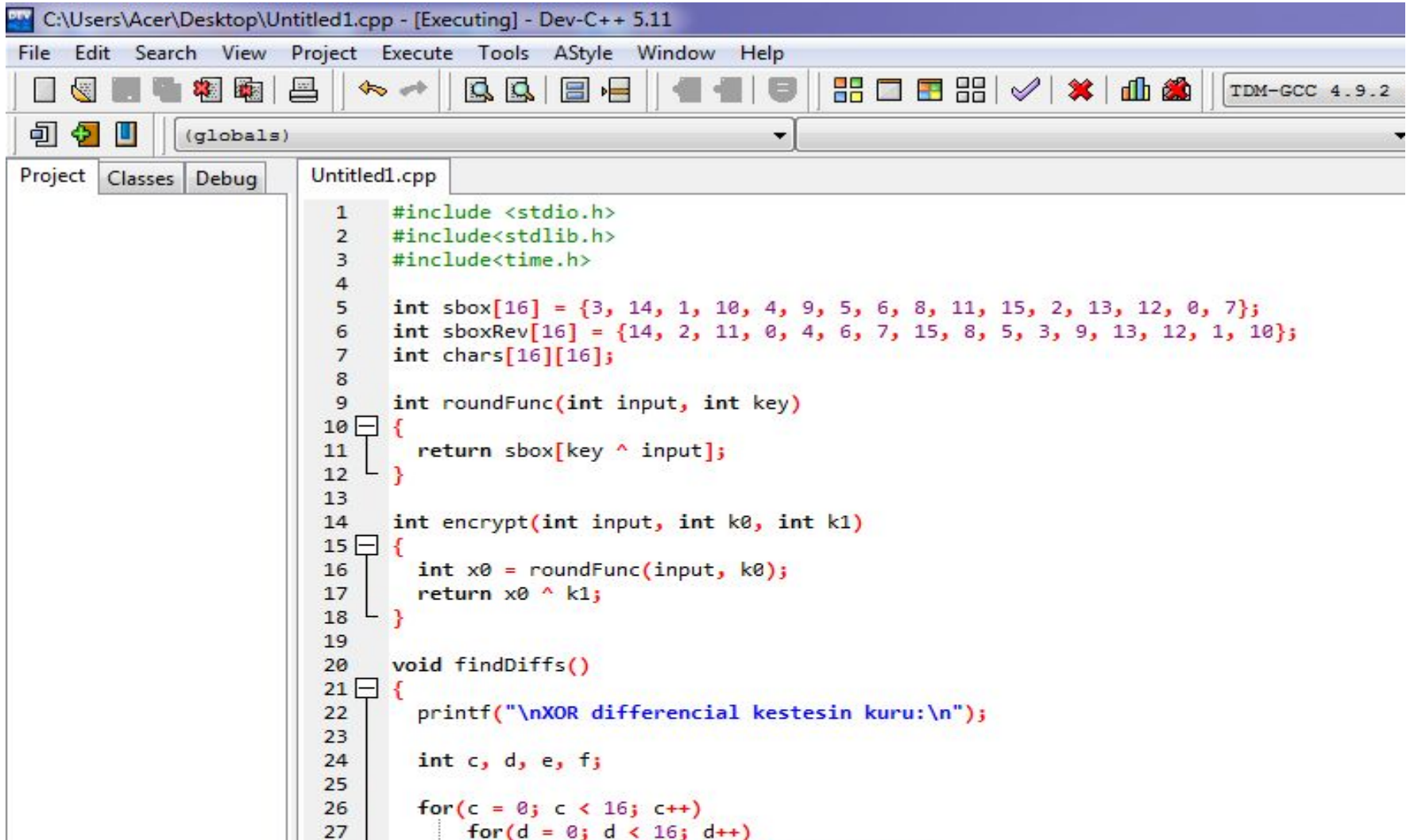
Программаның блок схемасы

8



Программа коды

9



The screenshot shows the Dev-C++ IDE interface. The title bar reads "C:\Users\Acer\Desktop\Untitled1.cpp - [Executing] - Dev-C++ 5.11". The menu bar includes File, Edit, Search, View, Project, Execute, Tools, AStyle, Window, and Help. The toolbar contains various icons for file operations and execution. The status bar at the bottom right indicates "TDM-GCC 4.9.2". The main editor window displays the following C++ code:

```
1  #include <stdio.h>
2  #include<stdlib.h>
3  #include<time.h>
4
5  int sbox[16] = {3, 14, 1, 10, 4, 9, 5, 6, 8, 11, 15, 2, 13, 12, 0, 7};
6  int sboxRev[16] = {14, 2, 11, 0, 4, 6, 7, 15, 8, 5, 3, 9, 13, 12, 1, 10};
7  int chars[16][16];
8
9  int roundFunc(int input, int key)
10 {
11     return sbox[key ^ input];
12 }
13
14 int encrypt(int input, int k0, int k1)
15 {
16     int x0 = roundFunc(input, k0);
17     return x0 ^ k1;
18 }
19
20 void findDiffs()
21 {
22     printf("\nXOR differential kestesin kuru:\n");
23
24     int c, d, e, f;
25
26     for(c = 0; c < 16; c++)
27         for(d = 0; d < 16; d++)
```

Программа коды

10

```
28     | | chars[c ^ d][sbox[c] ^ sbox[d]]++;
29
30     | for(c = 0; c < 16; c++)
31     | {
32     |     | for(d = 0; d < 16; d++)
33     |     |     | printf(" %x ", chars[c][d]);
34     |     |     | printf("\n");
35     |     | }
36
37     | printf("\nYktimaldylygy jogary differencialdardy korsetu:\n");
38
39     | for(c = 0; c < 16; c++)
40     |     | for(d = 0; d < 16; d++)
41     |     |     | if (chars[c][d] == 6)
42     |     |     |     | printf(" 6/16: %i -> %i\n", c, d);
43     |     | }
44
45     | int knownP0[10000];
46     | int knownP1[10000];
47     | int knownC0[10000];
48     | int knownC1[10000];
49
50     | int goodP0, goodP1, goodC0, goodC1;
51
52     | int numPairs;
53
54
55     | int chardat0[16];
56     | int chardatmax = 0;
57
58     | void genCharData(int indiff, int outdiff)
59     | {
60     |     | printf("\nDifferencial negizinde aralyk mumkin manderdi generaciyalau(%i -> %i):\n", indiff, outdiff);
61     |
62     |     | chardatmax = 0;
63     |     | int f;
64     |     | for(f = 0; f < 16; f++)
```

Программа коды

11

```
65     {
66         int myComp = f ^ indiff;
67
68         if ((sbox[f] ^ sbox[myComp]) == outdiff)
69         {
70             printf(" Mumkin bolgan: %i + %i -> %i + %i\n", f, myComp, sbox[f], sbox[myComp]);
71             chardat0[chardatmax] = f;
72             chardatmax++;
73         }
74     }
75 }
76
77 void genPairs(int indiff)
78 {
79     printf("\nGeneraciyalau %i belgili kiris differencial juptyary %i.\n", numPairs, indiff);
80
81     int realk0 = rand() % 16;
82     int realk1 = rand() % 16;
83
84     printf(" Nakty K0 = %i\n", realk0);
85     printf(" Nakty K1 = %i\n", realk1);
86
87     int c;
88     for(c = 0; c < numPairs; c++)
89     {
90         knownP0[c] = rand() % 16;
91         knownP1[c] = knownP0[c] ^ indiff;
92         knownC0[c] = encrypt(knownP0[c], realk0, realk1);
93         knownC1[c] = encrypt(knownP1[c], realk0, realk1);
94     }
95 }
96
97 void findGoodPair(int outdiff)
98 {
99     printf("\nJaksy jupty izdeu:\n");
```

Программа коды

12

```
100     int c;
101     for(c = 0; c < numPairs; c++)
102         if ((knownC0[c] ^ knownC1[c]) == outdiff)
103             {
104                 goodC0 = knownC0[c];
105                 goodC1 = knownC1[c];
106                 goodP0 = knownP0[c];
107                 goodP1 = knownP1[c];
108                 printf(" JAKSY JUPTY IZDEU: (P0 = %i, P1 = %i) -> (C0 = %i, C1 = %i)\n", goodP0, goodP1, goodC0, goodC1);
109                 return;
110             }
111     printf("JAKSY JUP TABYLGAN JOK!\n");
112 }
113
114 int testKey(int testK0, int testK1)
115 {
116     int c;
117     int crap = 0;
118     for(c = 0; c < numPairs; c++)
119     {
120         if ((encrypt(knownP0[c], testK0, testK1) != knownC0[c]) || (encrypt(knownP1[c], testK0, testK1) != knownC1[c]))
121             {
122                 crap = 1;
123                 break;
124             }
125     }
126
127     if (crap == 0)
128         return 1;
129     else
130         return 0;
131 }
132
133 void crack()
134 {
135     printf("\nBatyrmalardyn ornyn aldyn ala kyskartu:\n");
```

Программа коды

13

```
136
137
138 int f;
139 for(f = 0; f < chardatmax; f++)
140 {
141     int testK0 = chardat0[f] ^ goodP0;
142     int testK1 = sbox[chardat0[f]] ^ goodC0;
143
144     if (testKey(testK0, testK1) == 1)
145         printf(" KILT! (%i, %i)\n", testK0, testK1);
146     else
147         printf(" (%i, %i)\n", testK0, testK1);
148 }
149
150 int main()
151 {
152     srand(time(NULL));
153
154     findDiffs();
155
156     numPairs = 8;
157
158     genCharData(4, 7);
159     genPairs(4);
160     findGoodPair(7);
161     crack();
162
163     while(1){}
164     return 0;
165 }
166
```

Sel: 0

Lines: 166

Length: 3856

Insert

Done parsing in 0,156 seconds

Программа нәтижесі

14

```
XOR differential keskesin kuru:
10 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
0 2 0 4 0 0 0 2 0 0 2 0 6 0 0
0 2 2 0 2 0 0 2 0 2 0 2 2 0 2
0 0 2 0 2 0 0 0 0 2 4 0 4 0 2
0 0 0 0 2 4 6 0 0 0 0 2 0 0 2
0 0 2 0 2 2 2 2 4 0 0 0 2 0 2
0 0 0 2 2 0 2 2 0 4 0 0 2 0 2
0 0 0 2 2 0 2 2 0 0 4 0 0 2 4
0 0 2 2 2 2 4 0 4 2 0 0 0 0 0
0 2 0 0 2 0 0 0 2 2 2 4 0 2 0
0 4 2 2 0 0 0 0 0 4 2 2 0 0 0
0 2 4 0 2 0 0 0 0 0 2 2 0 2 4
0 2 0 2 0 0 2 2 0 2 2 0 0 0 4
0 0 0 2 0 0 2 0 0 2 4 2 4 0 0
0 0 0 0 2 0 4 2 0 0 0 2 6 0 0

Yktimaldylygy jogary differentialdardy korsetu:
6/16: 1 -> 13
6/16: 4 -> 7
6/16: 8 -> 5
6/16: 15 -> 14

Differential negizinde aralyk mumkin manderdi generaciyalau<4 -> 7>:
Mumkin bolgan: 0 + 4 -> 3 + 4
Mumkin bolgan: 1 + 5 -> 14 + 9
Mumkin bolgan: 4 + 0 -> 4 + 3
Mumkin bolgan: 5 + 1 -> 9 + 14
Mumkin bolgan: 9 + 13 -> 11 + 12
Mumkin bolgan: 13 + 9 -> 12 + 11

Generaciyalau 8 belgili kiris differential jupty 4.
Nakty K0 = 12
Nakty K1 = 14

Jaksy jupty izdeu:
JAKSY JUPTY IZDEU: <P0 = 5, P1 = 1> -> <C0 = 5, C1 = 2>

Batyrmalardyn ornyn aldyn ala kyskartu:
<5, 6>
<4, 11>
<1, 1>
<0, 12>
KILT! <12, 14>
<8, 9>
```

C++ Builder-де интерфейс қосылған программа нәтижесі

15

XOR шифрлеу алгоритмі

Мәзір Автор

Ықтималдылығы жоғары дифференциалдарды корсету
6/16: 1->13
6/16: 4->7
6/16: 8->5
6/16: 15->14
Дифференциал негизинде аралык мумкин маңдерди генерациялау 4->7
Мумкин болган:0+4->3+4
Мумкин болган:1+5->14+9
Мумкин болган:4+0->4+3
Мумкин болган:5+1->9+14
Мумкин болган:9+13->11+12
Мумкин болган:13+9->12+11
Генерациялау 8 белгілі кіріс дифференциал жұптары 4

Нақты K0 = 13
Нақты K1 = 15
Жаксы жұпты іздеу:
Жаксы жұпты іздеу: (P0 = 13 , P1 = 9)-> (C0 = 12 , C1 = 11)
Жаксы жұпты іздеу: (P0 = 12 , P1 = 8)-> (C0 = 1 , C1 = 6)
Жаксы жұпты іздеу: (P0 = 13 , P1 = 9)-> (C0 = 12 , C1 = 11)
Батырмалардын орынын алдын ала кыскарту:
КІЛТІ (13 , 15)
(12 , 2)
(9 , 8)
(8 , 5)
(4 , 7)
(0 , 0)

16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	2	2	0	0	0	0	0	2	0	2	4	2	2	0	0
0	0	2	2	0	2	2	0	0	2	0	2	4	0	0	0
0	4	0	0	0	0	2	2	0	2	0	2	0	2	2	0
0	0	2	2	2	2	0	0	0	2	2	0	2	0	0	2
0	0	0	0	4	0	2	2	6	2	0	0	0	0	0	0
0	0	0	0	0	2	2	0	0	4	0	0	0	2	2	4
0	2	2	0	6	2	0	0	0	0	0	0	0	2	0	2
0	0	0	0	0	2	4	2	2	4	2	0	0	0	0	0
0	0	2	2	0	0	0	0	2	0	2	4	0	2	2	0
0	0	0	4	0	4	0	0	0	0	2	2	2	2	0	0
0	2	2	0	0	0	0	4	2	0	0	2	0	0	4	0
0	0	0	4	2	0	2	0	0	0	4	0	2	0	2	0
0	6	2	0	0	0	0	0	0	0	0	0	2	0	4	2
0	0	0	0	0	0	2	2	2	0	2	0	2	0	0	6
0	0	2	2	2	2	0	4	0	0	0	0	0	4	0	0

XOR дифференциал кестесін құру

Бетті тазалау

НАЗАРЛАРЫҢЫЗҒА
РАХМЕТ