Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)

Лабораторная работа № 4

Изучение шифров DES, 3DES И Магма

Студент: _____ Чернякова Валерия, группа 1304

Руководитель: _____ Племянников А.К., доцент каф. ИБ

Санкт-Петербург 2024

Цель работы

Повысить компетенции в работе с методами симметричного шифрования: DES и его модификации, а также Магма. Исследовать на практике режимы работы данных шифров.

Задачи:

- Изучить преобразования DES
- Исследовать DES в режимах работы ECS и CBC
- Разработать схему в CrypTool 2 для определения версии 3DES, реализованной в CrypTool 2
- Изучить преобразования Магма
- Провести исследования Магма в режимах простой замены и простой замены с зацеплением

Шифр «DES»

Задание

1. Ручной расчет субблоков и раундовых ключей шифра для первого раунда. Сравнение с результатами демо-приложения.
2. Ручной расчет обратного преобразования шифровки.
3. Выбрать случайный текст на английском языке (не менее 1000 знаков) и зашифровать его DES в режиме ECB.
4. Для одного и того же шифротекста оценить время проведения атаки «грубой силы» в случаях, когда известно n – 4, n – 6, n – 8, ..., 2 байт секретного ключа. Зафиксировать результаты измерений в таблице.
5. Повторить подобные измерения для DES в режиме CBC.
6. Разработать схему в CrypTool 2 для экспериментального определения всех версий 3-DES, реализованных в Cryptool 2

Исходные данные

Открытый текст (не более 64 бит):

M = chernyak

Ключ (64 бит):

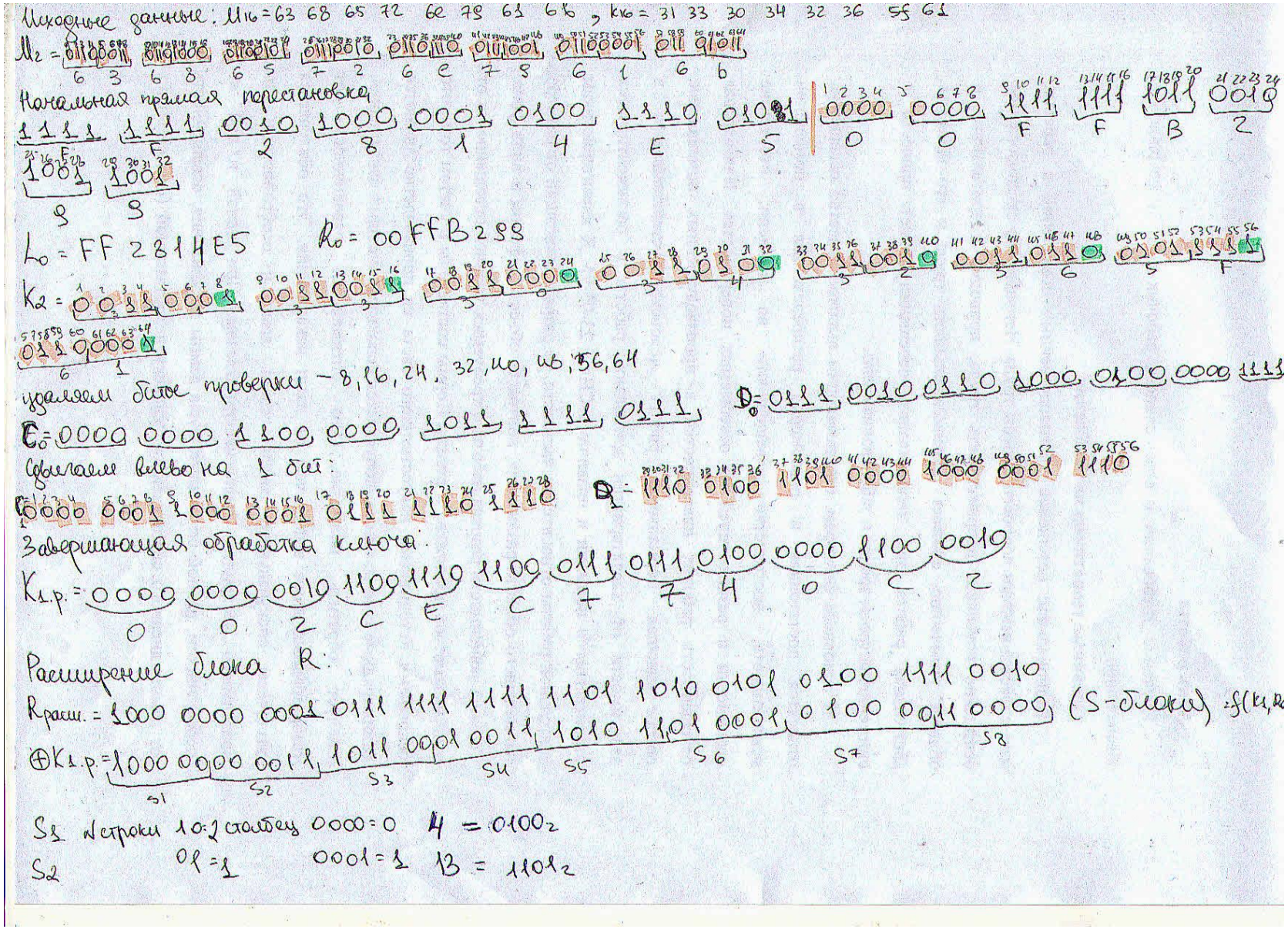
K = 130426_a

Байтовое представление:

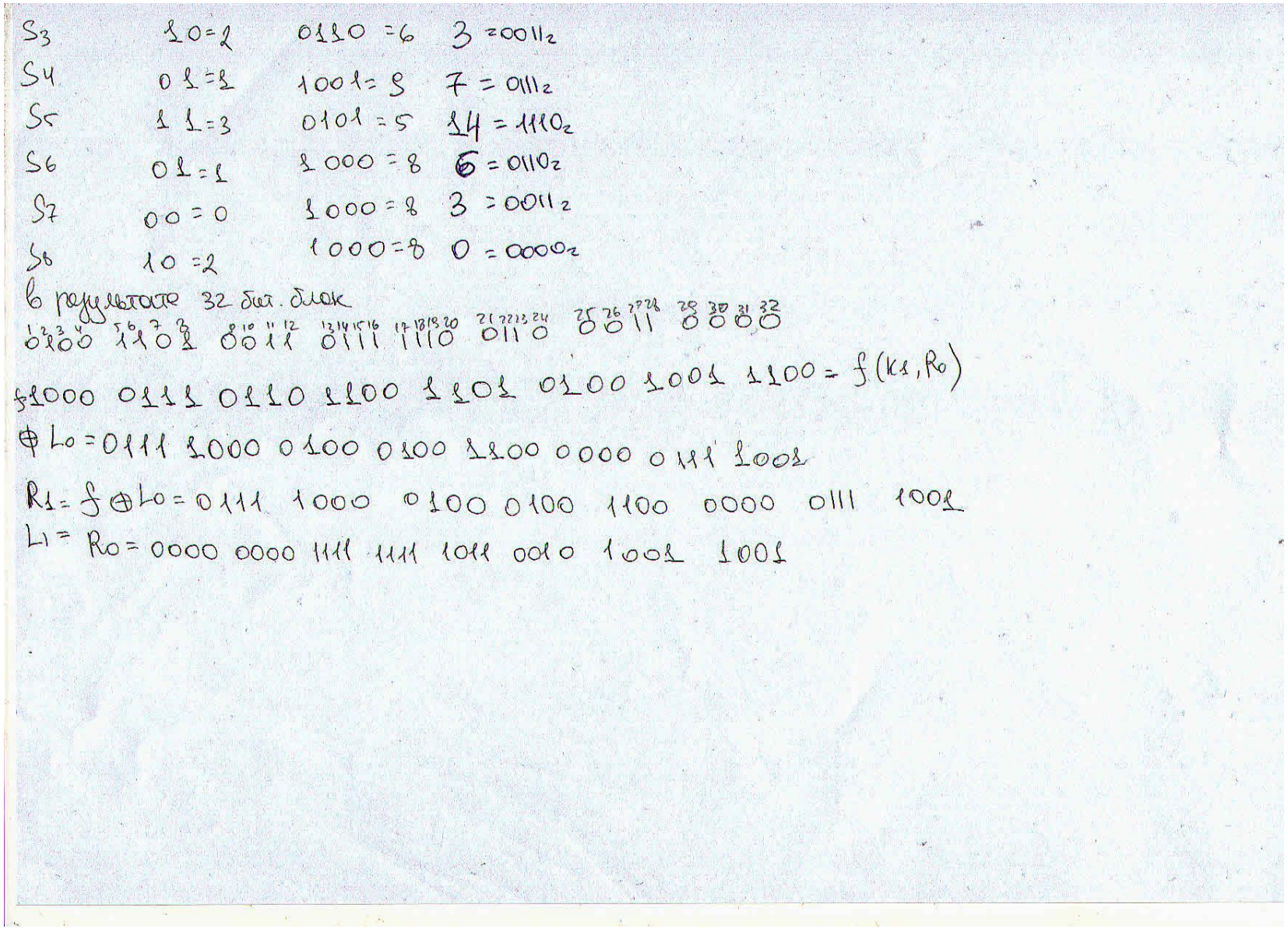
M_{16} = 63 68 65 72 6e 79 61 6b

K_{16} = 31 33 30 34 32 36 5f 61

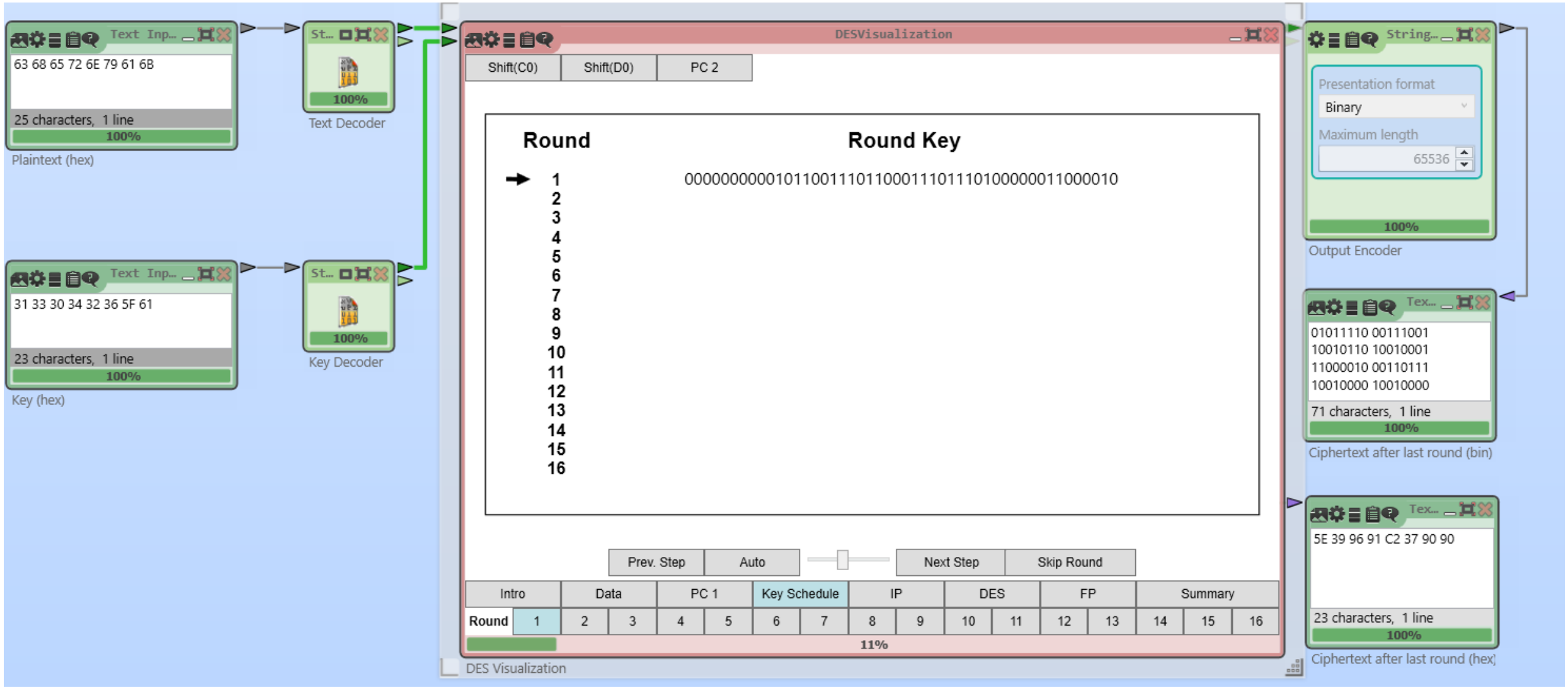
Ручные преобразования 1 раунда



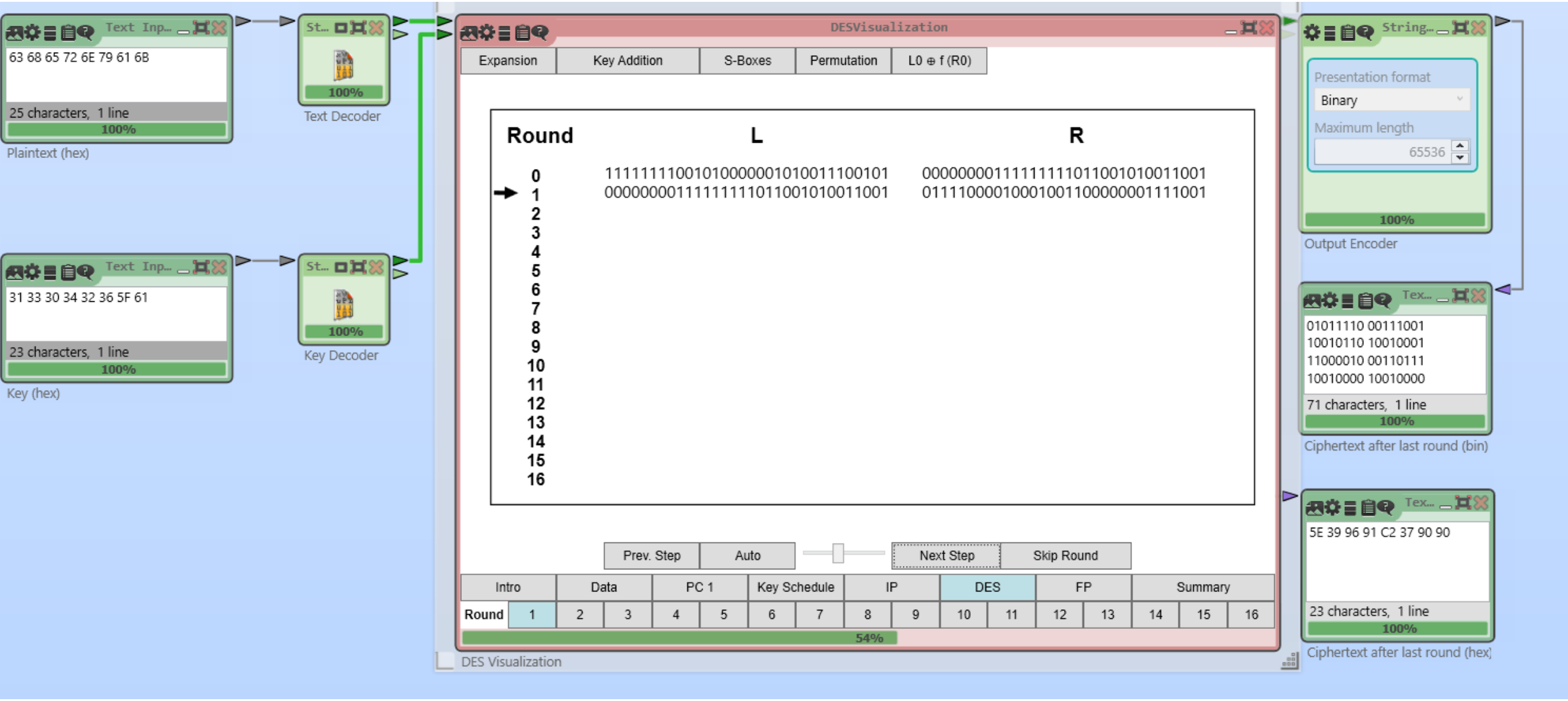
Ручные преобразования 1 раунда. Продолжение



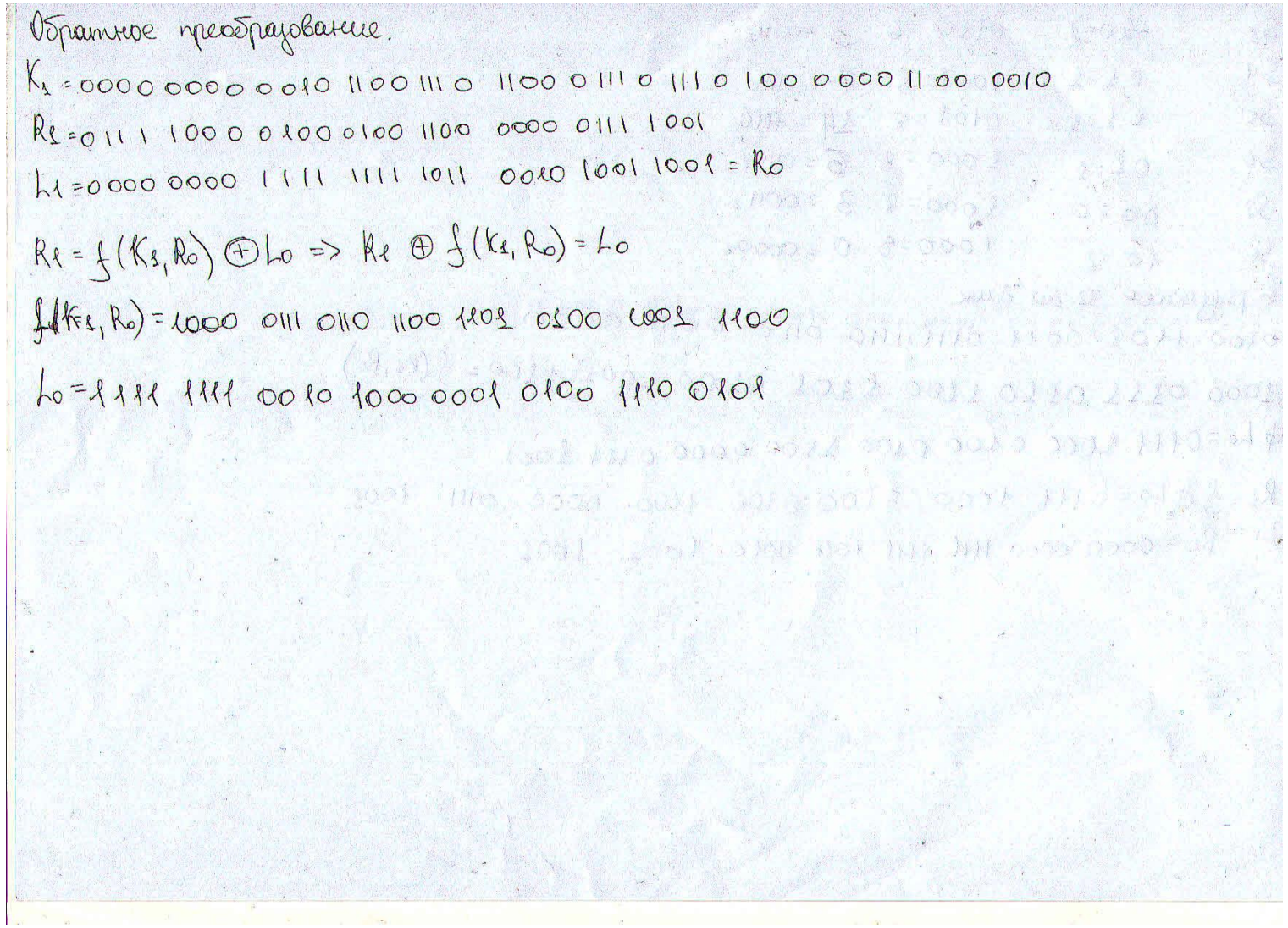
CrypTool 2. Ключ первого раунда



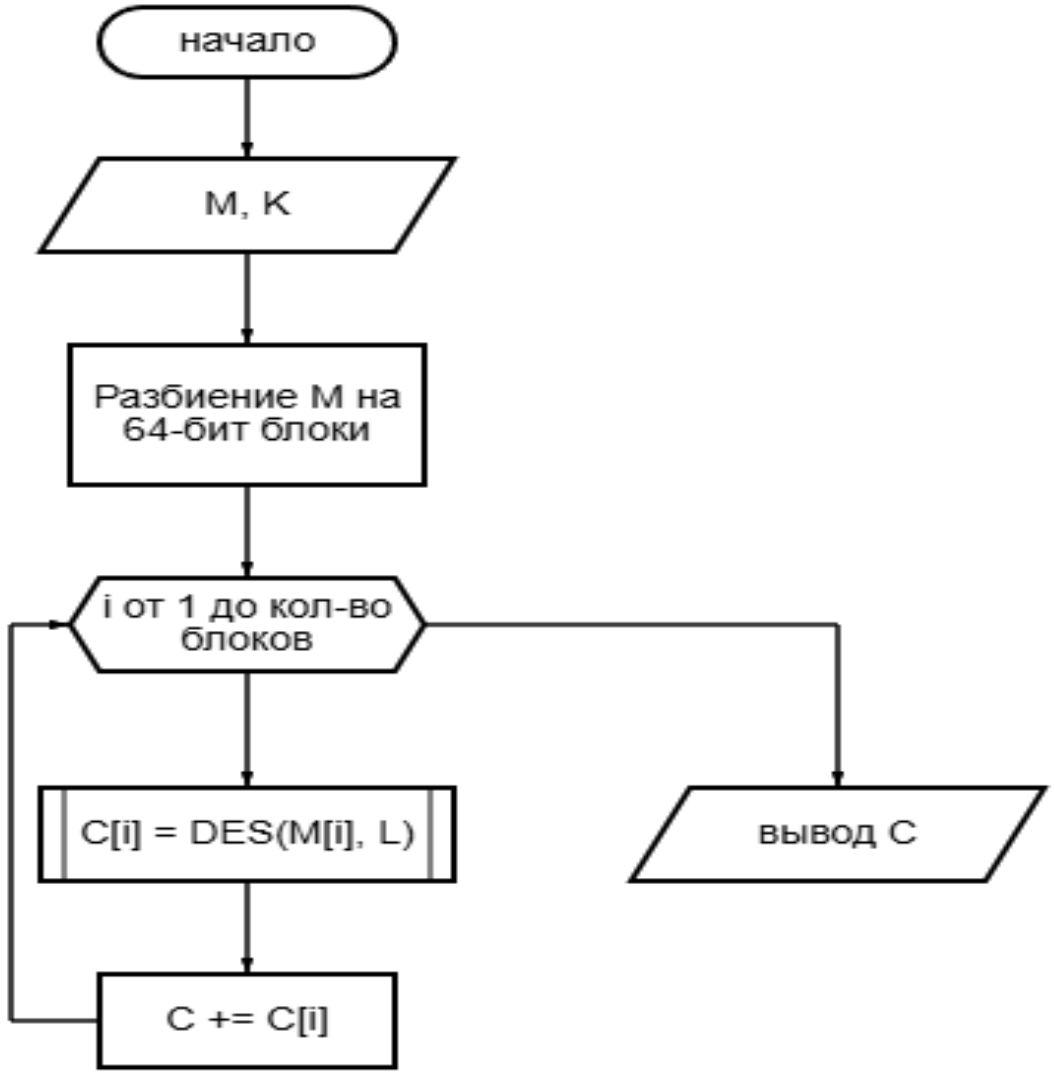
CrypTool 2. L_1 и R_1



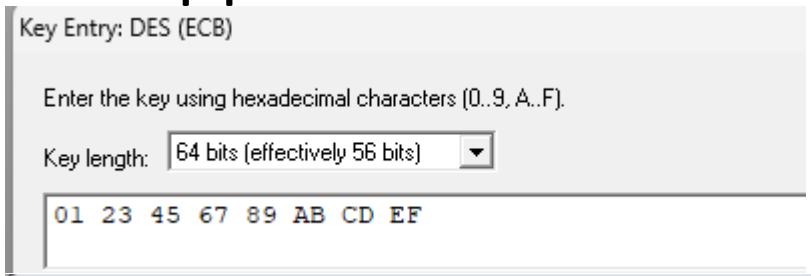
Ручные преобразования 1 раунда. Обратное



DES: схема режима ECB. Электронная кодовая книга



Шифрование английского текста DES в режиме ECB



startingexample-en.txt

The United Kingdom of Great Britain has the excellent transport infrastructure. Not only the huge tourist flow, but also the development of the country itself and, in particular, the business sphere contributed there. The total length of all roads is at least 399 thousand kilometers. At the same time, there are relatively few highways in the country. They make only about three and a half thousand kilometers. You can travel by car in any region of the country. Don't forget that the UK has the left-hand traffic. In London, there is a metro or a tube that embraces 12 underground, land and mixed lines. It is worth noting that the lines are often split into separate small branches, so you should always follow the transport route.

There are also taxi services in the country. The most expensive vehicles are black cabs. They can be stopped simply on the street. Cars are always upscale, with a clean and comfortable interior. Drivers use a meter. The less expensive taxi should be called on the phone. In this case, you need to clarify the price, since there is no meter in the cabin. Large cities have trams. In London, you can even find two-story trams. However, buses are considered the most popular way of traveling around the city. They run from 4-5 am until 1 am.

DES (ECB) encryption of <startingexample-en.txt>, key <01 23 45 67 89 AB CD EF>

```
00000000   46 24 08 C5 6A 86 D0 0E D5 E8 47 4D 86 58 F3 6B   F$..j.....GM.X.k
00000010   97 A1 4C 26 5F 02 18 39 B0 2E C9 17 84 18 17 36   ..L&_..9.......6
00000020   AB C8 D4 A8 FB A0 E9 8A 5F 1A 30 1C C2 86 7E 75   ........_.0...~u
00000030   EB B1 2E 65 A3 74 F6 3C 7A 04 78 0B AD 6A 12 D8   ...e.t.<z.x..j..
00000040   CD 71 17 98 BB 91 6F DE 7C E3 C3 0F 11 F7 5B 44   .q....o.|.....[D
00000050   21 09 A0 34 10 13 9E FE 60 9D 09 4C 56 35 8D AA   !..4....`..LV5..
00000060   6C 41 3C 04 2A BC 5C C7 CA D3 71 7A A1 B4 08 F8   lA<.*.\...qz....
00000070   BE 45 7A E8 3F 6C 03 8B C8 1B 8E C5 3C 4E 2F C9   .Ez.?l......<N/.
00000080   CA 43 99 55 93 E9 6B 29 DE E4 6E E8 A5 3D 9A E6   .C.U..k)..n..=..
00000090   5E 17 36 AD B8 30 31 56 8E 49 68 DA F0 74 BC 55   ^.6..01V.Ih..t.U
000000A0   7F 2C C6 E0 3D 52 AD A4 BF B8 CD 36 67 98 40 ED   .,..=R.....6g.@.
000000B0   E2 CF C8 2D D4 02 96 D5 0A 6C 70 76 35 8B 3D 9E   ...-.....lpv5.=.
000000C0   C1 77 C2 82 20 57 12 02 64 4C D9 6A 6D D7 5E 36   .w.. W..dL.jm.^6
000000D0   97 40 17 B2 0F 25 F9 0A 2A 4F D8 2C 88 DE 10 CE   .@...%..*O.,....
000000E0   93 45 CD 2B E0 21 3D 7A 2B 36 21 77 5B 86 72 97   .E.+.!=z+6!w[.r.
000000F0   6B 0E F1 AA 44 76 A8 5E E7 B0 B2 3B 3C 28 57 3E   k...Dv.^...;<(W>
00000100   EE 6B 9D 27 7B E4 C1 25 ED 1D A6 52 42 A6 3C 2C   .k.'{..%...RB.<,
00000110   13 05 49 6D 44 30 FC 2A A8 D1 AF 08 F8 ED 14 BD   ..ImD0.*........
00000120   5E 15 39 73 67 C8 77 24 79 C5 8F DA A8 E6 BB 0E   ^.9sg.w$y.......
00000130   CA 69 6F F4 94 01 88 6A F5 71 2A DF AB 27 F8 73   .io....j.q*..'.s
00000140   EC 88 7A 7B AB FA DD 65 CA FF 83 6F 76 6B 6C D0   ..z{...e...ovkl.
00000150   C1 3F 38 DE D5 89 A5 D1 23 CE 91 F9 9A C6 7E B2   .?8.....#.....~.
00000160   9D 87 C3 83 A6 25 72 F7 A2 69 66 93 7C 01 AF 82   .....%r..if.|...
00000170   CC 6A 80 BD 7F 9D 2C 10 91 19 BE 92 7B 96 11 7D   .j....,.....{..}
00000180   89 B8 2A 8F AD 17 68 04 EA 0F 18 64 BD 71 E7 46   ..*...h....d.q.F
00000190   DE CE 08 BB F6 78 4A 59 FE EB 12 F3 2C D0 2F F7   .....xJY....,./.
000001A0   37 A1 A3 31 E1 F1 2F 9D 4E C7 0E F7 8D A0 69 12   7..1../.N.....i.
000001B0   78 F2 02 2F D9 CA 43 01 4F 24 8A 7B 67 38 04 D8   x../..C.O$.{g8..
000001C0   81 B7 F4 A0 FF C8 9A EC 42 A5 25 FD 7A 2D 01 CE   ........B.%.z-..
000001D0   9F 7A 6D 29 86 09 59 D0 76 5B 99 6A D5 78 4F 90   .zm)..Y.v[.j.xO.
000001E0   60 4A 76 10 CB CF 81 92 9E 9C 22 D3 66 B1 5A AA   `Jv.......".f.Z.
000001F0   EC C4 CE B7 28 47 0F 5E 70 BC 37 3F BD 0A 3D F0   ....(G.^p.7?..=.
00000200   0C DC A7 B3 FD 07 78 D3 0E E4 6B 2D 8B E4 B6 0F   ......x...k-....
00000210   D4 E0 1D 66 CF FE 73 2C 02 81 6C 4F 54 5F 0B 5B   ...f..s,..lOT_.[
00000220   36 92 0A 7B BB B9 D4 EF 53 71 5D 11 8C 4F 2A 8D   6..{....Sq]..O*.
00000230   B0 26 88 25 B5 BE EE A7 EA 86 7C D0 95 A8 9D 94   .&.%......|.....
00000240   39 DF BE B2 14 E3 D3 20 F0 61 26 12 E0 53 58 AE   9...... .a&..SX.
00000250   B5 3C 2B 66 D4 9E BF FB 4B AF 8D FA 01 8E D0 61   .<+f....K......a
00000260   D4 8F 5F 5F B6 59 29 02 00 86 E2 53 5C 23 05 A2   .. .Y).....S\#..
```

Оценка времени проведения атаки «грубой силы». ECB

Известные байты	Оценка времени взлома
0	1.1 * 10^4 лет
2	251 день
3	2 дня
4	22 минуты
5	10 секунд
6	< 1 секунды
7	< 1 секунды

56-bit brute-force search 0% completed.
Remaining time: 1.1e+004 years

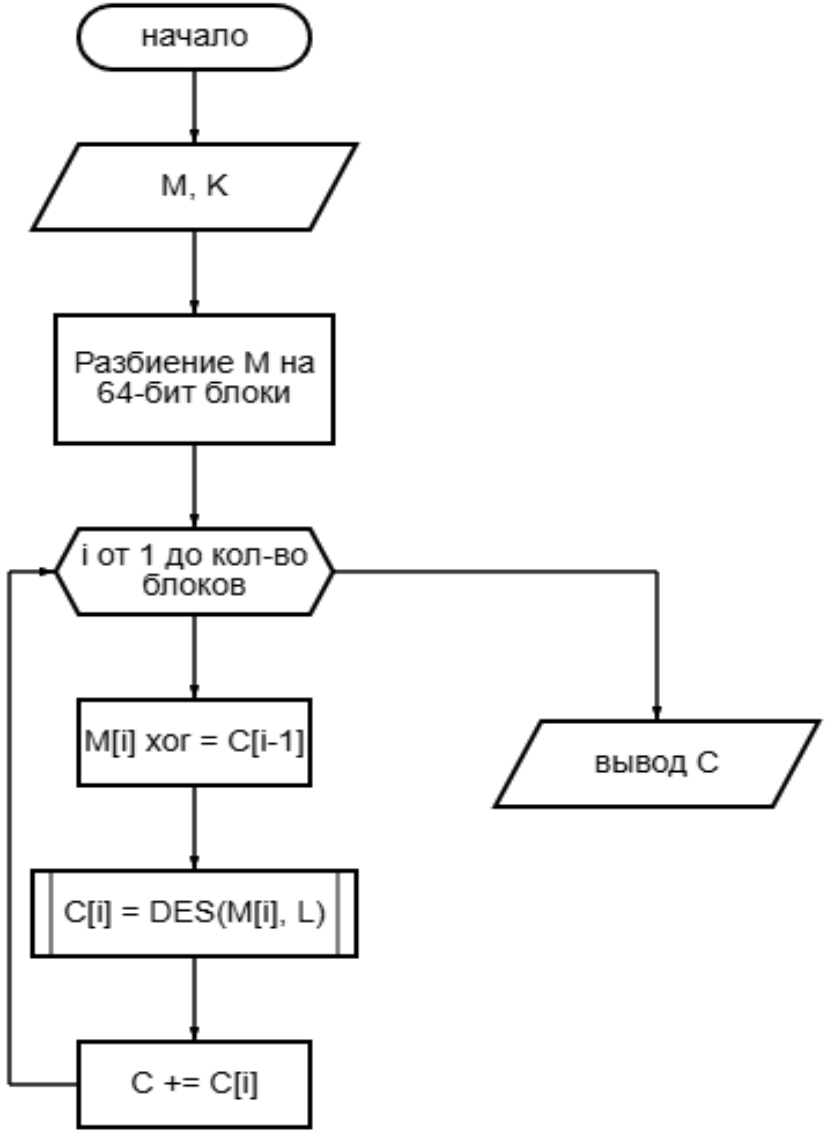
42-bit brute-force search 0% completed.
Remaining time: 251.5 days

35-bit brute-force search 0% completed.
Remaining time: 2.0 days

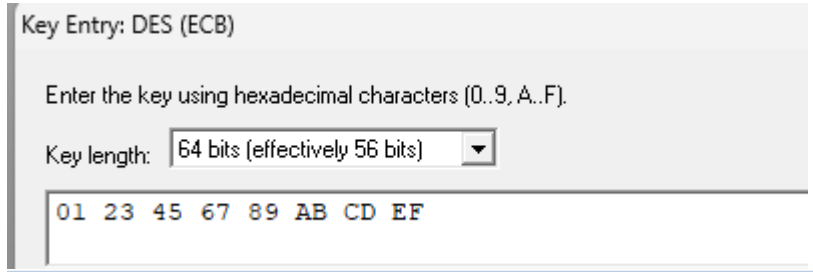
28-bit brute-force search 0% completed.
Remaining time: 00:22 h

21-bit brute-force search 4% completed.
Remaining time: 00:00:10 h

DES: схема режима CBC. Сцепление шифрованных блоков



Шифрование английского текста DES в режиме CBC



startingexample-en.txt

The United Kingdom of Great Britain has the excellent transport infrastructure. Not only the huge tourist flow, but also the development of the country itself and, in particular, the business sphere contributed there. The total length of all roads is at least 399 thousand kilometers. At the same time, there are relatively few highways in the country. They make only about three and a half thousand kilometers. You can travel by car in any region of the country. Don't forget that the UK has the left-hand traffic. In London, there is a metro or a tube that embraces 12 underground, land and mixed lines. It is worth noting that the lines are often split into separate small branches, so you should always follow the transport route.

There are also taxi services in the country. The most expensive vehicles are black cabs. They can be stopped simply on the street. Cars are always upscale, with a clean and comfortable interior. Drivers use a meter. The less expensive taxi should be called on the phone. In this case, you need to clarify the price, since there is no meter in the cabin. Large cities have trams. In London, you can even find two-story trams. However, buses are considered the most popular way of traveling around the city. They run from 4-5 am until 1 am.

DES (CBC) encryption of <startingexample-en.txt>, key <01 23 45 67 89 AB CD EF>

```
00000000   46 24 08 C5 6A 86 D0 0E 4E 40 38 A3 26 21 01   F$..j...N@8.&!.
0000000F   97 AE 1F 8E 00 03 60 F2 90 7B 71 6F 52 9F CE   ......`..{qoR..
0000001E   42 9D 9B 5C 57 A7 C3 50 29 E2 20 A1 67 ED 1F   B..\W..P). .g..
0000002D   77 E0 0E 78 88 6F B8 A4 E4 DC 42 B4 52 15 FE   w..x.o....B.R..
0000003C   BF 90 BB AC FA 97 4E FB B7 98 EF 06 7B 47 FC   ......N.....{G.
0000004B   DC FF B9 78 0B D1 6F 2C C5 BD EB E1 46 01 2B   ...x..o,....F.+
0000005A   34 E9 52 76 C3 8A B1 6D DE C8 70 36 3B 81 17   4.Rv...m..p6;..
00000069   A9 F0 96 4C 9C 31 AE 4E 33 53 64 36 EA 1F 68   ...L.1.N3Sd6..h
00000078   A3 41 EF E0 54 9A E5 BD B7 F6 92 52 6D 5B 78   .A..T......Rm[x
00000087   AF B7 42 A6 81 E0 E5 EF B0 CE 58 8F 47 9F 9C   ..B.......X.G..
00000096   FE 60 92 CD 97 C9 A6 F8 81 D4 34 3C 60 F5 E1   .`........4<`..
000000A5   8D AC 24 E0 2F 1E 38 CF BD A3 F1 D5 F2 3C 83   ..$./.8......<.
000000B4   58 25 DA EE 37 16 01 81 44 B4 C4 D2 E0 CB DC   X%..7...D......
000000C3   E5 F3 A6 69 DE F9 7E BE A8 DF 10 2C 74 24 69   ...i..~....,t$i
000000D2   83 6E 4A 0A DD 2D 66 1D D6 2E 18 26 44 6C B4   .nJ..-f....&Dl.
000000E1   EB 69 85 D3 C6 98 C2 57 CA AB 2F 87 ED B4 5B   .i.....W../...[
000000F0   A5 4D 6F 33 18 EF 54 10 D5 53 64 E9 8A 89 75   .Mo3..T..Sd...u
000000FF   0F 5C 4F 23 12 13 BD 0F F7 E4 D4 1F EC F4 C7   .\O#............
0000010E   78 F0 D2 5B 95 4D EF C2 2F 0A 97 D6 7C 3F 7E   x..[.M../...|?~
0000011D   7A A0 D4 4E 4E 66 19 23 F3 D9 E5 85 E3 AE 76   z..NNf.#......v
0000012C   3C 50 E2 95 13 C4 EE 66 31 DE 8E 7E 57 8D DD   <P.....f1..~W..
0000013B   D6 AF 6C 42 F8 7D 72 B8 09 99 DF 26 33 9E 78   ..lB.}r....&3.x
0000014A   A0 84 0F 0F CF 18 D9 64 43 7C FF 52 3D 4B 78   .......dC|.R=Kx
00000159   BD C0 DB F4 1A 9C 09 6E DC 7B 61 3B BC BD 18   .......n.{a;....
00000168   07 49 65 32 2D FB 51 CB 7C CE B3 2F BF 9C 5E   .Ie2-.Q.|../..^
00000177   5E 91 78 62 E0 FE 52 D9 21 83 9A C7 D5 40 FE   ^.xb..R.!....@.
00000186   A1 C6 12 FC 22 05 E7 86 AD 1E E1 01 5D 2A E0   ....".......]*.
00000195   7A CA 27 8A 4B 82 32 84 45 4D 77 52 A8 04 B5   z.'.K.2.EMwR...
000001A4   36 4C EA EB 40 08 EA BF F6 F9 13 7A 8C E0 7E   6L..@......z..~
000001B3   72 40 96 08 E9 96 FA 29 40 43 CB 9A 4C AA 3A   r@.....)@C..L.:
000001C2   03 F1 A7 4F 23 49 96 23 7E 5E 9F F0 64 85 A0      O#I.#~^..d..
```

Оценка времени проведения атаки «грубой силы». CBC

Известные байты	Оценка времени взлома
0	1.9 * 10^4 лет
2	1.1 год
3	3.3 дня
4	37 часов
5	17 секунд
6	< 1 секунды
7	< 1 секунды

56-bit brute-force search 0% completed.
Remaining time: 1.9e+004 years

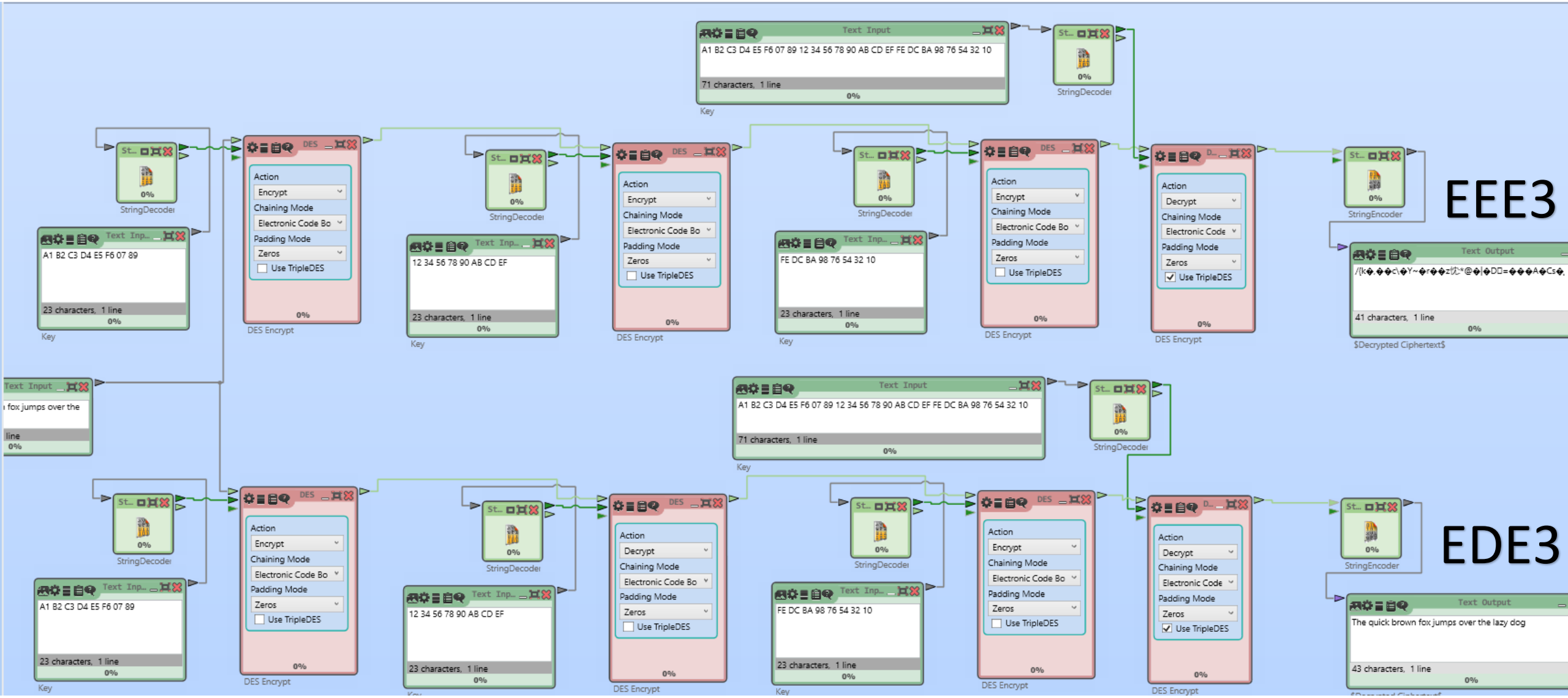
42-bit brute-force search 0% completed.
Remaining time: 1.1 years

35-bit brute-force search 0% completed.
Remaining time: 3.3 days

28-bit brute-force search 0% completed.
Remaining time: 00:37 h

21-bit brute-force search 4% completed.
Remaining time: 00:00:17 h

Анализ 3-DES. Ключи 24 байта.



Анализ 3-DES. Ключи 16 байт.

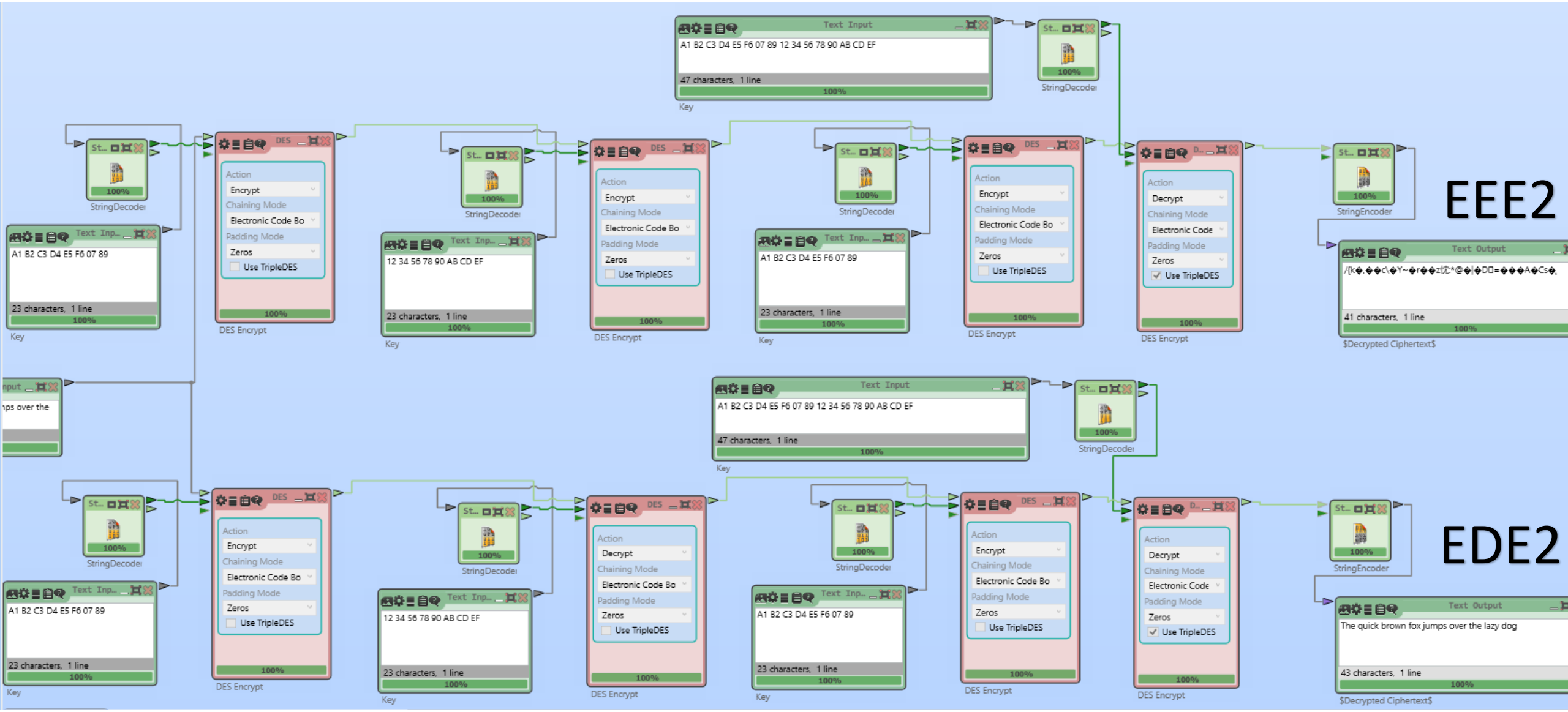
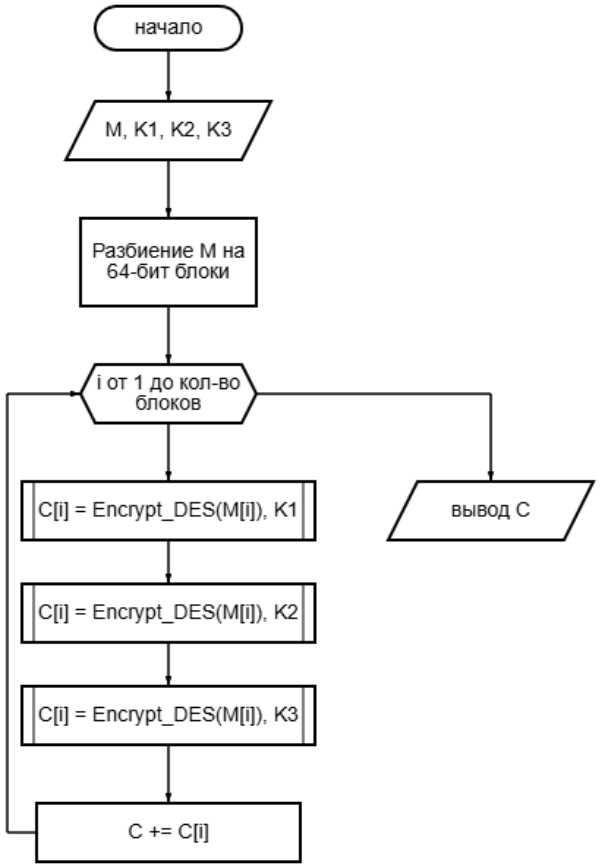
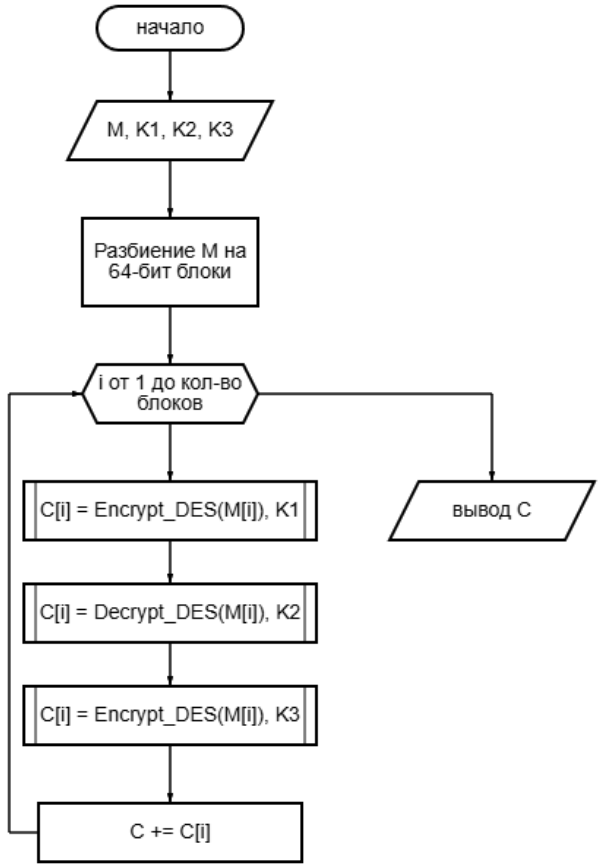
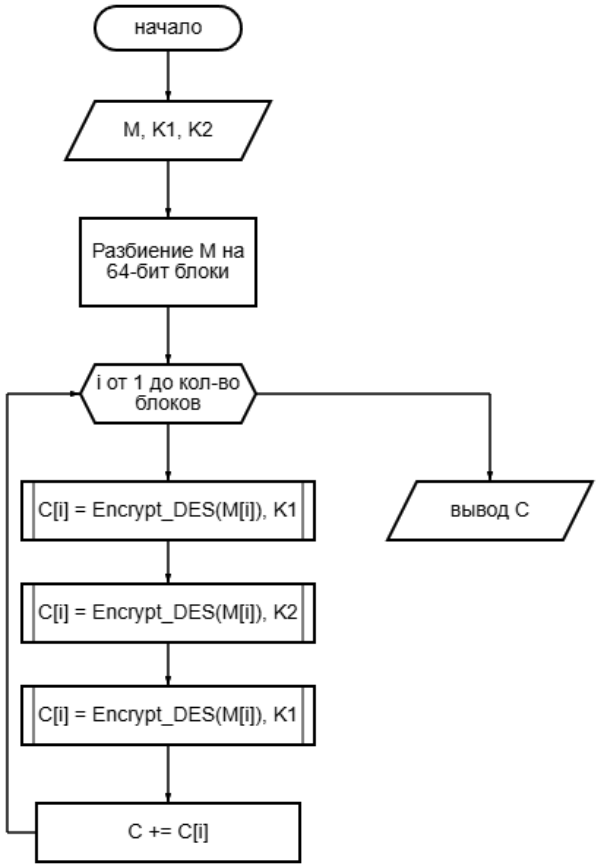
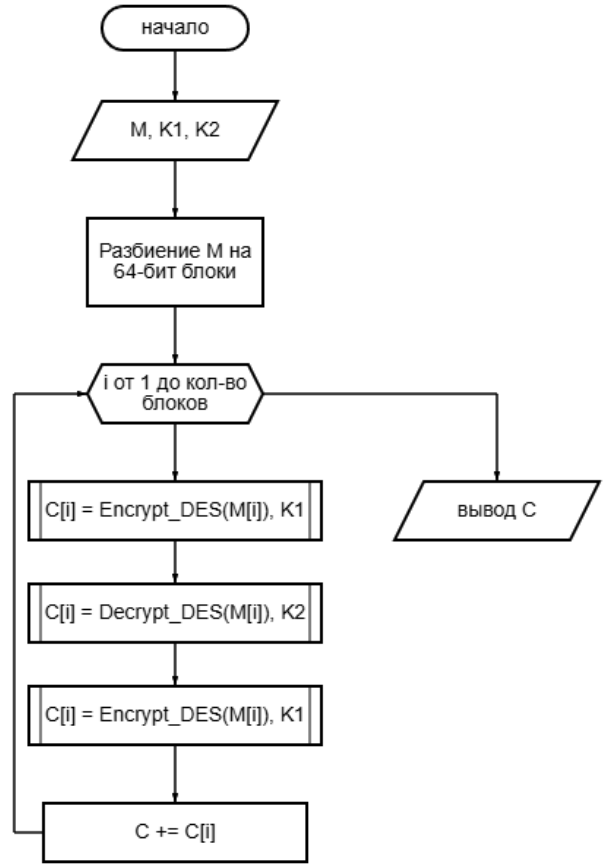


Схема Triple-DES









Шифр «Магма»

Задание

1. Изучить преобразования шифра Магма с помощью приложения ЛИТОРЕЯ.
2. Рассчитать руками субблоки и раундовые ключей шифра для первого раунда. Сравнение с результатами демо-приложения.
3. Рассчитать руками обратное преобразование шифровки.
4. Провести исследование шифра Магма в режимах работы простой замены и простой замены с зацеплением, используя приложение ЛИТОРЕЯ.
5. Создать картинку со своими ФИО (формат bmp).
6. Зашифровать картинку шифром Магма в режиме ECB.
7. Зашифровать картинку шифром Магма в режиме CBC с тем же ключом.
8. Сохранить шифровки в виде картинок для отчета.
9. Сжать исходную и две зашифрованных картинки средствами CrypTool.
10. Зафиксировать размеры полученных файлов в таблице

Исходные данные

Открытый текст M = “Chernyak”

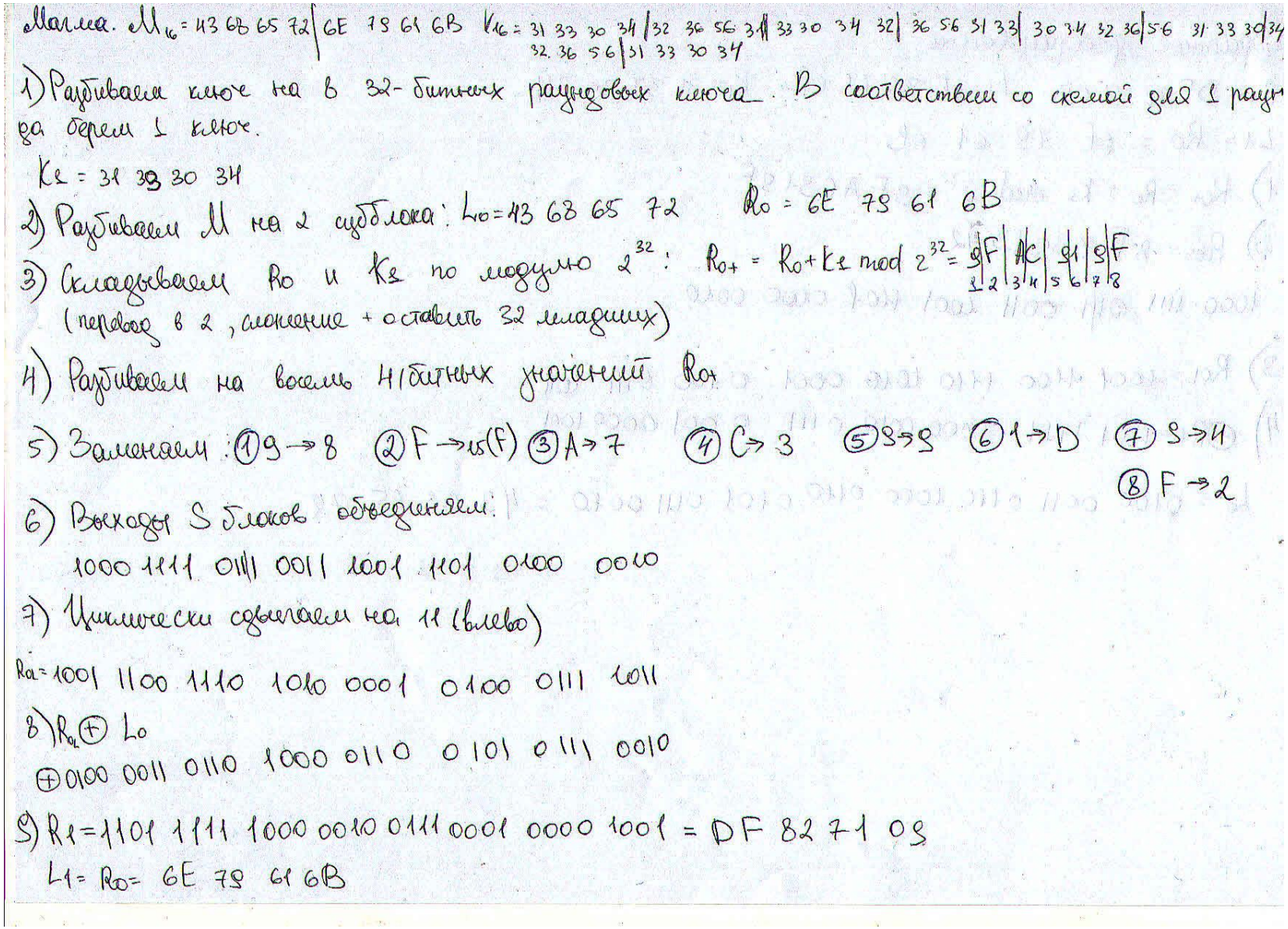
Ключ K = “130426V130426V130426V130426V1304”

Байтовое представление:

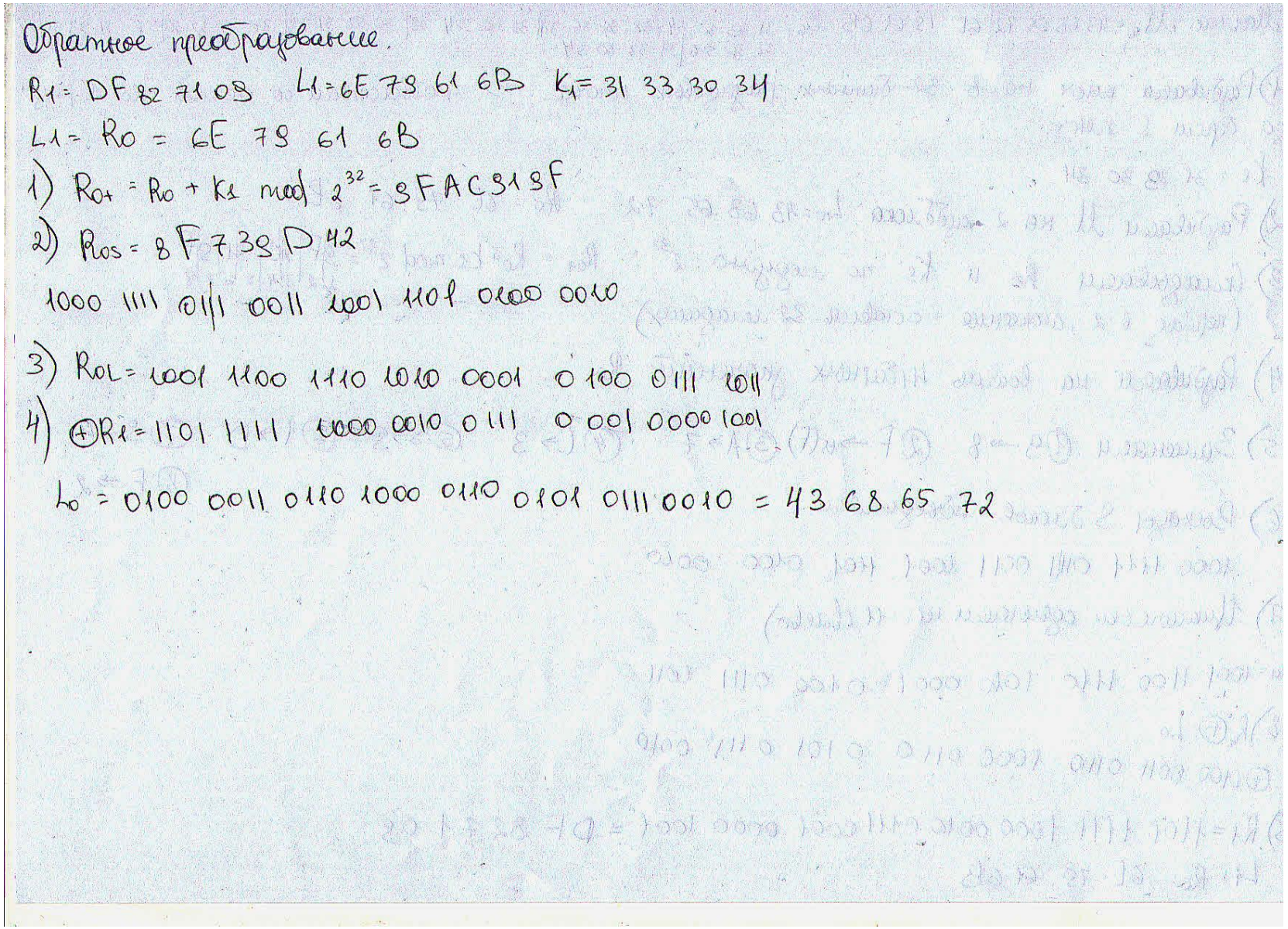
M_{16} = 43 68 65 72 6e 79 61 6b

K_{16} = 31 33 30 34 32 36 56 31 33 30 34 32 36 56 31 33 30 34 32 36 56 31 33 30 34 32 36 56 31 33 30 34

Ручные преобразования 1 раунда



Ручные преобразования 1 раунда. Обратно



Обратное преобразование.

$R_1 = DF\ 82\ 71\ 08$ $L_1 = 6E\ 79\ 61\ 6B$ $K_1 = 31\ 33\ 30\ 34$

$L_1 = R_0 = 6E\ 79\ 61\ 6B$

1) $R_{0+} = R_0 + K_1 \bmod 2^{32} = 9FAC319F$

2) $R_{0S} = 8F739D42$

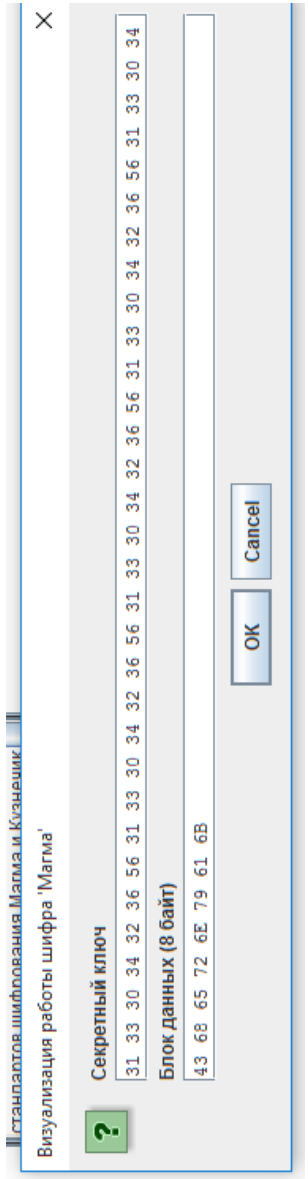
1000 1111 0111 0011 1001 1101 0100 0010

3) $R_{0L} =$ 1001 1100 1110 1010 0001 0100 0111 1011

4) $\oplus R_1 =$ 1101 1111 1000 0010 0111 0001 0000 1001

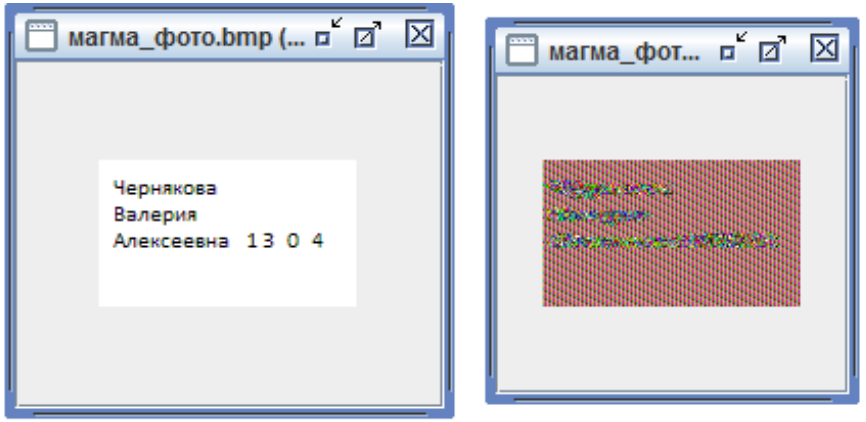
$L_0 =$ 0100 0011 0110 1000 0110 0101 0111 0010 $= 43\ 68\ 65\ 72$

ЛИТОРЕЯ. Первый раунд



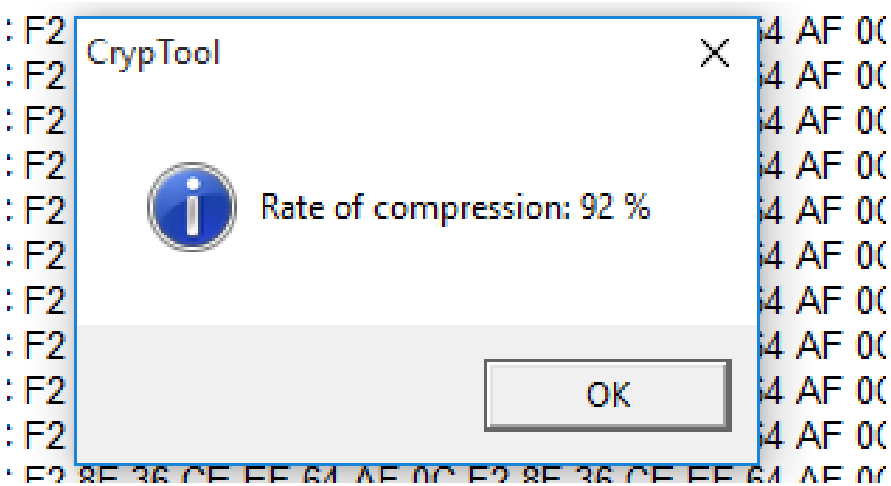
Субблок L: 43 68 65 72	Субблок R: 6E 79 61 6B		Ключ раунда: 31 33 30 34
		Преобразование: 'сложение по модулю 2^32'	
		Результат: 9F AC 91 9F	
		Преобразование: 'подстановка S'	
		Результат: F7 8B 03 E1	
		Преобразование: 'циклический сдвиг <<11'	
		Результат: 58 1F 0F BC	
		Преобразование: 'сложение XOR'	
Субблок L': 6E 79 61 6B	Субблок R': 1B 77 6A CE	Результат: 1B 77 6A CE	
		Раунд №1	>

Режим простой замены

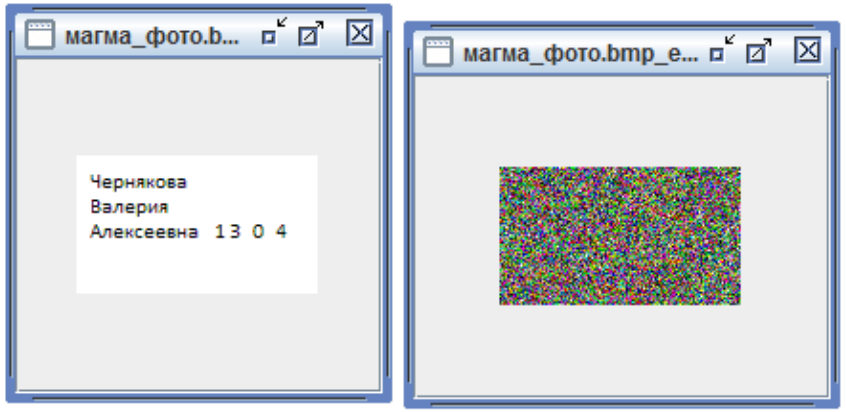


Текст на изображение относительно различим

Сжатие средствами CrypTool1 составило 0.92

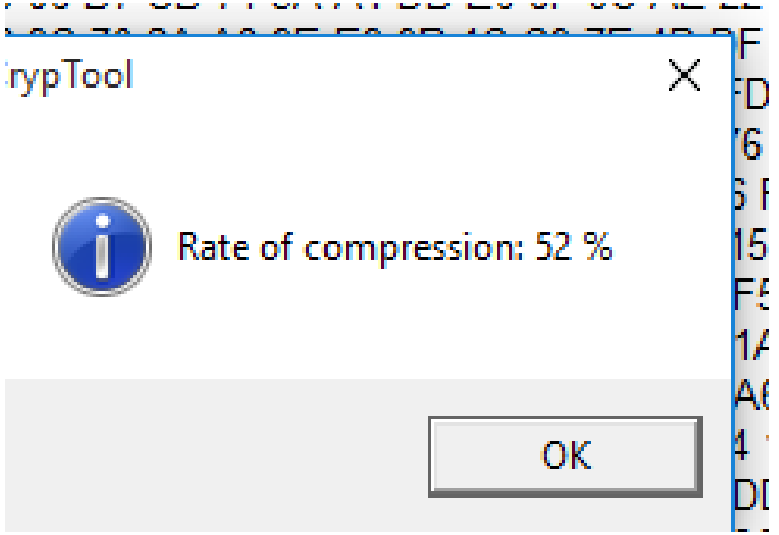


Режим простой замены с зацеплением



Текст на изображение невозможно различить

Сжатие средствами CrypTool1 составило 0.52



Заключение

Изучен шифр DES и выявлены следующие характеристики:

- Блочный симметричный шифр. Длина блока на входе 64 бит. Длина ключа 64 бит (56 ключ + 8 четность). Алгоритм включает 2 перестановки (начальную и конечную) и 16 раундов Фейстеля.

Изучена работа DES в режимах ECB и CBC и выявлены следующие характеристики:

- В режиме ECB каждый блок шифруется независимым ключом. В режиме CBC на шифрование каждого следующего блока влияет результат шифрования предыдущего.
- Средствами CrypTool1 оценено время атаки «грубой силы» в зависимости от количества известных байт. Чем больше байт известно, тем быстрее происходит атака. Также для EBC нужно меньше времени, чем для CBC.

Изучена работа 3DES и выявлены следующие характеристики:

- Для EDE3 и EEE3 используется 3 различных ключа, первая модификация отличается от второй чередование шифровка-расшифровка-шифровка, второе включает только шифровку. Средствами CrypTool2 выявлено, что он поддерживает только EDE3.
- Для EDE2 и EEE2 используется 2 различных ключа, первая модификация отличается от второй чередование шифровка-расшифровка-шифровка, второе включает только шифровку. Средствами CrypTool2 выявлено, что он поддерживает только EDE2.

Изучена работа шифра Магма и выявлены следующие характеристики:

- Блочный симметричный шифр. Длина блока на входе 64 бита. Длина ключа 256 бит. Алгоритм включает 32 раунда Фейстеля.
- Средствами ЛИТОРЕЯ и CrypTool1 произведен анализ шифра простой замены и с зацеплением на основе фото типа bmp. Степень сжатия файла в первом случае (0.92) больше, чем во втором (0.52). Это говорит о том, что при режиме простой замены с зацеплением энтропия данных больше.