

**МИНОБРНАУКИ РОССИИ**  
**САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ**  
**ЭЛЕКТРОТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ**  
**«ЛЭТИ» ИМ. В.И. УЛЬЯНОВА (ЛЕНИНА)**  
**Кафедра МО ЭВМ**

**ОТЧЕТ**  
**по лабораторной работе №4**  
**по дисциплине «Криптография и защита информации»**  
**ТЕМА: ИЗУЧЕНИЕ И ИССЛЕДОВАНИЕ ШИФРОВ DES, 3-DES и МАГМА.**

Студент гр. 0303

Калмак Д.А.

Преподаватель

Племянников А.К.

Санкт-Петербург

2023

## **Цель работы.**

Изучить и исследовать шифры DES, 3-DES и Магма.

## **Порядок выполнения работы.**

1. Изучить преобразования DES по шаблонной схеме DES Visualisation из CrypTool 2 с учетом рекомендаций Методического пособия (задание на с. 20 )

2. Провести исследование DES в режимах работы ECB и CBC, используя CrypTool 1 и с учетом рекомендаций Методического пособия (задание на с. 22 - оценка трудоемкости атаки "грубой силы" )

3. Разработать схему в CrypTool 2 для экспериментального определения версии 3-DES.

4. Изучить преобразования шифра Магма с помощью приложения ЛИТОРЕЯ, с учетом рекомендаций Методического пособия (задание на с. 20)

5. Провести исследование шифра Магма в режимах работы простой замены и простой замены с зацеплением, используя приложение ЛИТОРЕЯ и с учетом рекомендаций Методического пособия (задание на с. 21 - шифрование изображения в разных режимах работы)

## **Выполнение работы.**

### **1. Шифр DES**

#### **1.1 Преобразования DES по шаблонной схеме DES Visualisation**

Исходный текст: KALMAKDA

В бинарном виде: 01001011 01000001 01001100 01001101 01000001  
01001011 01000100 01000001

Ключ: 030307AN

В бинарном виде: 00110000 00110011 00110000 00110011 00110000  
00110111 01000001 01001110

1. Определим ключ первого раунда  $K_1$

Сделаем перестановку ключа в соответствии с таблицей.

57	49	41	33	25	17	9	1	58	50	42	34	26	18	$C_0$
10	2	59	51	43	35	27	19	11	3	60	52	44	36	
63	55	47	39	31	23	15	7	62	54	46	38	30	22	$D_0$
14	6	61	53	45	37	29	21	13	5	28	20	12	4	

$C = 0000000011000000001111110011$

$D = 1010101010100000100000001111$

Обе части сдвигаем на один влево, так как раунд первый.

i	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Число сдвига	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

$C = 0000000110000000011111100110$

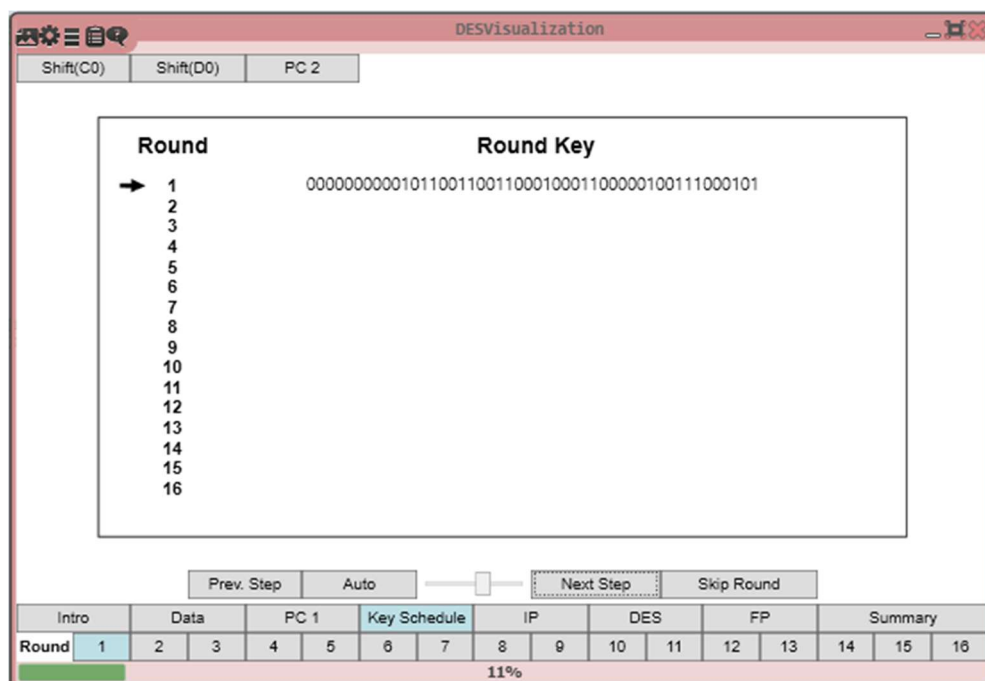
$D = 0101010101000001000000011111$

Обе части обрабатываем сжимающей перестановкой в соответствии с таблицей и получим первый раундовый ключ  $K_1$ .

14	17	11	24	1	5	3	28	15	6	21	10	23	19	12	4
26	8	16	7	27	20	13	2	41	52	31	37	47	55	30	40
51	45	33	48	44	49	39	56	34	53	46	42	50	36	29	32

$K_1 = 000000000010110011001100010001100000100111000101$

Полученный ключ совпадает с ключом, полученным в Cryptool 2.



## 2. Произведем первый раунд зашифровки исходного текста

Сделаем перестановку исходного текста в соответствии с таблицей и разделим на два субблока.

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

$$L = 11111111000000000100110010111011$$

$$R = 000000000000000000010110100100001$$

Расширим субблок R с помощью расширяющей таблицы.

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

$$R_e = 100000000000000000000000000101011010100100000010$$

Вычисляем XOR  $K_1$  с полученным результатом R.

$$R_{xor} = 1000000000010110011001100010100111010000011000111$$

Полученный результат R необходимо разделить на восемь блоков по шесть бит и каждый блок заменить с помощью таблицы замен для каждого блока. Первый и последний бит соответствуют номеру строки таблицы, а остальные номеру столбца таблицы.

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7	$S_1$
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8	
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0	
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13	
0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10	$S_2$
1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5	
2	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15	
3	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9	
0	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8	$S_3$
1	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1	
2	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7	
3	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12	
0	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15	$S_4$
1	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9	
2	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4	
3	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14	

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
0	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15	$S_5$
1	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9	
2	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4	
3	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14	
0	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9	$S_6$
1	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6	
2	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14	
3	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3	
0	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11	$S_7$
1	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8	
2	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6	
3	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13	
0	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1	$S_8$
1	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6	
2	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2	
3	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12	
0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7	$S_9$
1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2	
2	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8	
3	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11	

$$R_s = 01000001111110010011110100001000$$

Сделаем перестановку с помощью таблицы.

16	7	20	21	29	12	28	17
1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9
19	13	30	6	22	11	4	25

$$f(R, K_1) = 10111100000000011110000111001100$$

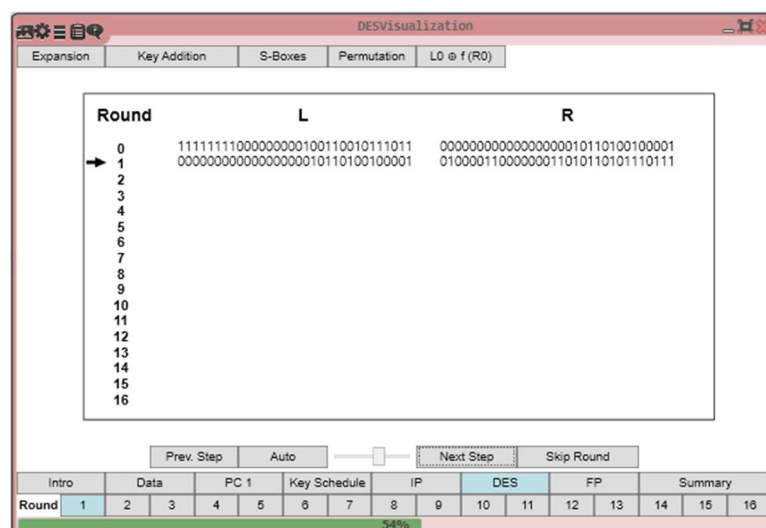
Вычисляем XOR L с полученным результатом.

$$R_1 = 01000011000000011010110101110111$$

Левый субблок  $L_1 = R$ . Получили шифротекст после первого раунда.

$$00000000000000000001011010010000101000011000000011010110101110111$$

Полученный шифротекст совпадает с шифротекстом, полученным в Cryptool 2.



### 3. Расшифруем полученный шифротекст

Необходимо поменять местами  $L_1$  и  $R_1$ .

$R = 000000000000000000010110100100001$

$L = 010000110000000011010110101110111$

Выполним XOR ( $L, f(R, K_1)$ ).

$L = 11111111000000000100110010111011$

$R = 000000000000000000010110100100001$

Сделаем перестановку соединенных субблоков с помощью таблицы, которая содержит обратные перестановки к начальной.

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

01001011010000010100110001001101010000010100101101000100010000001

Разделим на блоки по 8 бит.

01001011 01000001 01001100 01001101 01000001 01001011 01000100 01000001

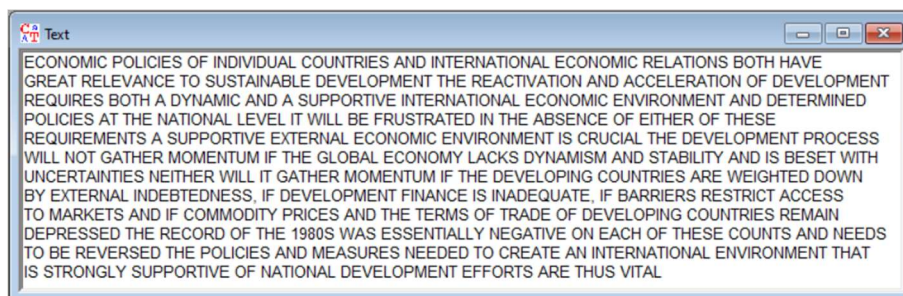
K A L M A K D A

KALMAKDA

Расшифрованный текст соответствует исходному тексту.

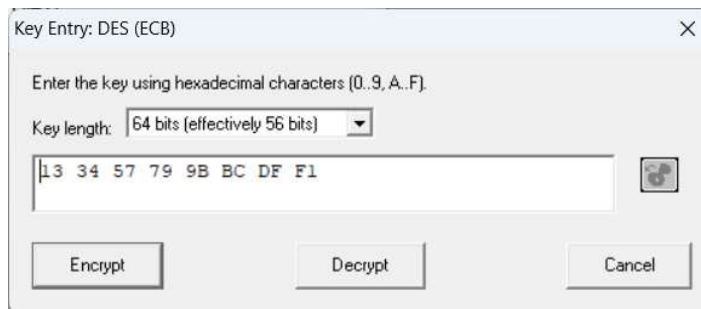
## 1.2 Исследование DES в режимах работы ECB и CBC

Выбран исходный текст на английском языке, в котором количество символов больше тысячи.

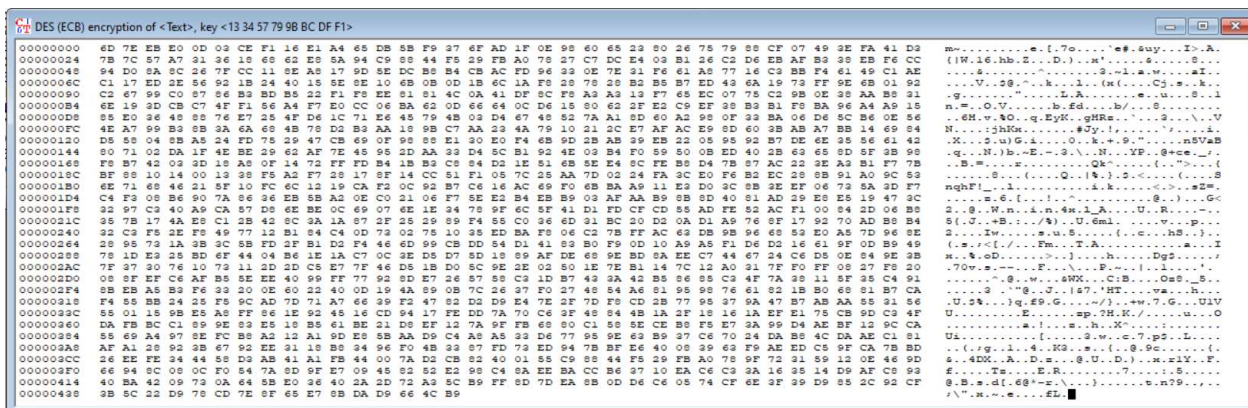


Выбран ключ: 13 34 57 79 9B BC DF F1

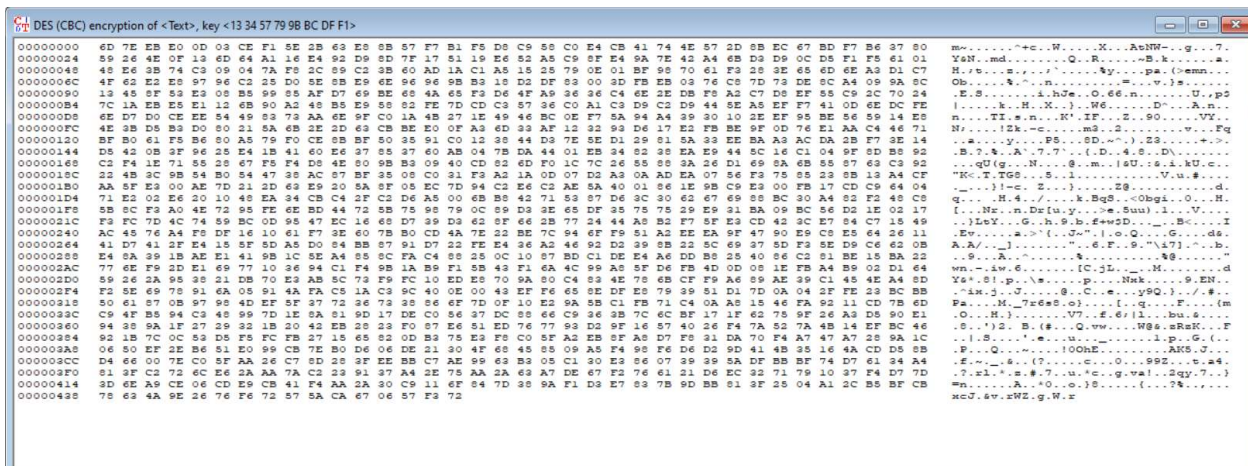




Исходный текст зашифрован с помощью DES (ECB).



Исходный текст зашифрован с помощью DES (CBC).



Для двух шифротекстов ECB и CBC оценено время проведения атаки «грубой силы» в случаях, когда известна часть ключа.

Известный ключ	Время проведения атаки грубой силы на ECB	Время проведения атаки грубой силы на CBC
13 34 57 79 9B BC DF --	<1 секунды	<1 секунды
13 34 57 79 9B BC -- --	1 секунда	1 секунда
13 34 57 79 9B -- -- --	27 секунд	43 секунды

13 34 57 79 -- -- -- --	58 минут	1 час 32 минуты
13 34 57 -- -- -- -- --	5 дней	8 дней
13 34 -- -- -- -- -- --	1.7 года	2.8 года

Исходя из полученных данных, время проведения атаки грубой силы растет экспоненциально. При этом время проведения атаки грубой силы для CBC больше ECB и отношение растет с уменьшением длины известной части ключа.

## 2. Шифр 3-DES

### 2.1 Схема в Cryptool 2 для экспериментального определения версии 3-DES

Шифр 3-DES имеет четыре модификации:

DES-EEE3 – три ключа с последовательным шифрованием

DES-EDE3 – три ключа с шифрованием, дешифрованием, шифрованием

DES-EEE2 - два ключа с последовательным шифрованием, на первом и последнем шифровании один ключ

DES-EDE2 - два ключа с шифрованием, дешифрованием, шифрованием, на первом и последнем шифровании один ключ

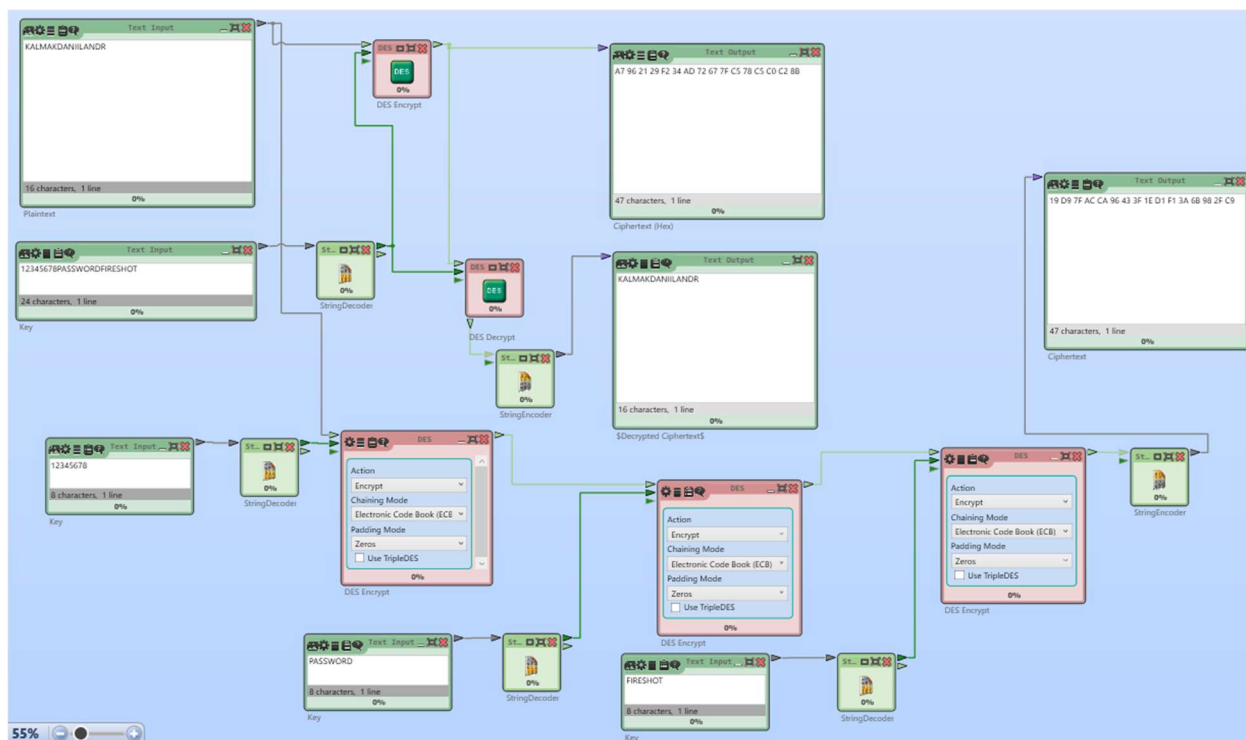
Самая популярная разновидность это DES-EDE3 и DES-EDE2.

За исходный текст возьмем: KALMAKDANIILANDR

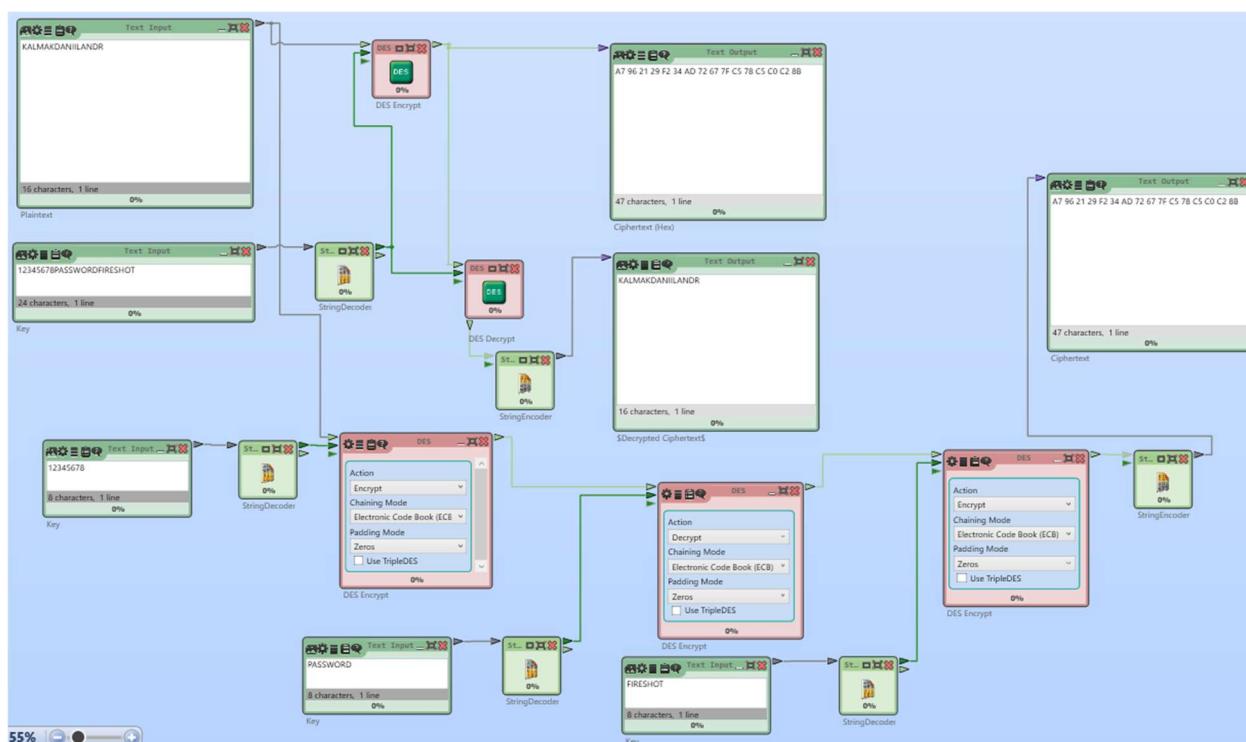
За ключ возьмем: 12345678PASSWORDFIRESHOT – по 8 символов на один ключ для TripleDES.

Составим схему для определения версии с тремя ключами. Для настройки шифрования тремя блоками DES Encrypt необходимо убрать опцию USE TripleDES. В каждом блоке выберем режим Encrypt и проверим результат шифрования – они оказались разные. Значит Cryptool 2 использует не EEE3.





В среднем блоке DES Encrypt выставим Decrypt, чтобы был EDE3. Результаты совпали. Значит Cryptool 2 использует EDE3.



За ключ возьмем: 12345678PASSWORD – по 8 символов на один ключ для TripleDES.

Составим схему для определения версии с двумя ключами. Для настройки шифрования тремя блоками DES Encrypt необходимо убрать опцию USE TripleDES. Первый ключ подсоединить к третьему блоку. В каждом блоке

The screenshot displays a NetLogo simulation of DES encryption and decryption. The interface consists of several text input and output boxes, and several DES Encrypt and StringEncoder blocks.

**Top Section:**

- Text Input:** Plaintext: KALMAKDANILANDR (36 characters, 1 line)
- DES Encrypt:** Takes Plaintext as input. Output: 3B 40 A4 2D F2 93 CB F5 2D A5 B8 46 28 0E 03 B7 (47 characters, 1 line)
- Text Output:** Ciphertext (Hex)

**Middle Section:**

- Text Input:** Key: 12345678PASSWORD (16 characters, 1 line)
- StringDecoder:** Takes Key as input. Output: KALMAKDANILANDR (16 characters, 1 line)
- DES Decrypt:** Takes Ciphertext (Hex) as input. Output: KALMAKDANILANDR (16 characters, 1 line)
- StringEncoder:** Takes Key as input. Output: \$Decrypted Ciphertext\$

**Bottom Section:**

- Text Input:** Key: 12345678 (8 characters, 1 line)
- StringDecoder:** Takes Key as input. Output: 12345678 (8 characters, 1 line)
- DES Encrypt:** Takes Plaintext and Key as input. Output: 3B 40 A4 2D F2 93 CB F5 2D A5 B8 46 28 0E 03 B7 (47 characters, 1 line)
- Text Output:** Ciphertext
- DES Decrypt:** Takes Ciphertext as input. Output: KALMAKDANILANDR (16 characters, 1 line)
- StringEncoder:** Takes Key as input. Output: \$Decrypted Ciphertext\$

The simulation demonstrates the process of encrypting a plaintext message using a key, converting the ciphertext to a string, and then decrypting it back to the original plaintext.

The screenshot displays a NetLogo simulation of a DES encryption and decryption process. The interface is set against a light blue background. At the top left, there is a 'Text Input' box labeled 'Plaintext' containing the text 'KALMAKDANILANDOR'. Below it is another 'Text Input' box labeled 'Key' containing the text '12345678PASSWORD'. To the right of these inputs are two 'DES' boxes. The first 'DES' box is labeled 'DES Encrypt' and has a '0%' progress indicator. It receives input from the 'Plaintext' and 'Key' boxes and outputs to a 'Text Output' box labeled 'Ciphertext (Hex)' containing the text '38 40 A4 2D F2 93 CB F5 2D A5 BB 46 28 0E 03 87'. Below the 'Ciphertext (Hex)' box is another 'Text Output' box labeled 'Decrypted Ciphertext' containing the text 'KALMAKDANILANDOR'. To the right of the 'Decrypted Ciphertext' box is a 'Text Input' box labeled 'Ciphertext' containing the text '38 40 A4 2D F2 93 CB F5 2D A5 BB 46 28 0E 03 87'. Below the 'Ciphertext' box is a 'Text Output' box labeled 'Decrypted Ciphertext' containing the text 'KALMAKDANILANDOR'. In the center of the interface is a 'StringDecoder' box. To its right is a 'DES Decrypt' box with a '0%' progress indicator. Below the 'DES Decrypt' box is a 'StringDecoder' box. At the bottom left, there is a 'Text Input' box labeled 'Key' containing the text '12345678'. To its right is a 'StringDecoder' box. Below the 'StringDecoder' box is a 'DES Encrypt' box with a '0%' progress indicator. To the right of the 'DES Encrypt' box is a 'Text Input' box labeled 'PASSWORD' containing the text 'PASSWORD'. Below the 'PASSWORD' box is a 'StringDecoder' box. At the bottom right, there is a 'DES Decrypt' box with a '0%' progress indicator. To its right is a 'StringDecoder' box. A 'Fullscreen' button is located in the center of the interface, overlapping the 'StringDecoder' and 'DES Decrypt' boxes.

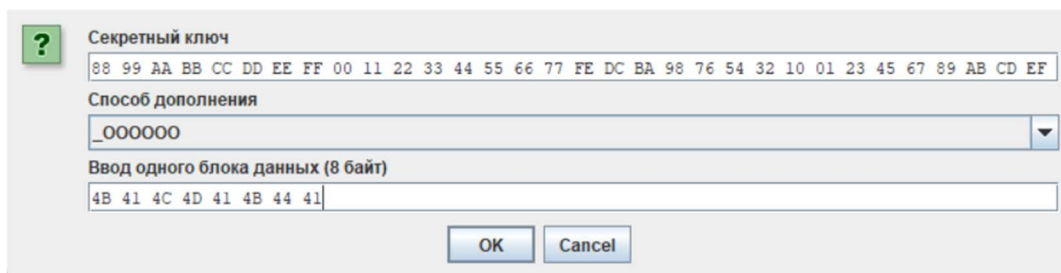
### 3. Шифр Магма

#### 3.1 Преобразования шифра Магма с помощью приложения ЛИТОРЕЯ

Исходный текст: KALMAKDA

Вид в шестнадцатеричной системе: 4B 41 4C 4D 41 4B 44 41

Ключ: 88 99 AA BB CC DD EE FF 00 11 22 33 44 55 66 77 FE DC BA 98  
76 54 32 10 01 23 45 67 89 AB CD EF



1. Определим ключ первого раунда  $K_1$ , используя схему раундовых ключей.

Раунд	1	2	3	4	5	6	7	8
Ключ	1	2	3	4	5	6	7	8
Раунд	9	10	11	12	13	14	15	16
Ключ	1	2	3	4	5	6	7	8
Раунд	17	18	19	20	21	22	23	24
Ключ	1	2	3	4	5	6	7	8
Раунд	25	26	27	28	29	30	31	32
Ключ	8	7	6	5	4	3	2	1

Схема использования раундовых ключей

Ключ первого раунда  $K_1$ : первая из восьми частей ключа, 88 99 AA BB

Полученный ключ совпадает с ключом, полученным в ЛИТОРЕЯ.

Ключ  
раунда: 88  
99 AA BB

2. Произведем первый раунд зашифровки исходного текста.

Разобьем исходный текст на два субблока:

$L = 4B\ 41\ 4C\ 4D$

$R = 41\ 4B\ 44\ 41$

Сложим по модулю  $2^{32}$  блок R с ключом первого раунда  $K_1$ :

$C9\ E4\ EE\ FC$

Результат сложения разбивается на восемь 4-битных значений (блоков кода), каждое из которых подается для замены на вход S-блока (узла таблицы замен):

Номер S-блока	Значение															
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
1	1	7	E	D	0	5	8	3	4	F	A	6	9	C	B	2
2	8	E	2	5	6	9	1	C	F	4	B	0	D	A	3	7
3	5	D	F	6	9	2	C	A	B	7	8	1	4	3	E	0
4	7	F	5	A	8	1	6	D	0	9	3	E	B	4	2	C
5	C	8	2	1	D	4	F	6	7	0	A	5	3	E	9	B
6	B	3	5	8	2	F	A	D	E	1	7	4	C	9	6	0
7	6	8	2	3	9	A	5	C	1	E	4	7	B	D	0	F
8	C	4	6	2	A	5	B	9	E	8	D	7	0	3	F	1

$94\ E8\ 96\ F0$

Циклически сдвигается полученная часть на 11 бит влево:

$44\ B7\ 84\ A7$

Вычисляется XOR L с результатом:

$0F\ F6\ C8\ EA$

Полученный результат поместим в правую часть, а R в левую:

$41\ 4B\ 44\ 41\ 0F\ F6\ C8\ EA$

Раундовое преобразование совпадает с работой программы ЛИТОРЕЯ.

Субблок L: 4B 41 4C 4D	Субблок R: 41 4B 44 41	Ключ раунда: 88 99 AA BB
Преобразование: 'сложение по модулю 2 <sup>32</sup> '		
Результат: C9 E4 EE FC		
Преобразование: 'подстановка S'		
Результат: 94 E8 96 F0		
Преобразование: 'циклический сдвиг <<11'		
Результат: 4B 41 4C 4D		
Преобразование: 'сложение XOR'		
Субблок L': 41 4B 44 41	Субблок R': 0F F6 C8 EA	Результат: 0F F6 C8 EA
Раунд №1		
<<		>>

### 3. Расшифруем полученный шифротекст

Для расшифровки необходимо поменять субблоки местами и произвести те же операции, что и для шифровки.

Поменяем местами субблоки.

L = 0F F6 C8 EA

R = 41 4B 44 41

Сложим по модулю  $2^{32}$  блок R с ключом первого раунда  $K_1$ :

C9 E4 EE FC

Результат сложения разбивается на восемь 4-битных значений (блоков кода), каждое из которых подается для замены на вход S-блока (узла таблицы замен):

Номер S-блока	Значение															
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
1	1	7	E	D	0	5	8	3	4	F	A	6	9	C	B	2
2	8	E	2	5	6	9	1	C	F	4	B	0	D	A	3	7
3	5	D	F	6	9	2	C	A	B	7	8	1	4	3	E	0
4	7	F	5	A	8	1	6	D	0	9	3	E	B	4	2	C
5	C	8	2	1	D	4	F	6	7	0	A	5	3	E	9	B
6	B	3	5	8	2	F	A	D	E	1	7	4	C	9	6	0
7	6	8	2	3	9	A	5	C	1	E	4	7	B	D	0	F
8	C	4	6	2	A	5	B	9	E	8	D	7	0	3	F	1

94 E8 96 F0

Циклически сдвигается полученная часть на 11 бит влево:

44 B7 84 A7

Вычисляется XOR L с результатом:

4B 41 4C 4D

Полученный результат поместим в левую часть, а R в правую:

4B 41 4C 4D 41 4B 44 41

K A L M A K D A

KALMAKDA

Расшифрованный текст соответствует исходному тексту.

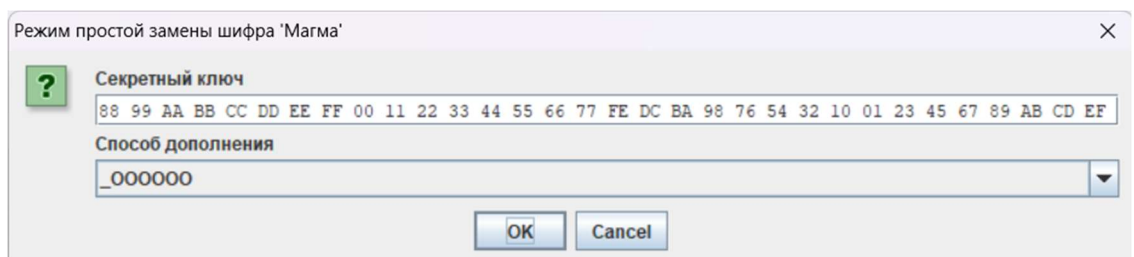
### 3.2 Исследование шифра Магма в режимах работы простой замены и простой замены с зацеплением, используя приложение ЛИТОРЕЯ (шифрование изображения в разных режимах работы)

1. Создано изображение с ФИО: КАЛМАК ДАНИИЛ АНДРЕЕВИЧ – в формате bmp.

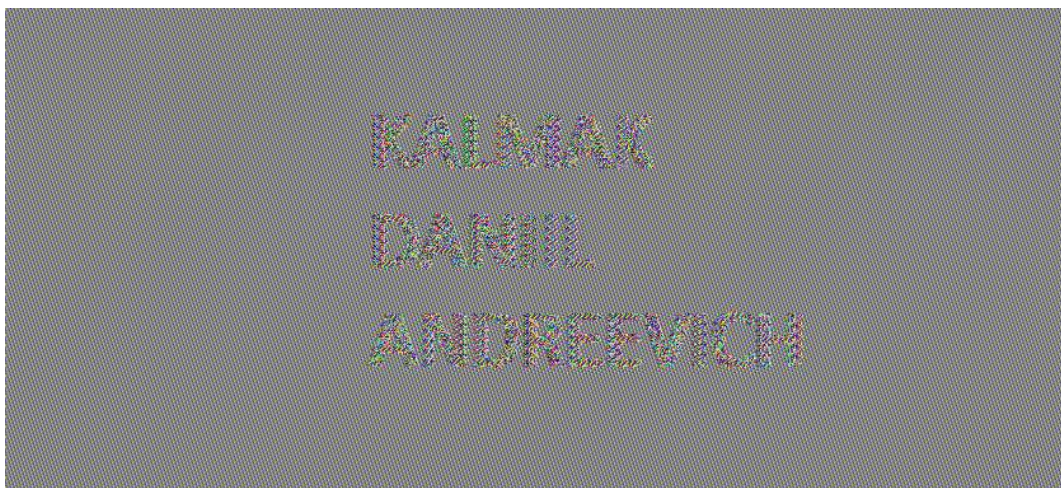
KALMAK  
DANIIL  
ANDREEVICH

Зашифровано изображение с помощью шифра Магма в режиме работы простой замены.

Ключ: 88 99 AA BB CC DD EE FF 00 11 22 33 44 55 66 77 FE DC BA 98  
76 54 32 10 01 23 45 67 89 AB CD EF







Зашифровано изображение с помощью шифра Магма в режиме работы простой замены с зацеплением.

Ключ: 88 99 AA BB CC DD EE FF 00 11 22 33 44 55 66 77 FE DC BA 98  
76 54 32 10 01 23 45 67 89 AB CD EF

Синхропосылка: 12 34 56 78 90 AB CD EF 23 45 67 89 0A BC DE F1 34  
56 78 90 AB CD EF 12

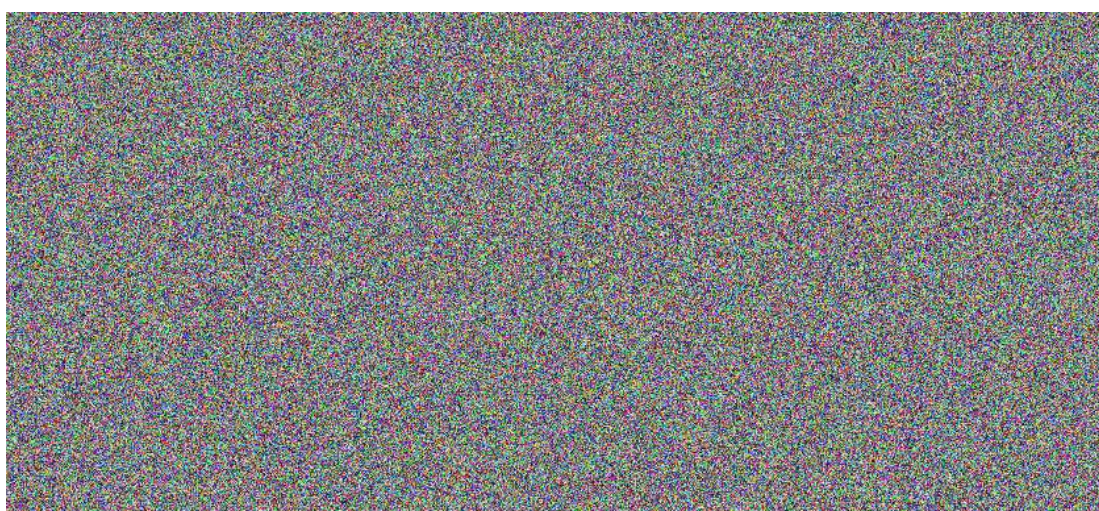
Режим простой замены с зацеплением шифра 'Магма' X

? Секретный ключ  
88 99 AA BB CC DD EE FF 00 11 22 33 44 55 66 77 FE DC BA 98 76 54 32 10 01 23 45 67 89 AB CD EF

Способ дополнения  
\_000000

Синхропосылка  
12 34 56 78 90 AB CD EF 23 45 67 89 0A BC DE F1 34 56 78 90 AB CD EF 12

OK Cancel



Изображение, зашифрованное с помощью режима простой замены, различимо. Такой режим работы шифрует одинаковые блоки одинаковым шифром.

Изображение, зашифрованное с помощью режима простой замены с сцеплением, неразлично. Такой режим работы шифрует с влиянием блоков друг на друга. Для изображений такой режим предпочтительный, поскольку получается случайный набор пикселей.

2. Сожмем исходную и две зашифрованных картинки средствами CrypTool

	Без сжатия	С сжатием
Исходное	938 кб	21 кб (97 %)
Простая замена	40 кб	38 кб (6 %)
Простая замена с сцеплением	938 кб	938 кб (0 %)

Такое соотношение обусловлено описанными выше характеристиками: одинаковый шифр для одинаковых блоков при простой замене и влияние блоков друг на друга при шифровании при простой замене с сцеплением.

## **Выводы.**

Таким образом, были исследованы три шифра: шифр DES, шифр 3-DES и Магма.

1. Шифр DES. Симметричный, текст шифруется блоками 64 бит, ключ 64 бит (56 бит фактического ключа + 8 четности). Процесс содержит две перестановки и 16 раундов Фейстеля с 48-битовыми ключами на каждый раунд.

1.1 Вручную определен ключ первого раунда, произведен первый раунд зашифровки исходного текста и успешно расшифрован шифротекст. Произведенные действия совпадают с Cryptool 2.

1.2 Время проведения атаки грубой силы растет экспоненциально для двух шифротекстов DES в режимах работы ECB и CBC, когда известна только часть ключа. Для атаки CBC требуется больше времени, чем для ECB, причем отношение времени растет с уменьшением длины известной части ключа.

2. Шифр 3-DES. Тройное использование DES.

2.1 Реализована схема в Cryptool 2 для экспериментального определения версии 3-DES. Установлено, что Cryptool 2 использует шифр 3-DES в двух модификациях: DES-EDE3 и DES-EDE2.

3. Шифр Магма. Симметричный, текст шифруется блоками 64 бит, ключ 256 бит. Процесс содержит 32 раунда Фейстеля с 32-битовыми ключами на основе ключа шифра.

3.1 Вручную определен ключ первого раунда, произведен первый раунд зашифровки исходного текста и вручную успешно расшифрован шифротекст. Произведенные действия совпадают с ЛИТОРЕЯ.

3.2 Зашифровано изображение с ФИО в режимах работы простой замены и простой замены с зацеплением. 1) Изображение в первом случае различимо в отличие от второго. 2) Все изображения были сжаты с помощью Cryptool 1. Изображение, шифрованное с помощью простой замены, сжато на 6 %, а с помощью простой замены с зацеплением на 0 %. В режиме работы простой замены одинаковые блоки шифруются в одинаковые блоки шифротекста, а при простой замене с зацеплением блоки влияют друг на друга при шифровании.

## ПРИЛОЖЕНИЕ А

### ЗАМЕЧАНИЯ К ПРОГРАММЕ ЛИТОРЕЯ

1. Циклический сдвиг на 11 бит влево выводится неверно, однако следующий результат верный.

Для 94 E8 96 F0 циклический сдвиг на 11 бит влево правильный ответ:  
44 B7 84 A7

Субблок L: 4B 41 4C 4D	Субблок R: 41 4B 44 41	Ключ раунда: 8B 99 AA BB
		Преобразование: 'сложение по модулю 2 <sup>32</sup> '
		Результат: C9 E4 EE FC
		Преобразование: 'подстановка S'
		Результат: 54 E8 96 F0
		Преобразование: 'циклический сдвиг <<11'
		Результат: 4B 41 4C 4D
		Преобразование: 'сложение XOR'
Субблок L: 41 4B 44 41	Субблок R: 0F F6 C8 EA	Результат: 0F F6 C8 EA
Раунд №1		

2. Падение субблоков замечено только на втором раунде.

Субблок L: 3D 46 CE 5E	Субблок R: 25 2D 8E C8	Ключ раунда: CC DD EE FF
		Преобразование: 'сложение по модулю 2 <sup>32</sup> '
		Результат: F2 0B 7D C7
		Преобразование: 'подстановка S'
		Результат: 22 5E 69 B9
25 2D 8E C8		Преобразование: 'циклический сдвиг <<11'
		Результат: 3D 46 CE 5E
		Преобразование: 'сложение XOR'
Раунд №2		

3. Таблица замен находится в текстовом файле, а не в программе.