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

Лабораторная работа №4
ИЗУЧЕНИЕ ШИФРОВ DES и МАГМА

Студент: _____ Порошина Алина, группа 0361

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

Санкт-Петербург 2024

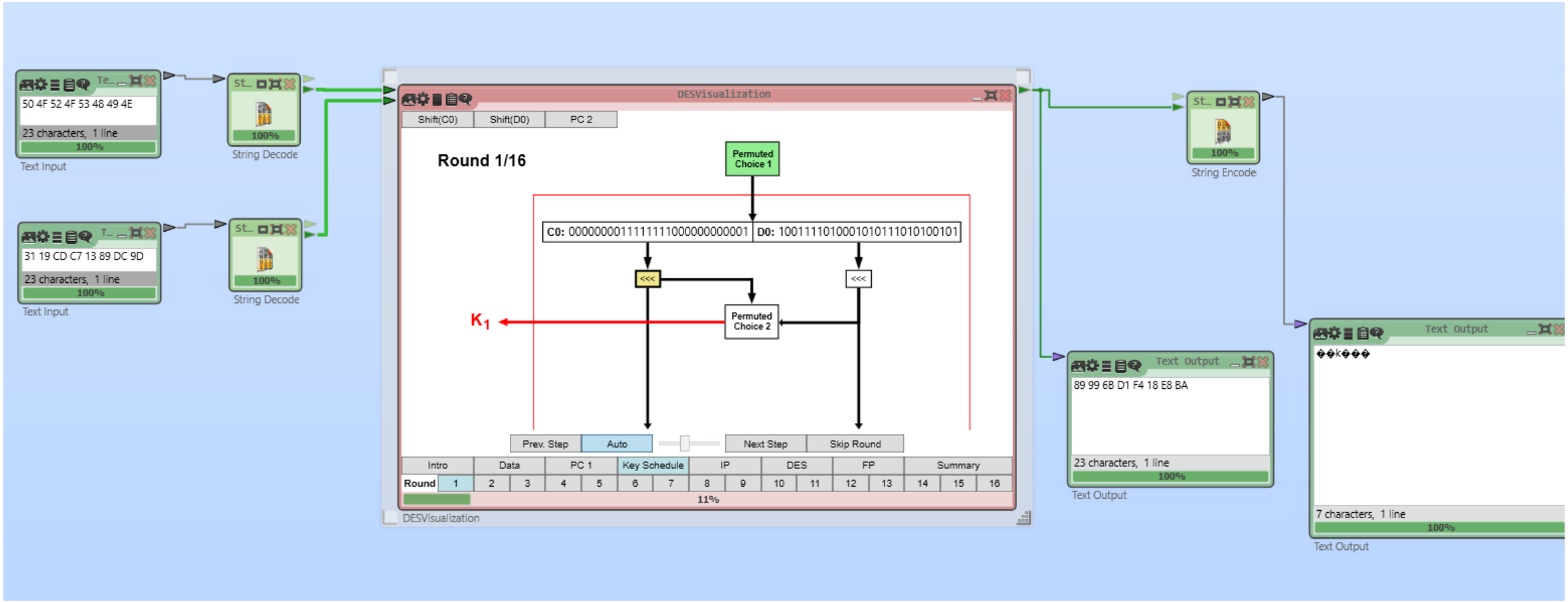
Цель работы

Цель работы: Приобретение навыков и знаний в области симметричных блочных шифров.

Задачи:

- Изучить преобразования DES
- Провести исследование DES в режимах работы ECB и CBC
- Провести исследование времени атаки методом грубой силы с известной частью ключа в режимах ECB и CBC DES
- Разработать схему в CrypTool 2 для определения версии 3DES, реализованной в CrypTool2
- Изучить преобразования ГОСТ 28147-89 Магма
- Провести исследования ГОСТ 28147-89 Магма в режимах простой замены и простой замены с зацеплением

DES: Исходные данные и результаты раунда



DES: Ручной расчет первого раунда

Ключ						
0	3	6	1	1	7	N

00110000001100110011011000110001001100010011011101001110

0	0	1	1	0	0	0	0	0	0	1	1	0	0	1	1	0	0	1	1	0	1	1	0	0	0	1	1	0	0	0	1	0	0	1	1	0	0	0	1	0	0	1	1	0	1	1	1	0	1	0	0	1	1	1	0								
0	0	1	1	0	0	0	1	0	0	0	1	1	0	0	1	1	1	0	0	1	1	0	1	1	1	0	0	0	1	1	1	0	0	0	1	0	0	1	1	1	0	0	0	1	0	0	1	1	1	0	1	1	1	0	0	1	0	0	1	1	1	0	1

0011000100011001110011011100011100010011100010011101110010011101

Расчет раундового ключа

Перестановка для ключа						
57	49	41	33	25	17	9
1	58	50	42	34	26	18
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
14	6	61	53	45	37	29
21	13	5	28	20	12	4

1	2	3	4	5	6	7	8
0	0	1	1	0	0	0	1
9	10	11	12	13	14	15	16
0	0	0	1	1	0	0	1
17	18	19	20	21	22	23	24
1	1	0	0	1	1	0	1
25	26	27	28	29	30	31	32
1	1	0	0	0	1	1	1
33	34	35	36	37	38	39	40
0	0	0	1	0	0	1	1
41	42	43	44	45	46	47	48
1	0	0	0	1	0	0	1
49	50	51	52	53	54	55	56
1	1	0	1	1	1	0	0
57	58	59	60	61	62	63	64
1	0	0	1	1	1	0	1

1	1	1	0	1	1	0
0	0	1	0	0	1	1
0	0	0	0	0	0	0
0	0	1	1	1	0	1
0	0	0	1	1	0	0
0	1	1	0	0	1	1
0	0	1	1	1	0	0
1	1	0	0	0	1	1

Сдвиг						
1	2	3	4	5	6	7
1	1	0	1	1	0	0
8	9	10	11	12	13	14
0	1	0	0	1	1	0
15	16	17	18	19	20	21
0	0	0	0	0	0	0
22	23	24	25	26	27	28
0	1	1	1	0	1	1
29	30	31	32	33	34	35
0	0	1	1	0	0	0
36	37	38	39	40	41	42
1	1	0	0	1	1	0
43	44	45	46	47	48	49
0	1	1	1	0	0	1
50	51	52	53	54	55	56
1	0	0	0	1	1	0

Сужение ключа					
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

0	0	0	1	1	1
0	1	0	0	0	0
1	0	1	1	0	0
0	0	1	0	1	1
1	0	1	1	0	1
0	1	0	1	0	0
1	1	0	0	0	0
1	0	1	1	0	1

Исходные данные:	Блок текста: 50 4F 52 4F 53 48 49 4E
	Исходный ключ: 31 19 CD C7 13 89 DC 9D
Получено:	Раундовый ключ: 000111010000101100001011101101010100110000101101

DES: Ручной расчет первого раунда

P	O	R	O	S	H	I	N														
P	O	R	O	S	H	I	N	НЕХ-БЛОК	50 4F 52 4F 53 48 49 4E												
0101000001001111010100100100111101010011010010000100100101001110																					

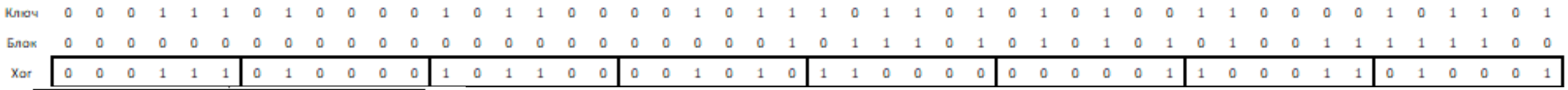
Начальная перестановка															
58	50	42	34	26	18	10	2	60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6	64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1	59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5	63	55	47	39	31	23	15	7

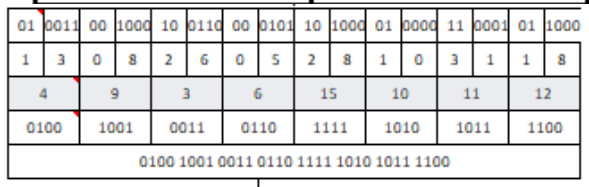
Переставленный входной текст															
1	1	1	1	1	1	1	1	0	0	0	1	0	1	0	1
1	0	0	0	1	0	1	0	0	1	0	1	1	0	1	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	1	1	0	1	0	1	0	1	0	0	1	1	1	1	0

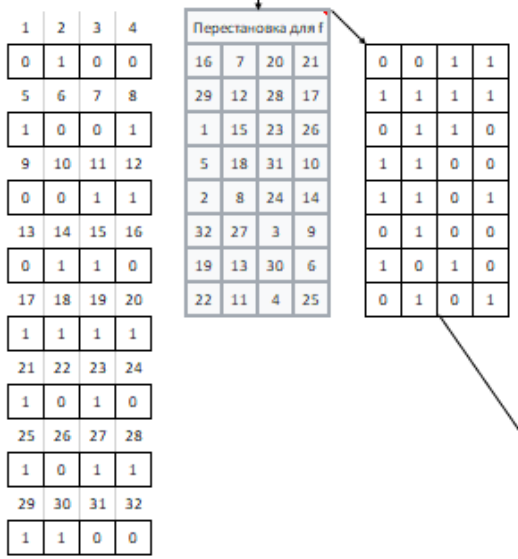
Начальная перестановка

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
0	1	0	1	0	0	0	0	0	1	0	0	1	1	1	1
17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
0	1	0	1	0	0	1	0	0	1	0	0	1	1	1	1
33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
0	1	0	1	0	0	1	1	0	1	0	0	1	0	0	0
49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64
0	1	0	0	1	0	0	1	0	1	0	0	1	1	1	0

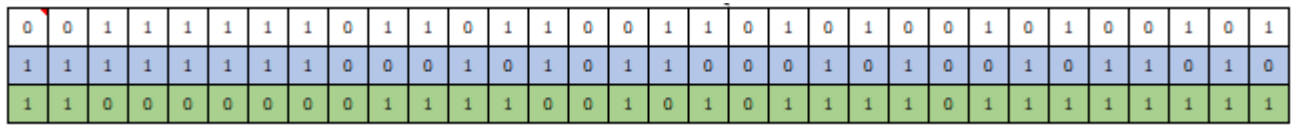
DES: Ручной расчет первого раунда



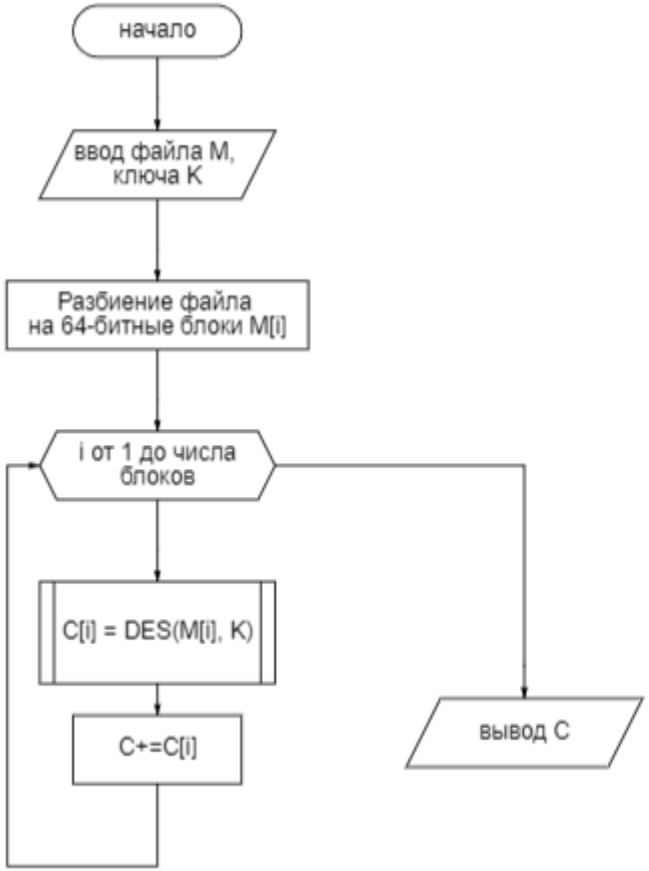


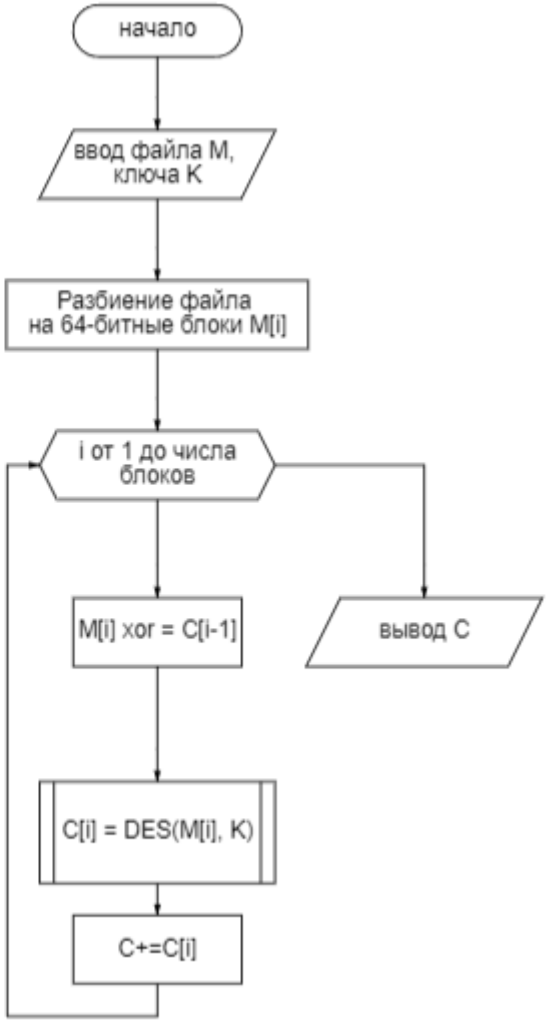


Расчет правого блока с использованием раундового ключа и S-блоков



DES: Схемы режимы ECB и CBC





Режим работы ECB:

Режим работы CBC

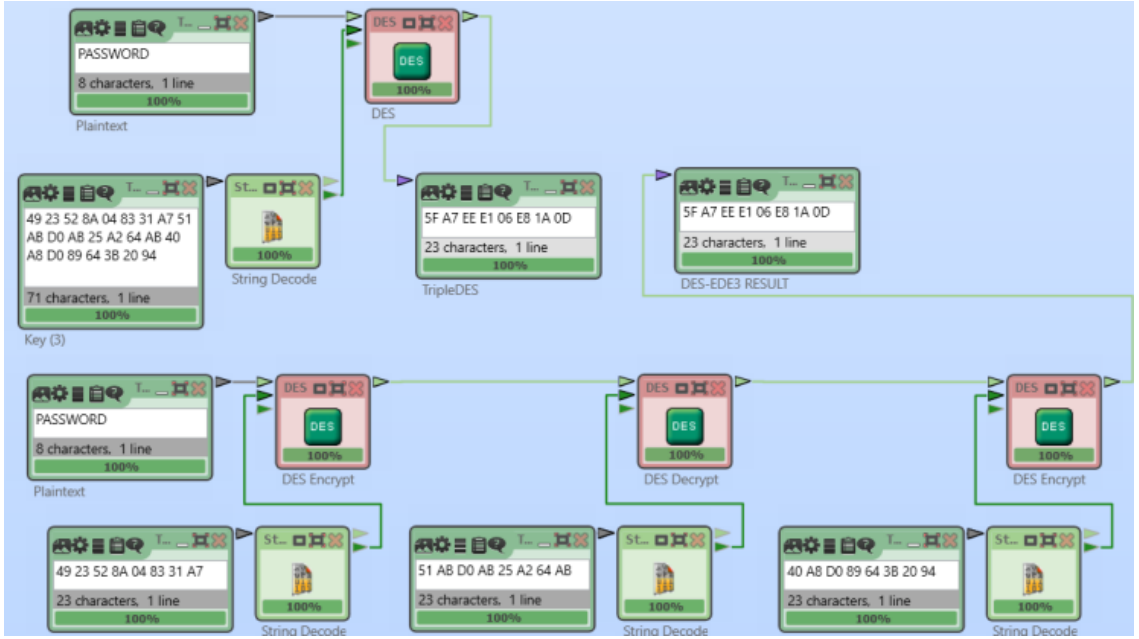
DES: Атака грубой силой

Кол-во символов	Неизвестные байты	Ожидаемое время
1061	1	< 1 с
1061	2	< 1 с
1061	3	35 с
1061	4	1,18 ч
1061	5	6,9 д
1061	6	2,5 г
1061	7	300 г
1061	8	36000 г

Кол-во символов	Неизвестные байты	Ожидаемое время
1061	1	< 1 с
1061	2	< 1 с
1061	3	23 с
1061	4	50 мин
1061	5	4,3 д
1061	6	1,5 г
1061	7	180 г
1061	8	22000 г

3-DES: Анализ реализации в CrypTool2

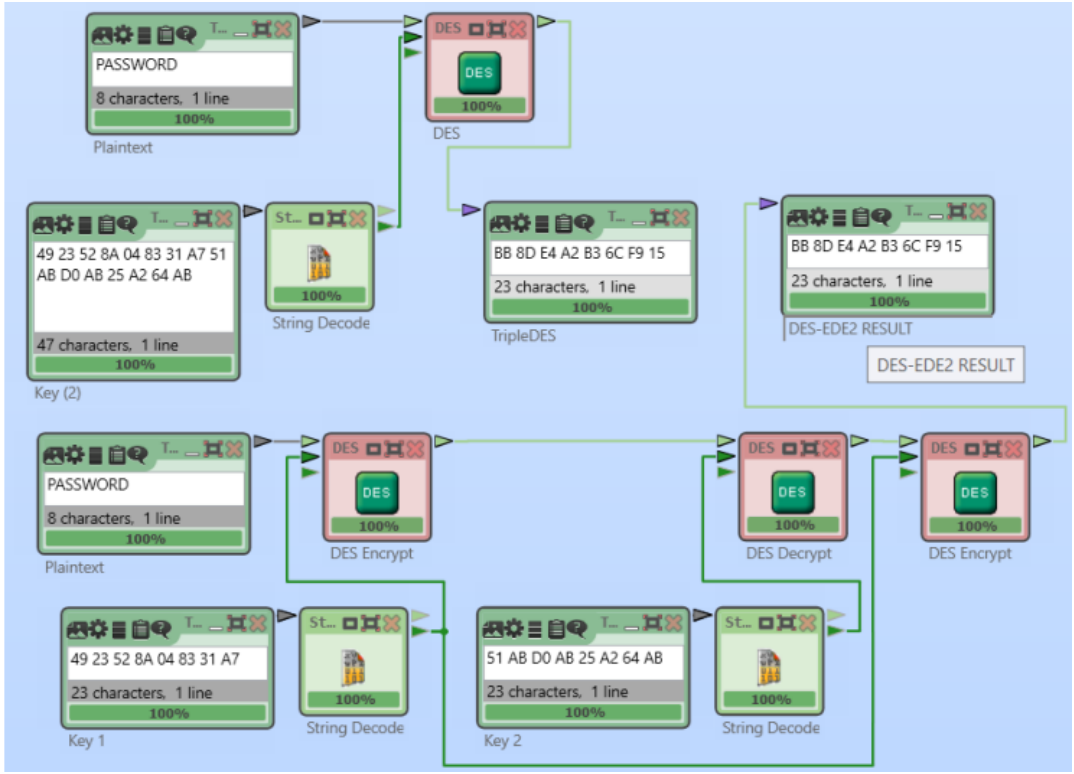
В программе CrypTool2 шифр 3-DES может быть настроен на использование ключей длиной 16 или 24 байта, что соответствует использованию двух или трех ключей для шифрования каждого отдельного блока при помощи DES. При использовании трех ключей результат будет аналогичен модели режима DES-EDE3.



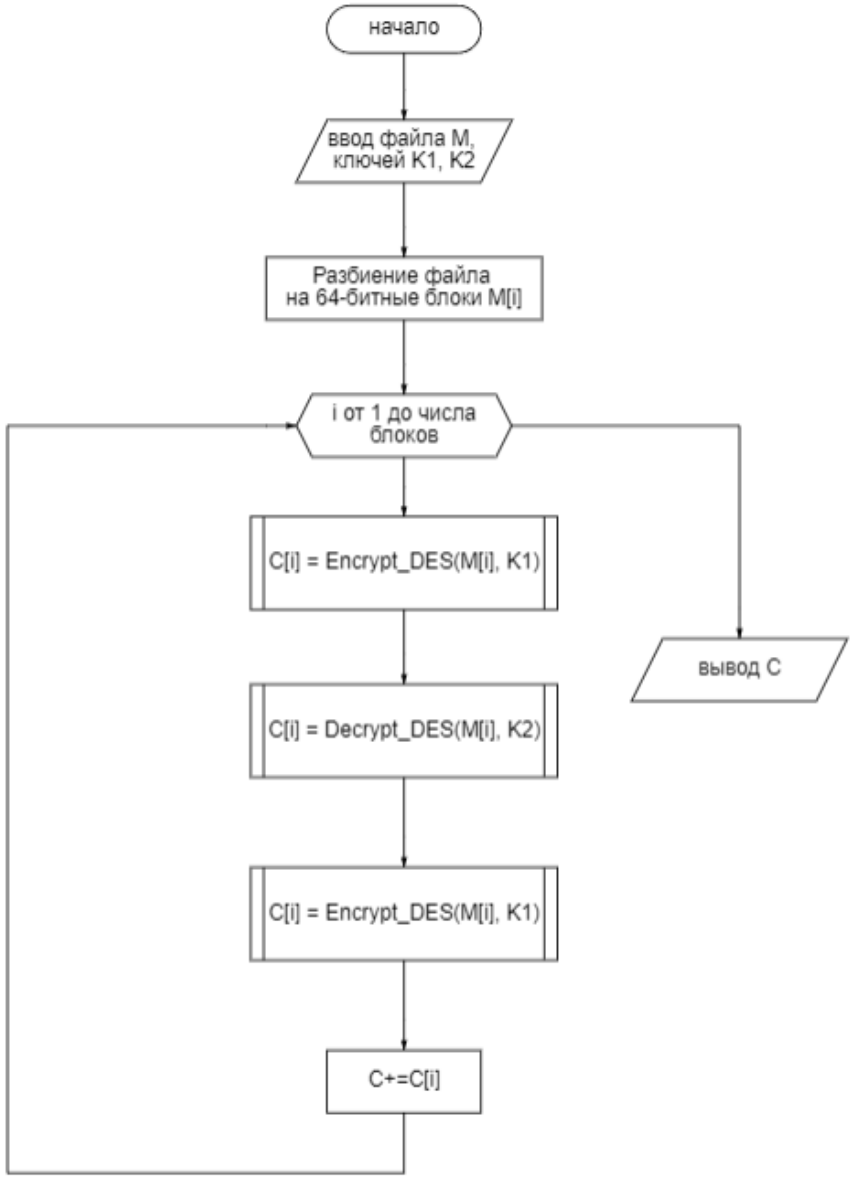
0361
HOLD ON

3-DES: Анализ реализации в CrypTool2

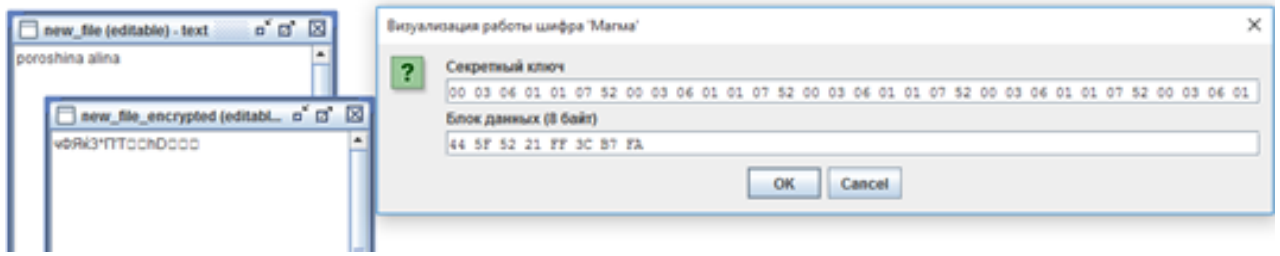
Если же на вход подать два ключа, то результат будет аналогичен построенной модели режима DES-EDE2



3-DES: Блок-схема



ГОСТ 28147-89 Магма: Расчет первого раунда шифрования



Исходные данные первого раунда:

Блок: 44 5F 52 21 FF 3C B7 FA

Раундовый ключ: 00 03 06 01

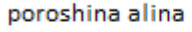
Результат:

Результат раунда: 60 2C 3B 1F

Результирующий блок: FF 3C B7 FA 60 2C 3B 1F

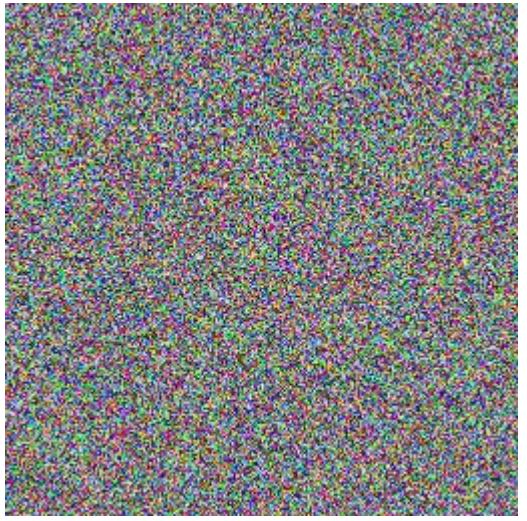
ГОСТ 28147-89 Магма: Шифрование картинок

Исходная картинка

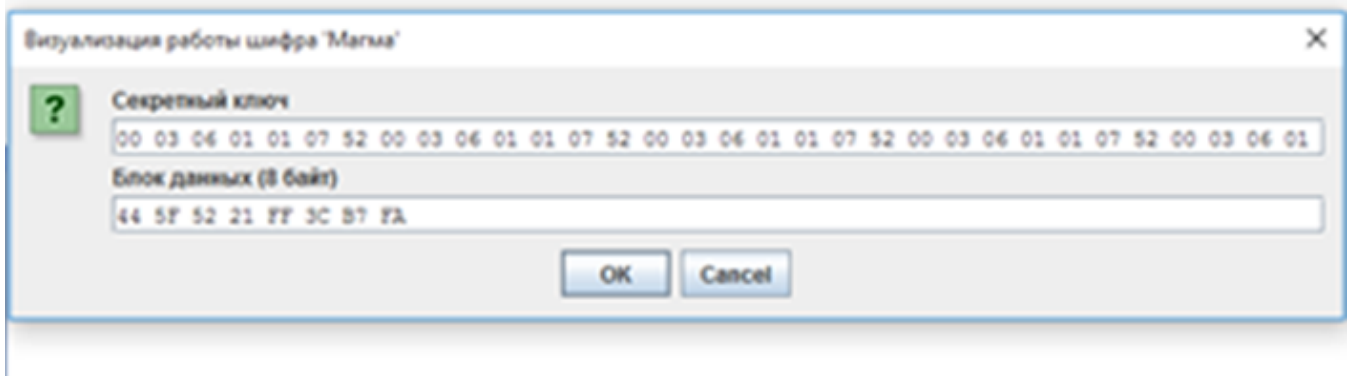


Шифровка ECB

Шифровка CBC



Ключ шифрования

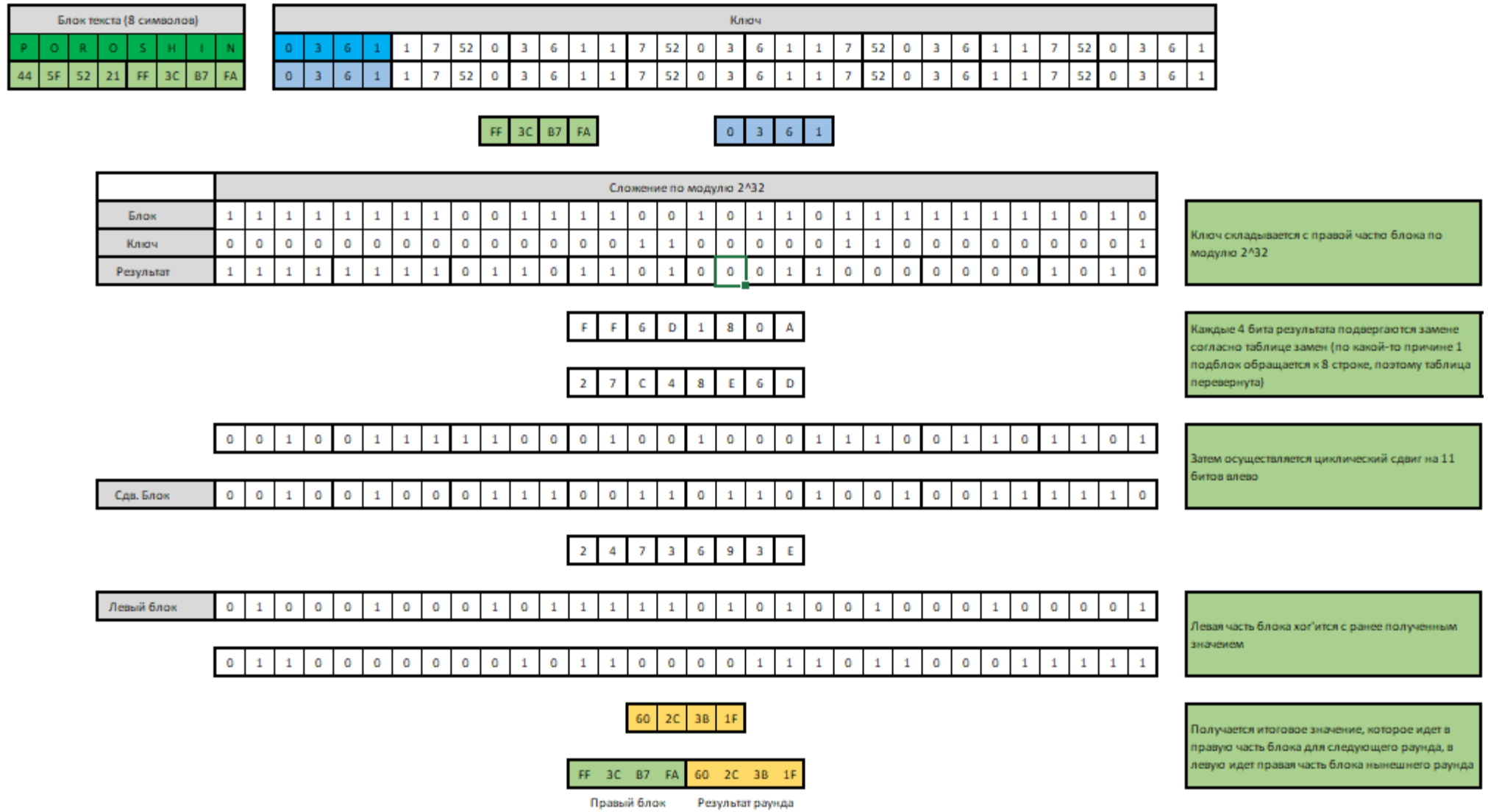


Результаты сжатия

Картинка	Процент сжатия, %
Начальная	98
ECB	11
CBC	0

0361 HOLD ON

ГОСТ 28147-89 Магма: Расчет первого раунда шифрования



Выводы

Заключение DES:

Изучен шифр DES и выявлены его следующие основные характеристики:

- Шифр блочный, симметричный;
- Длина блока на входе – 64 бит;
- Длина ключа – 64 бит(56 бит ключа + 8 бит четности), на его основе генерируется раундовые ключи;
- Алгоритм состоит из 2 перестановок(начальной и конечной) и 16 раундов Фейстеля.

Проведены ручные расчеты раундового ключа и результата для первого раунда, полученный результат совпадает с результатом автоматизированных расчетов CrypTool 2.

Заключение DES в режимах ECB и CBC:

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

- В режиме ECB каждый блок текста шифруется независимо поданным ключом;
- В режиме CBC на шифрование каждого последующего блока влияет результат шифрования предыдущего.

Средствами CrypTool 1 оценено время проведения атаки “грубой силой” при различном количестве известных байтов ключа для двух режимов и выявлены их следующие характеристики:

- Для текста, зашифрованного в режиме CBC время проведения атаки примерно в 2 раза больше, чем для текста, зашифрованного в режиме ECB.

Заключение 3DES:

Изучена работа 3DES в версиях 2EDE и 3EDE и выявлены его следующие основные характеристики:

- При подаче ключа размером в 128 бит 3DES работает по версии 2EDE и используется 2 ключа (первая половина входного ключа для этапов “зашифрования” и вторая половина для этапов “расшифрования”);
- При подаче ключа размером в 192 бит 3DES работает по версии 3EDE и используется 3 ключа (первая треть входного ключа для первого этапа “зашифрования”, вторая треть для этапа “расшифрования” и третья треть для второго этапа “зашифрования”).

Заключение ГОСТ 28147-89 Магма:

Изучен шифр ГОСТ 28147-89(“Магма”) и выявлены его следующие основные характеристики:

- Шифр блочный, симметричный, длина блока на входе – 64 бит;
- Длина ключа – 256 бит, на его основе генерируются раундовые ключи. Алгоритм состоит из 32 раундов сети Фейстеля.

Приведены ручные расчеты и получены результата для первого раунда, полученный результат совпадает с результатом автоматизированных расчетов (ЛИТОРЕЯ).

Спасибо за внимание!
Готова ответить на ваши вопросы.