Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»

им. В.И. Ульянова (Ленина)

Лабораторная работа №4

ИЗУЧЕНИЕ ШИФРОВ DES, 3DES И МАГМА

Студент: _____ Выонг В.З, группа 1362

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

Санкт-Петербург 2025

Цель работы

Цель: Приобретение навыков работы с шифрами DES, 3DES и ГОСТ 28147-89 Магма

Задачи:

1. Изучить преобразования DES по шаблонной схеме DES Visualisation из CrypTool 2;
2. Провести исследование DES в режимах работы ECB и CBC, используя CrypTool 1;
3. Разработать схему в CrypTool 2 для экспериментального определения всех тех версий 3-DES, которые реализованы в Cryptool 2;
4. Изучить преобразования шифра Магма с помощью приложения ЛИТОРЕЯ;
5. Провести исследование шифра Магма в режимах работы простой замены и простой замены с зацеплением, используя приложение ЛИТОРЕЯ.

Визуализация алгоритма зашифрования DES в инфографике

Открытый текст (hex): 01 A2 B3 C4 D5 E6 07 F8

Ключ (hex): 13 34 57 79 9B BC DF F1

Round	Left	Right	Key
1	10111110101001101000000001100110	10010111011110100110001001010101	00011011000000101110111111111100011100000011100010
2	10010111011110100110001001010101	00011110101011111011111110110111	01111001101011101101100111011011110010011110010 1
3	00011110101011111011111110110111	11110101001001101100010011000110	01010101111111001000101001000010110011111001100 1
4	11110101001001101100010011000110	01000111111001010101111011101110	01110010101011011101011011011001101010001110 1
5	01000111111001010101111011101110	10001011101000011010001111000000	01111100111011000000011111101011010100111010100 0
6	10001011101000011010001111000000	01010001001000101101110111110111	01100011101001010011111001010000011110110010111 1
7	01010001001000101101110111110111	00100010000100001000110001011000	11101100100001001011011111110110000110001011110 0
8	00100010000100001000110001011000	00100110111000011101001000111010	11110111100010100011101011000001001110111111101 1
9	00100110111000011101001000111010	01111111000111010111000110000110	11100000110110111110101111101101111001111000000 1
10	01111111000111010111000110000110	00101100000010110001101010001010	10110001111100110100011110111010010001100100111 1
11	00101100000010110001101010001010	11000011111001001111110101001000	00100001010111111010011110111011010011100001 10
12	11000011111001001111110101001000	00010000001000001111000001101001	01110101011100011111010110010100011001111110100 1
13	00010000001000001111000001101001	01010001111000000011000001110001	10010111110001011101000111111010101110100100000 1
14	01010001111000000011000001110001	11100100011110000111101010001000	01011111010000111011011111110010111001110011101 0
15	11100100011110000111101010001000	00011101001010100101011011011110	10111111100100011000110100111101001111110000101 0
16	00011101001010100101011011011110	00101100010101101011111111010010	11001011001111011000101100001110000101111111010 1

Шифровка (bin): 10000100 00111111 11011110 11100110 10011111 01100100 00011011 00000111

Шифровка (hex): 84 3F DE E6 9F 64 1B 07

DES: Начальная и конечная перестановки

Открытый текст (bin)

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

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

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

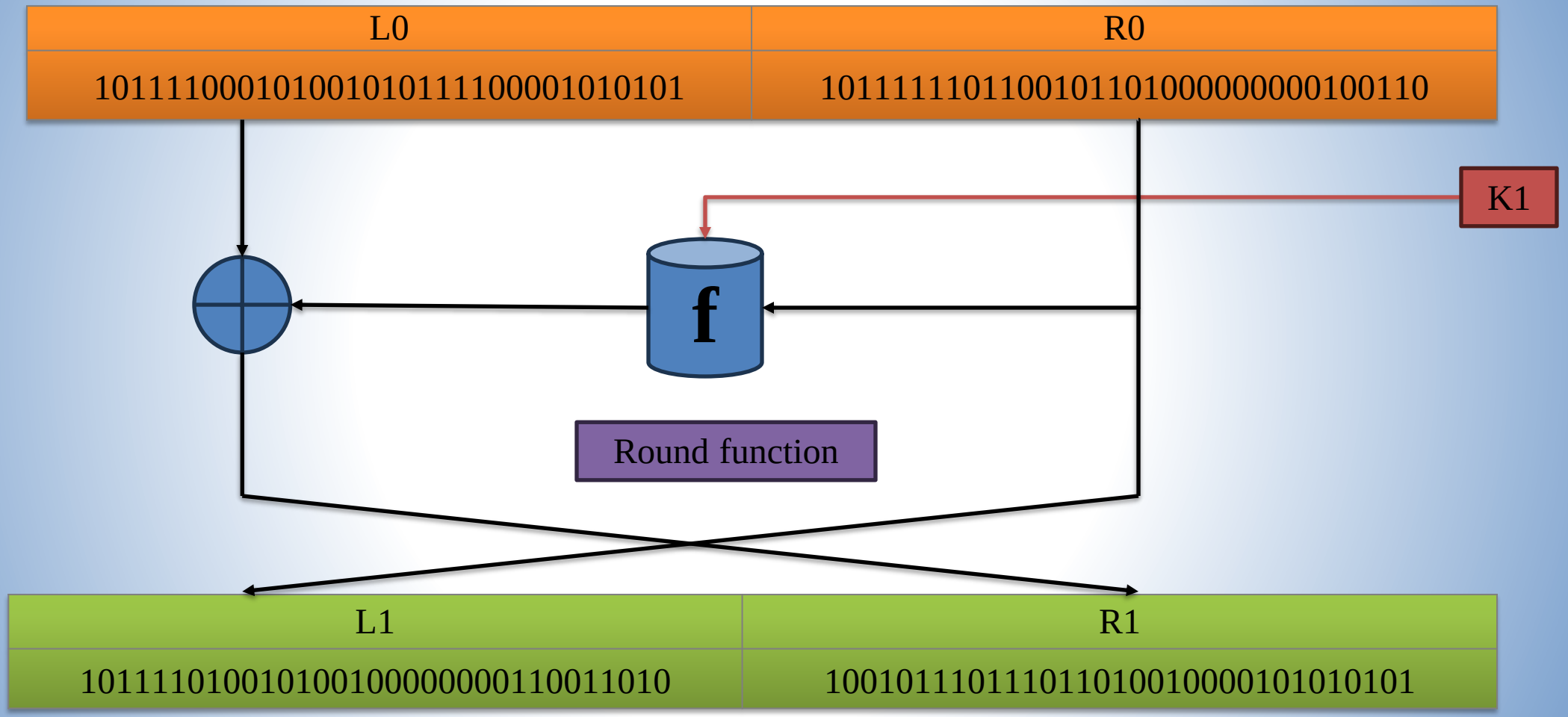
DES: Начальная и конечная перестановки

Шифротекста (после 16-ого раунда)															
0 0 0 1 1 1 0 1	0 0 1 0 1 0 1 0	0 0 1 0 1 0 1 1	0 1 1 0 1 1 1 1	0 0 0 1 0 1 1 0	0 0 0 1 0 1 0 1	1 0 1 1 1 1 1 1	0 1 0 0 1 0								

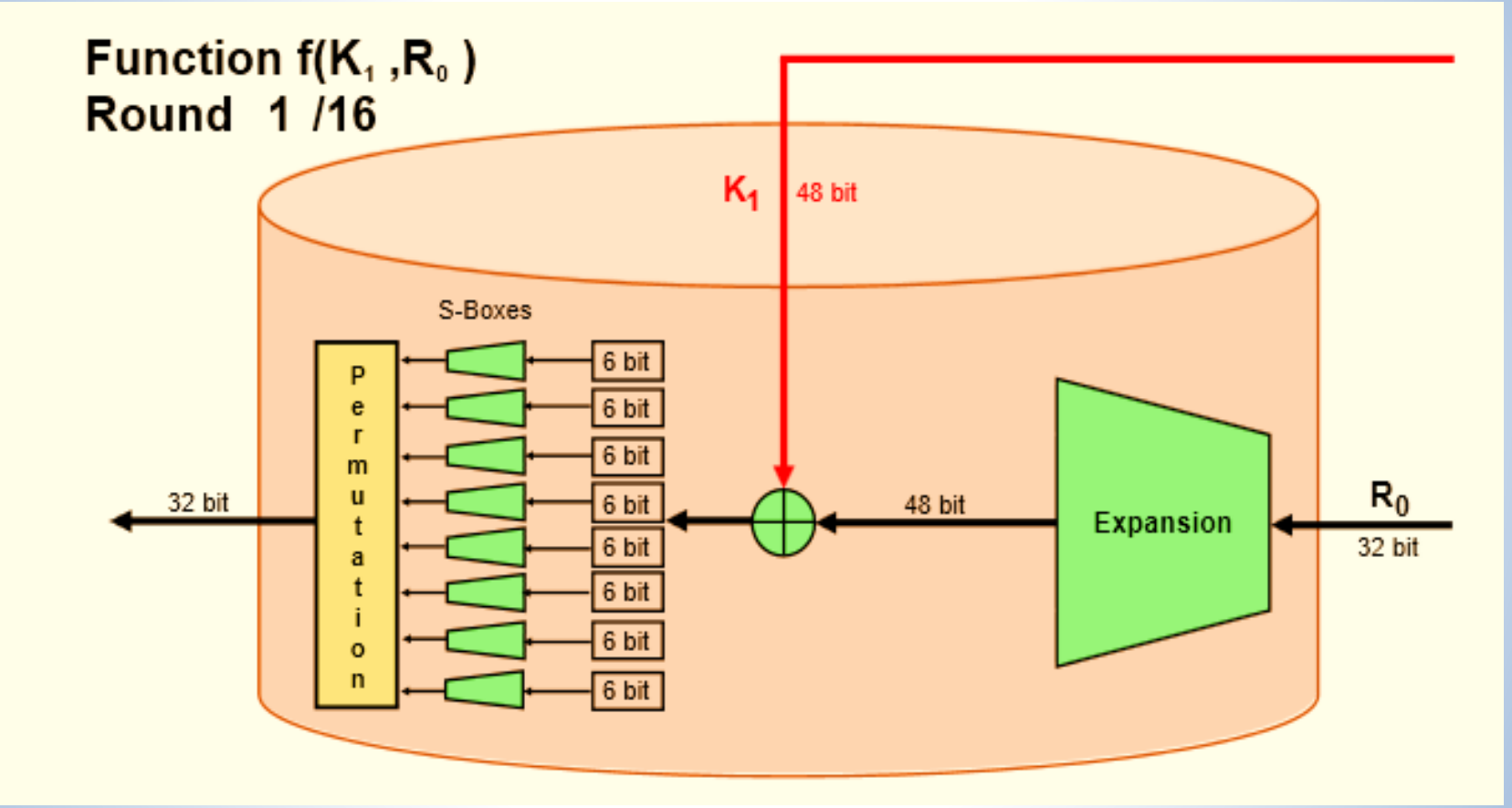
Конечная перестановка															
40	8	48	16	56	24	64	32	39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30	37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28	35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26	33	1	41	9	49	17	57	25

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

DES: Раунды DES



DES: Функция шифрования DES



DES: Алгоритм развертывания ключа DES

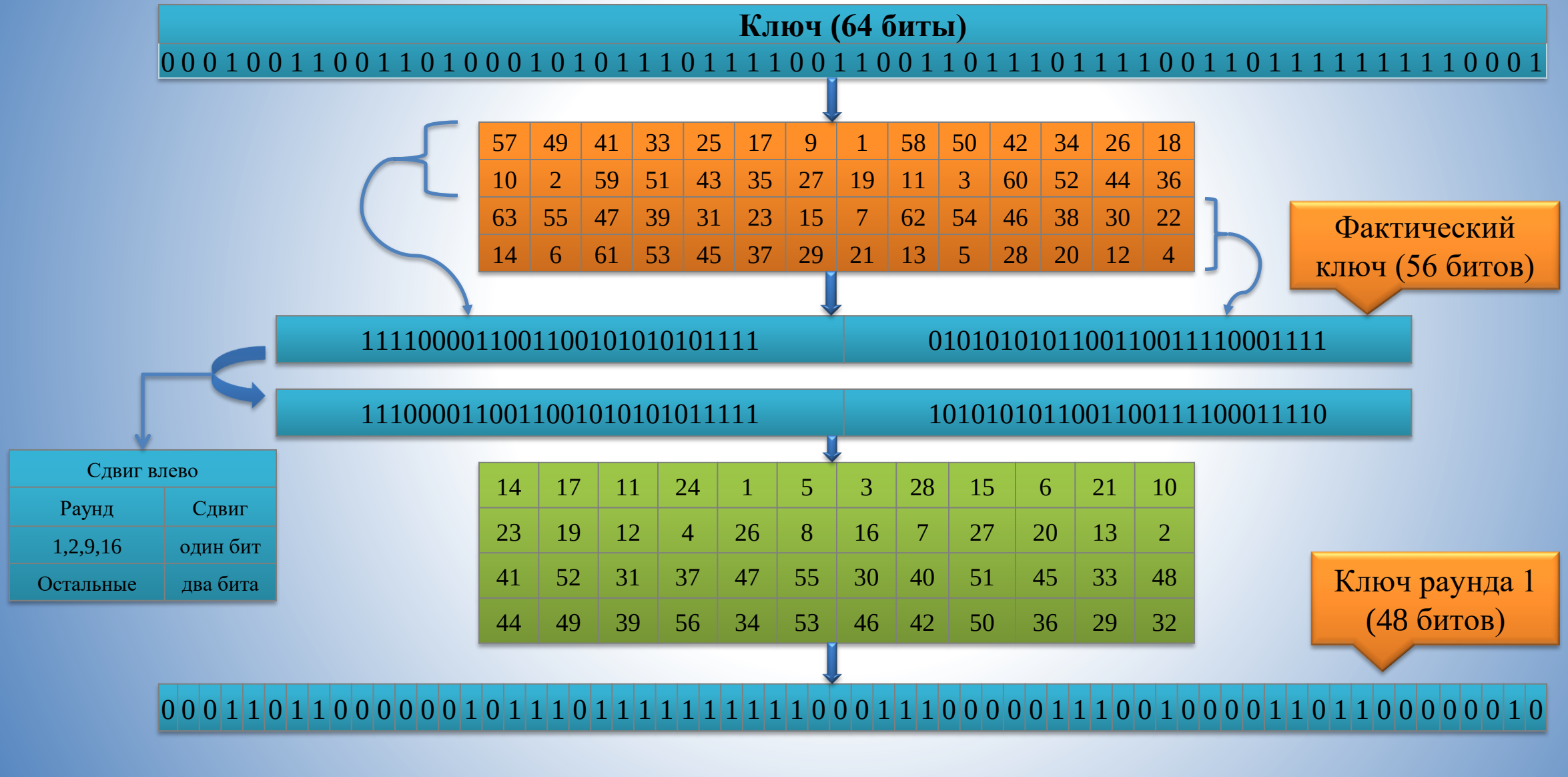


Схема протокола зашифрования сообщения в CrypTool 2

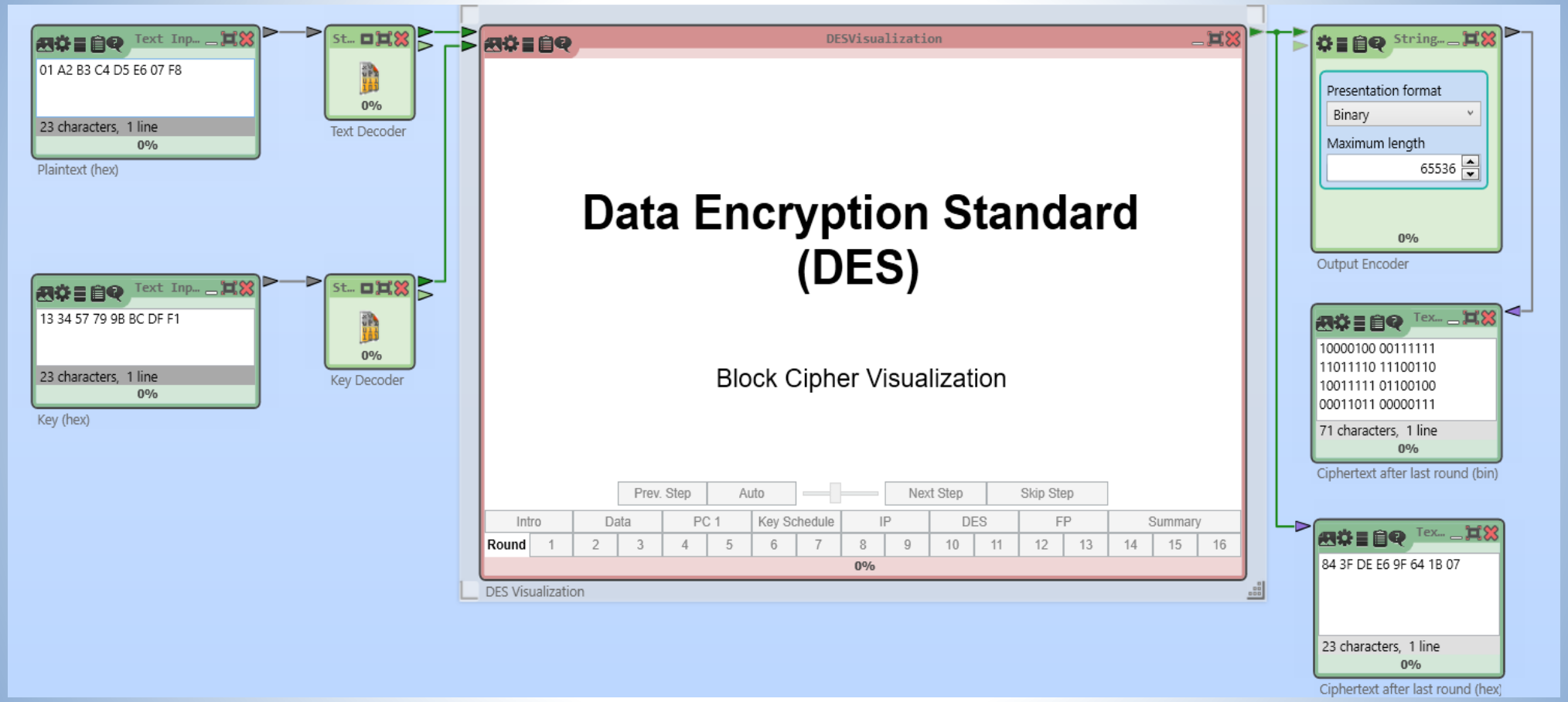
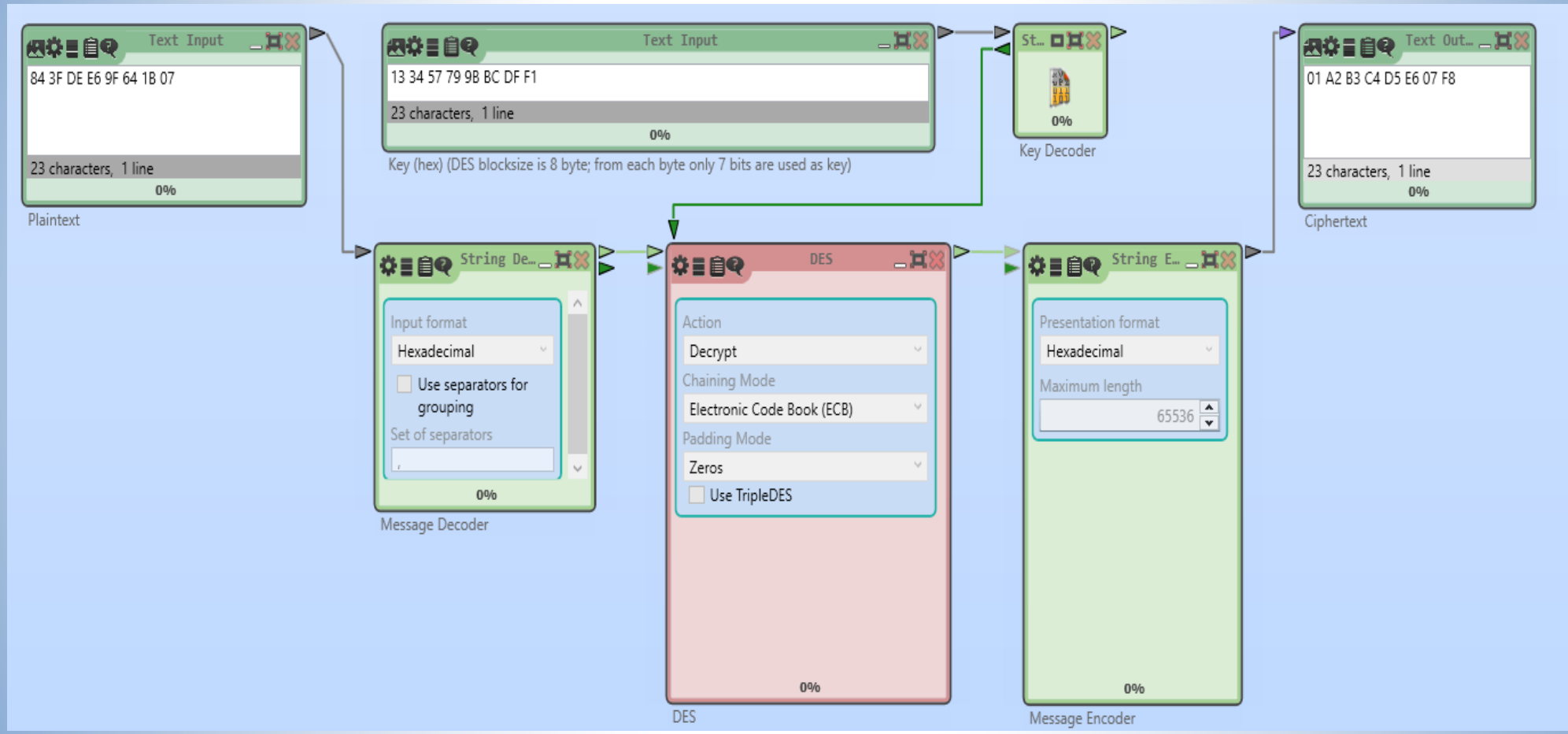
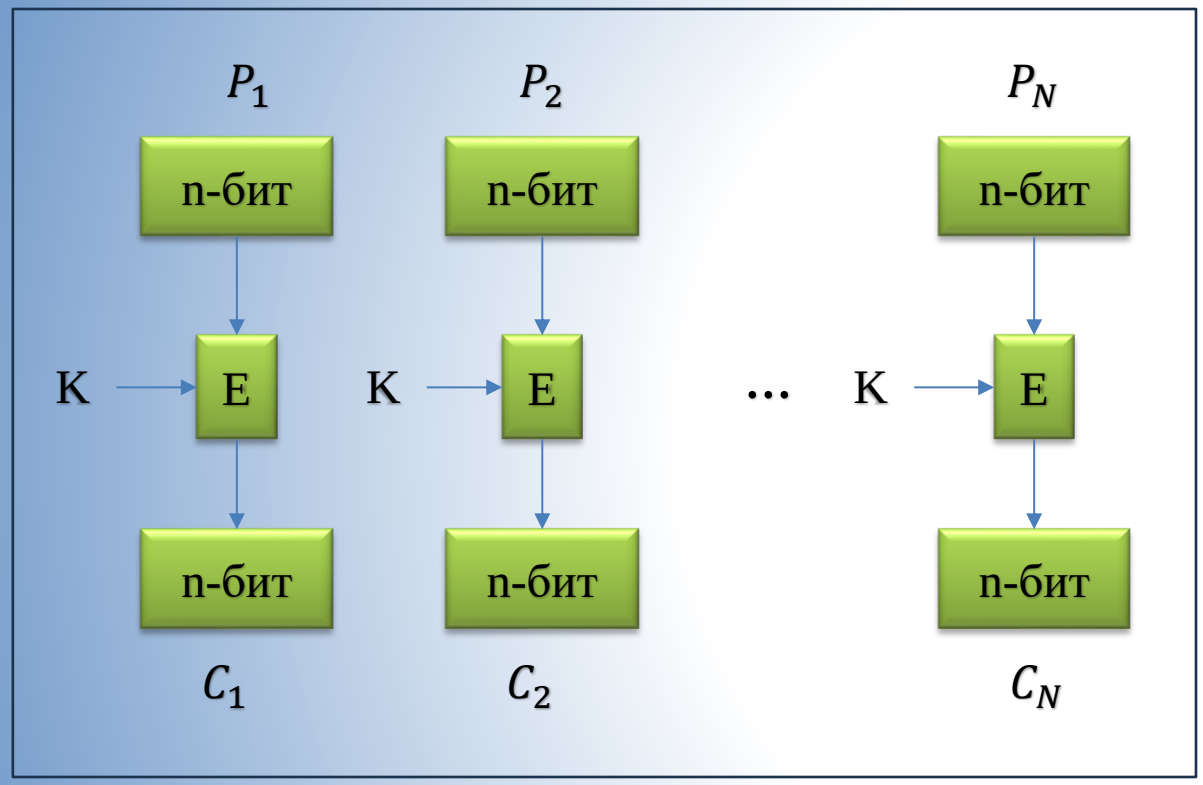


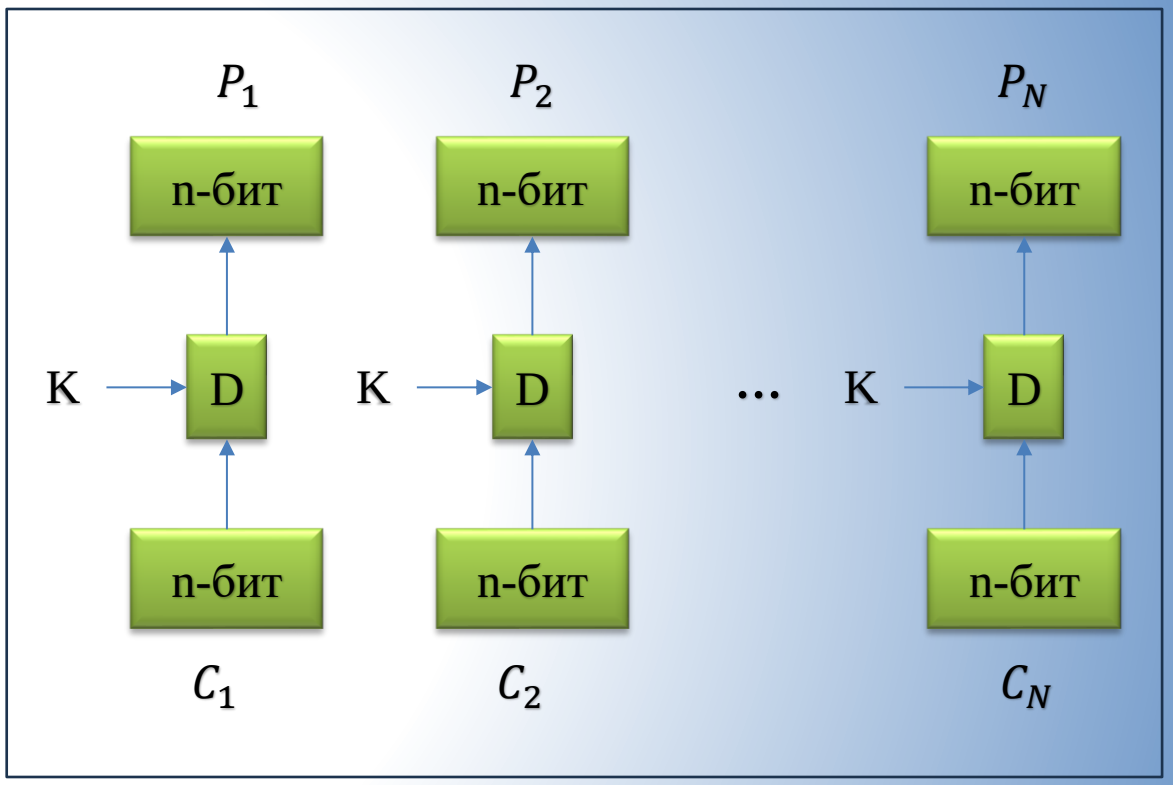
Схема протокола расшифрования сообщения в CrypTool 2



DES: Схемы режимов ECB



Шифрование

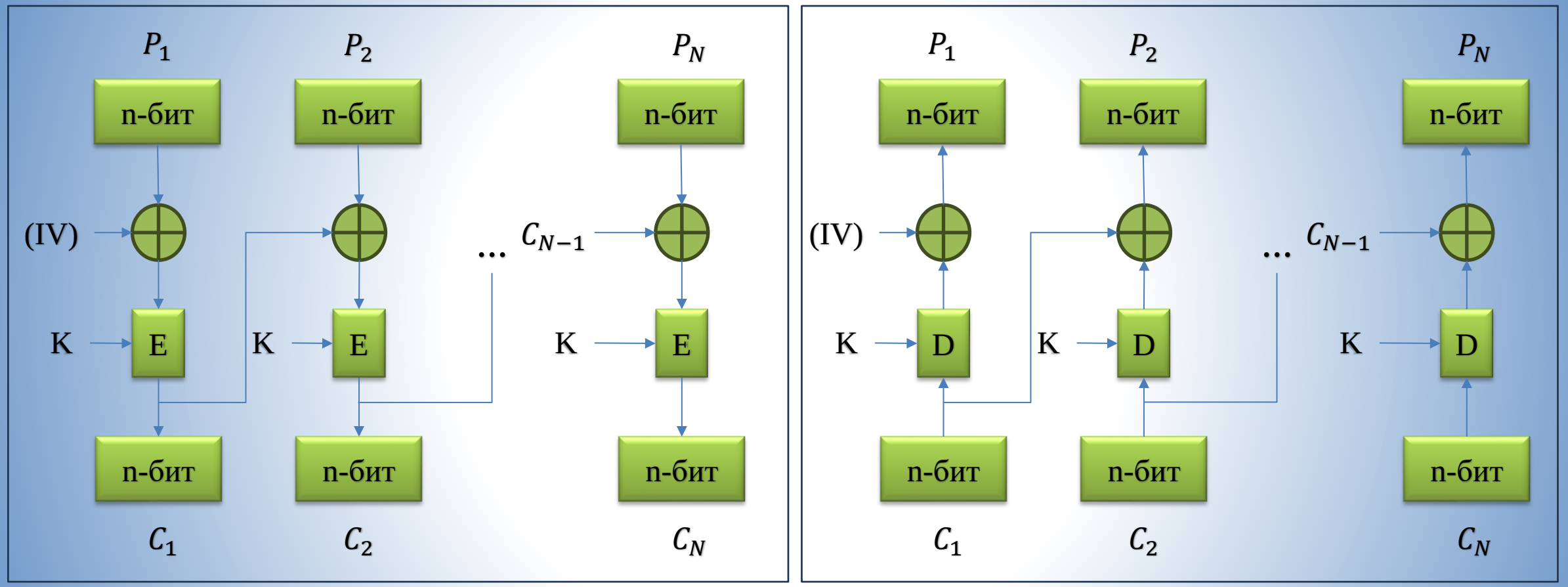


Дешифрование

E - Шифрование
P_i - Блок исходного текста i
K - Секретный ключ

D - Дешифрование
C_i - Блок зашифрованного текста

DES: Схемы режимов CBC



Шифрование

Дешифрование

E - Шифрование
P_i - Блок исходного текста i
K - Секретный ключ

D - Дешифрование
C_i - Блок зашифрованного текста

DES: Атаки "грубой силы"

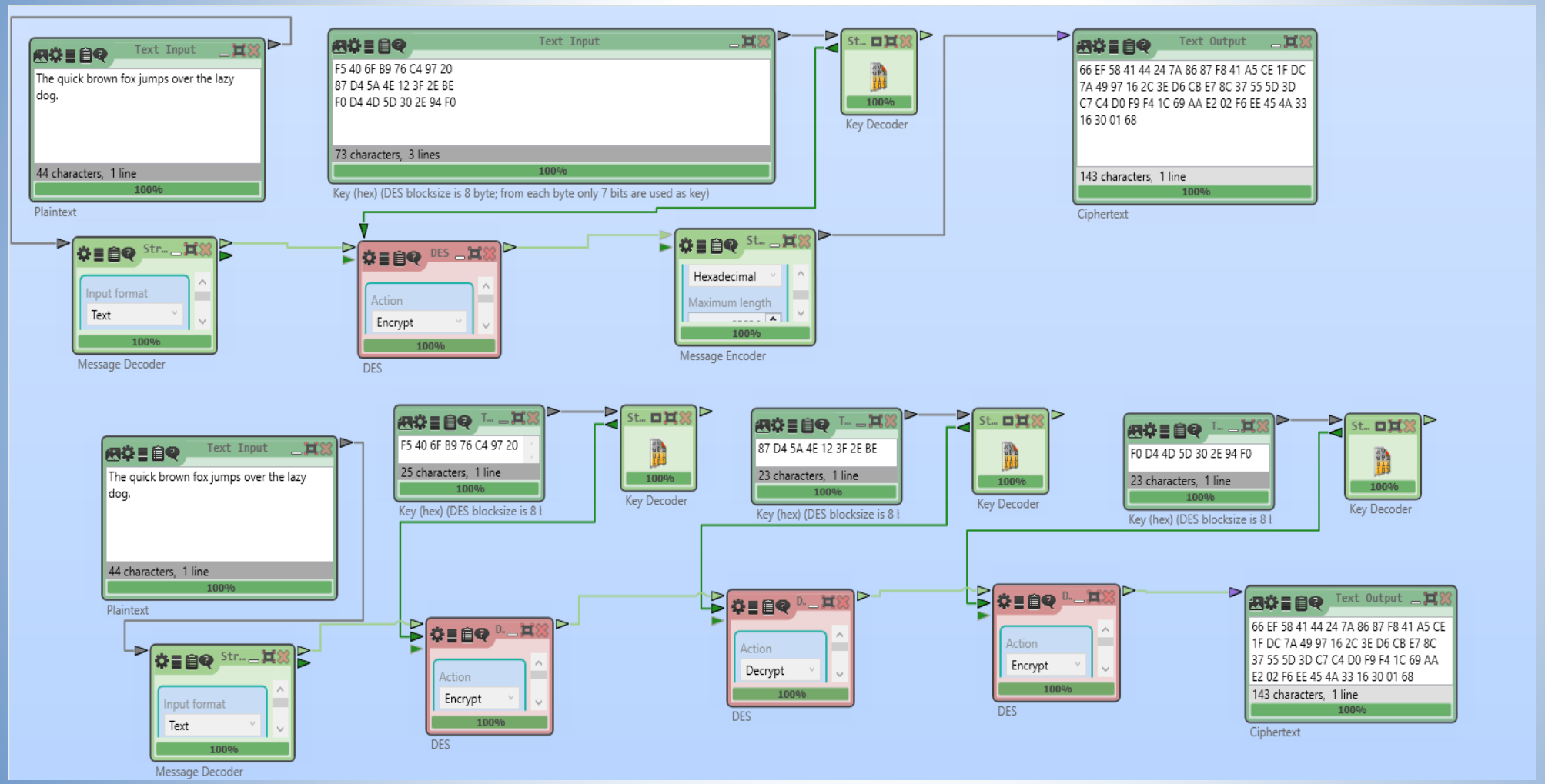
Кол-во символов	Известные байты	Ожидаемое время
1061	7	< 1 с
1061	6	< 1 с
1061	5	~ 23 с
1061	4	~ 50 мин
1061	3	~ 4.3 д
1061	2	~ 1.5 г
1061	1	~ 180 г
1061	0	~ 22000 г

DES режимов ECB

Кол-во символов	Известные байты	Ожидаемое время
1061	7	< 1 с
1061	6	< 1 с
1061	5	~ 35 с
1061	4	~ 1.18 ч
1061	3	~ 6.9 д
1061	2	~ 2.5 г
1061	1	~ 300 г
1061	0	~ 36000 г

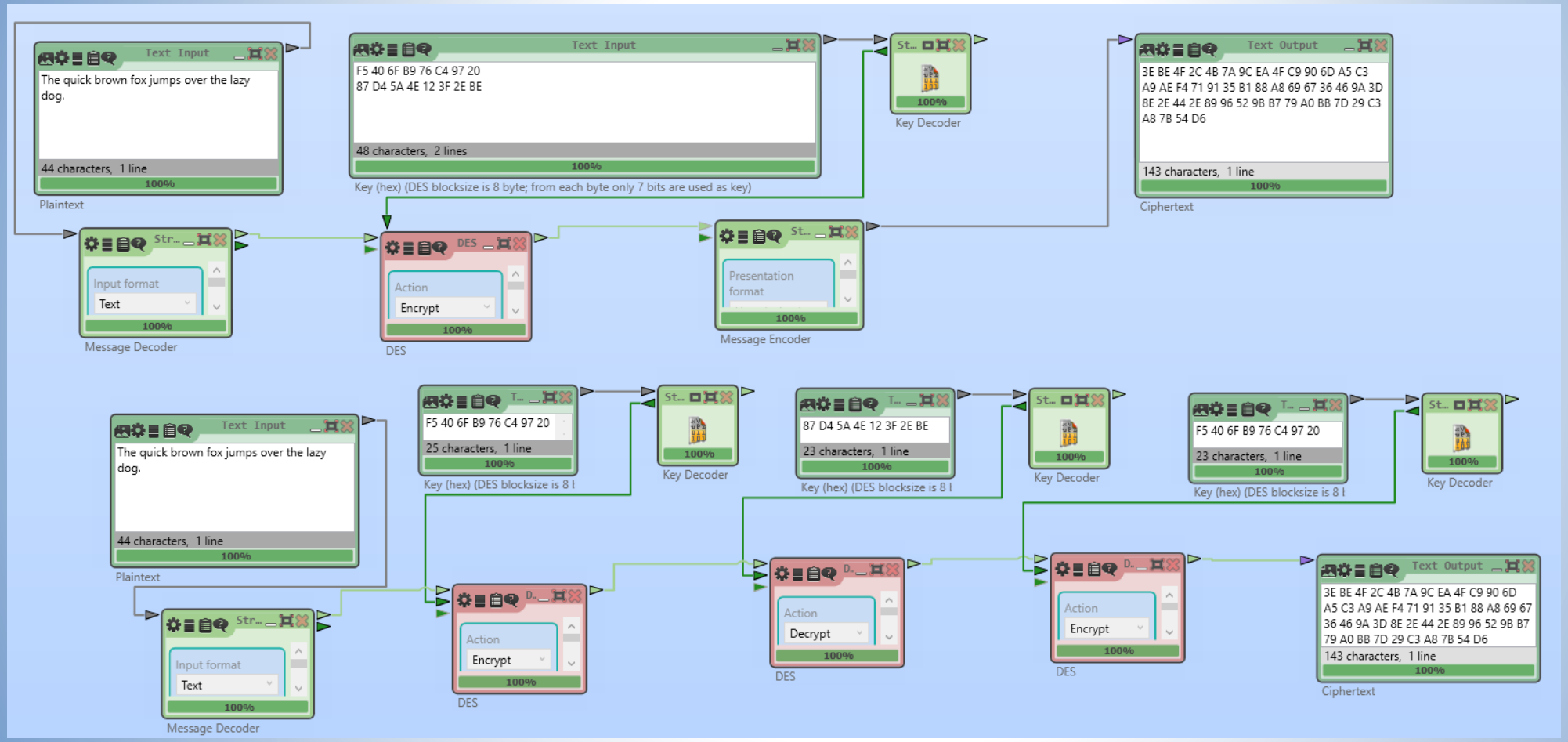
DES режимов CBC

3-DES: Разработанная схема в CrypTool 2



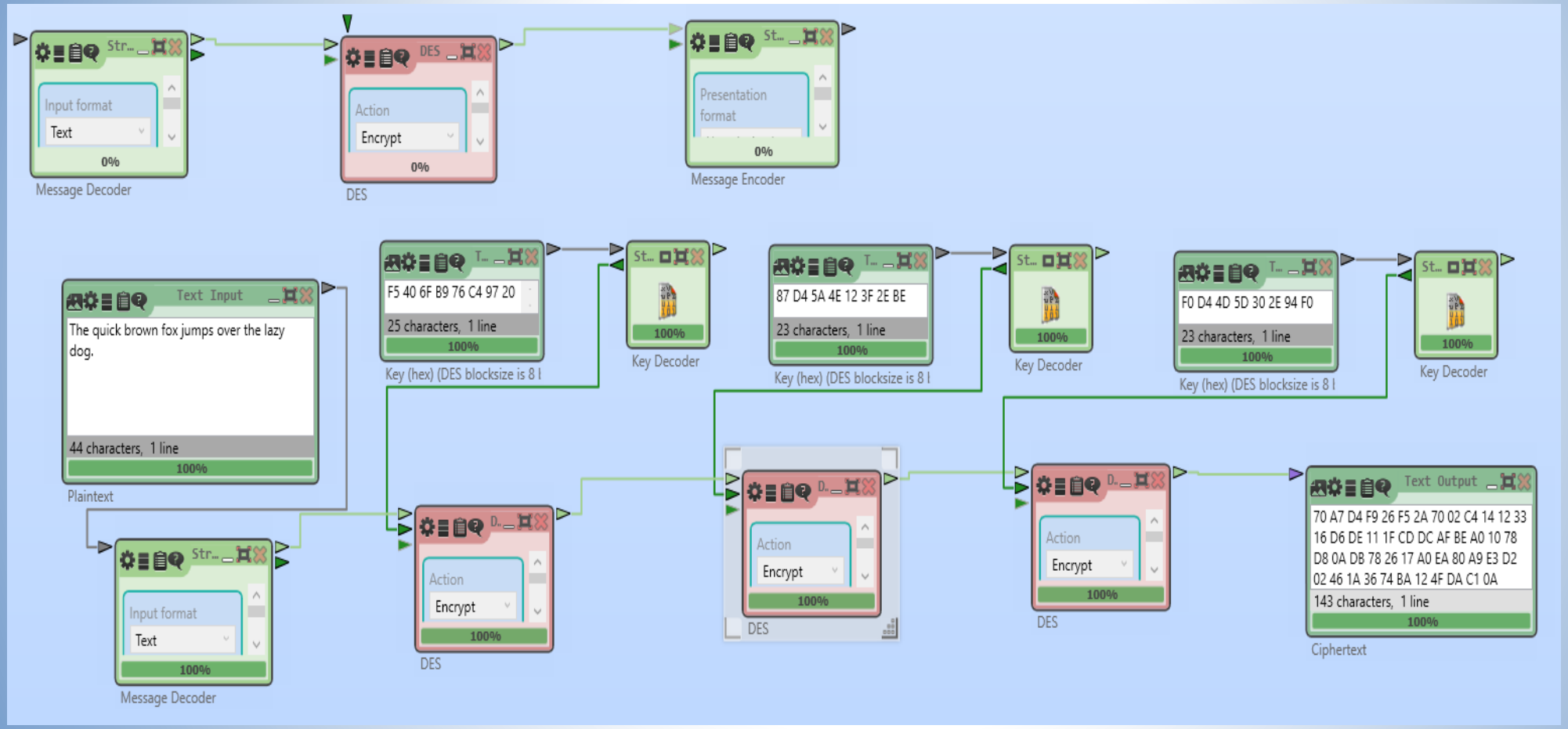
Модель режима DES-EDE3

3-DES: Разработанная схема в CrypTool 2



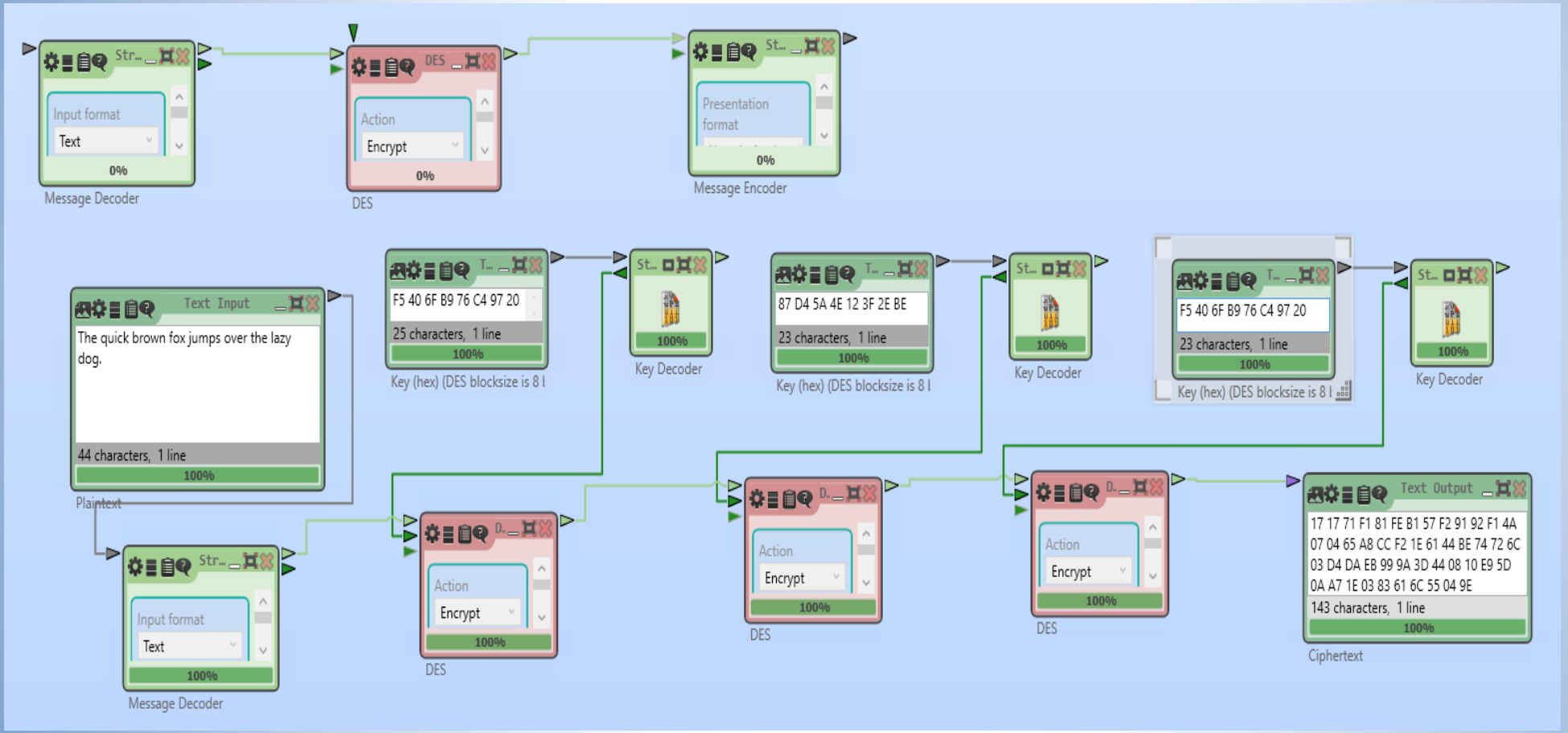
Модель режима DES-EDE2

3-DES: Разработанная схема в CrypTool 2



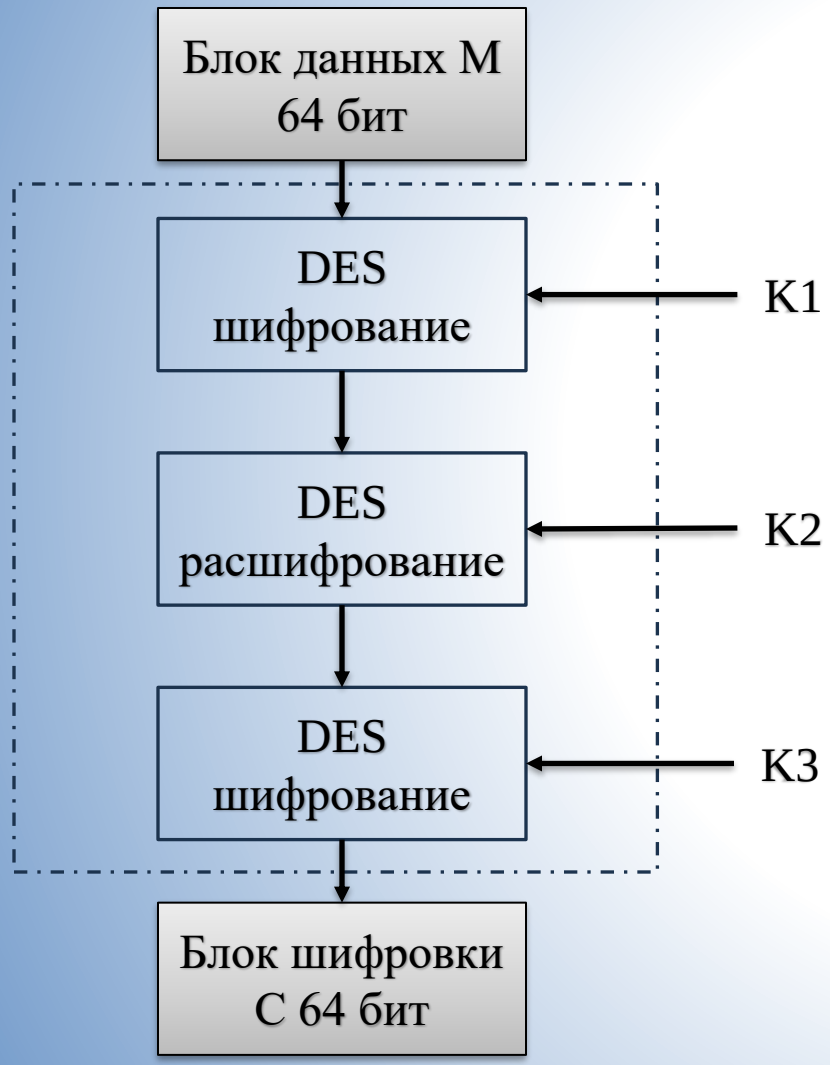
Модель режима DES-EEE3

3-DES: Разработанная схема в CrypTool 2

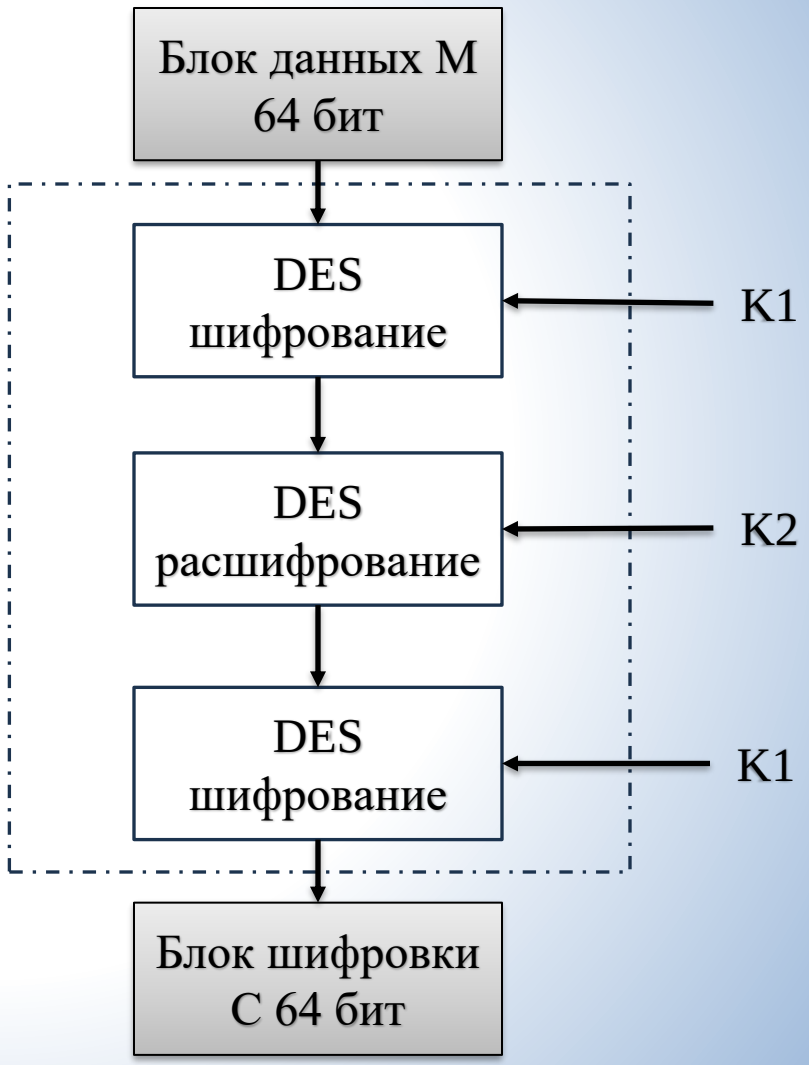


Модель режима DES-EEE2

3-DES: Схема алгоритма шифрования DES-EDE3, DES-EDE2

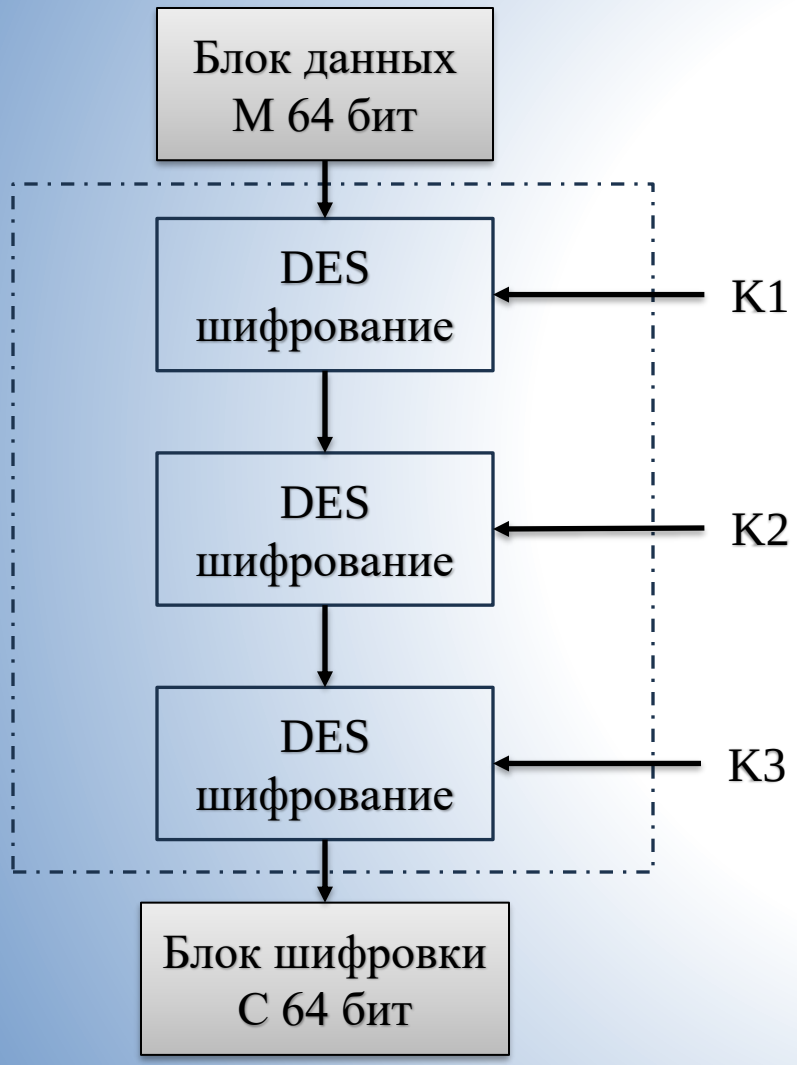


DES-EDE3

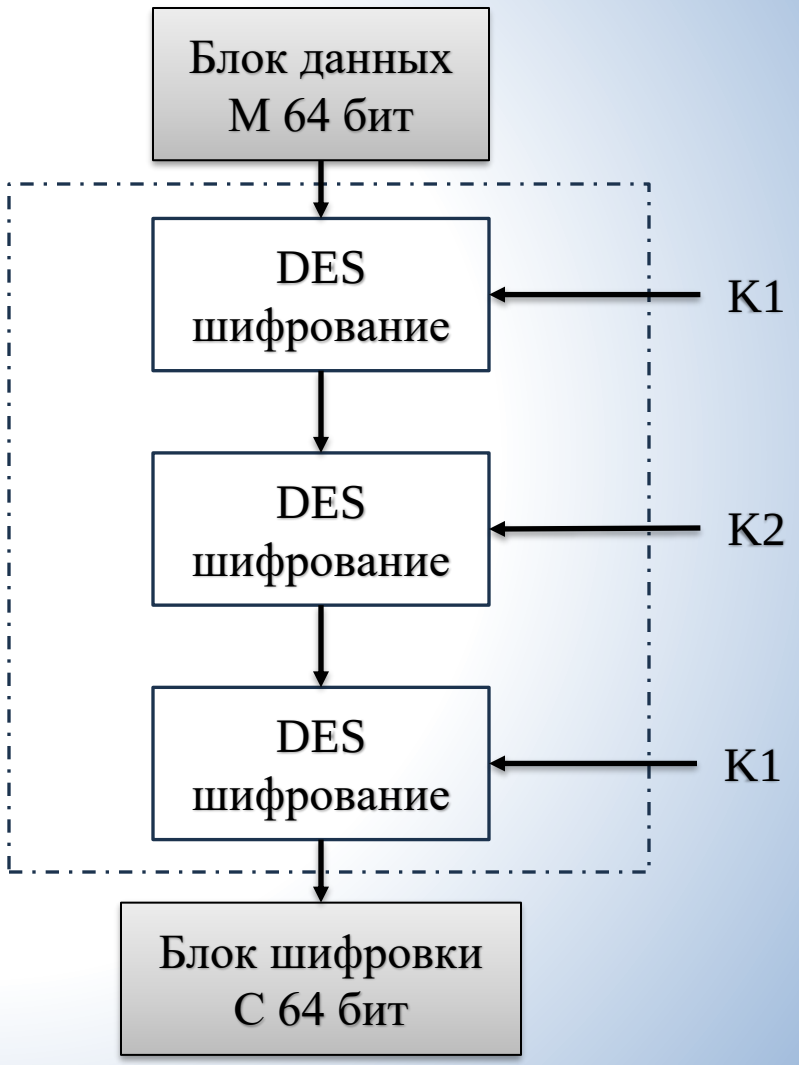


DES-EDE2

3-DES: Схема алгоритма шифрования DES-EEE3, DES-EEE2

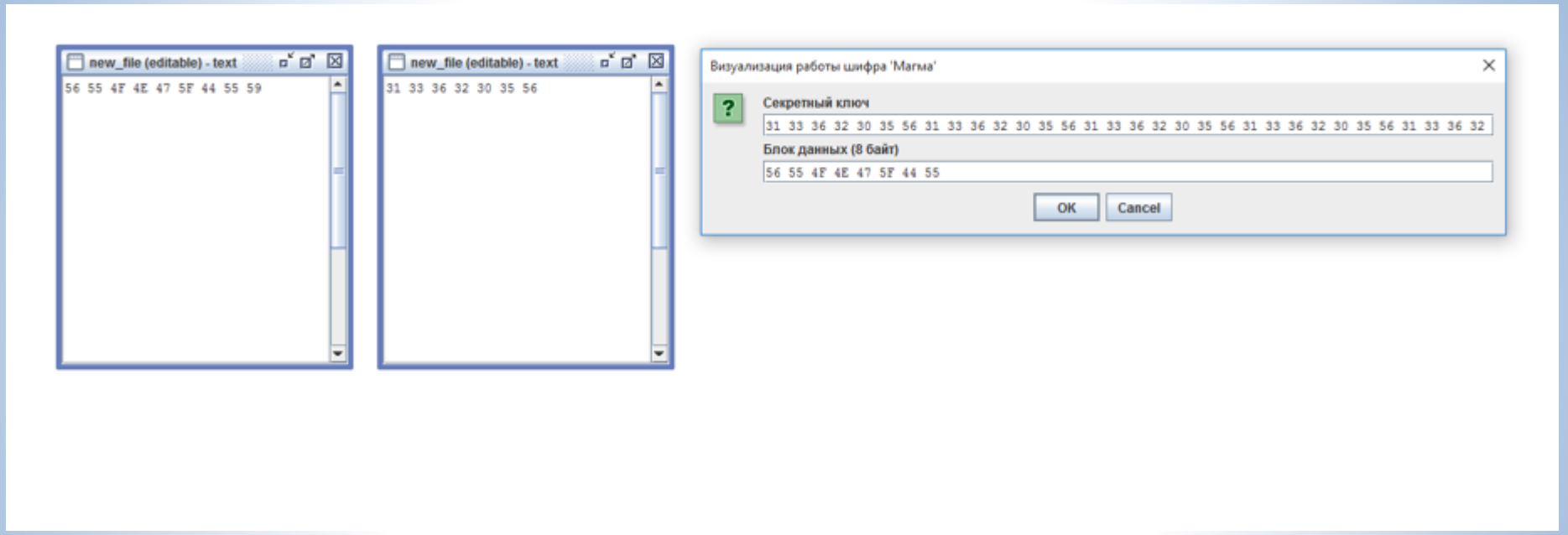


DES-EEE3



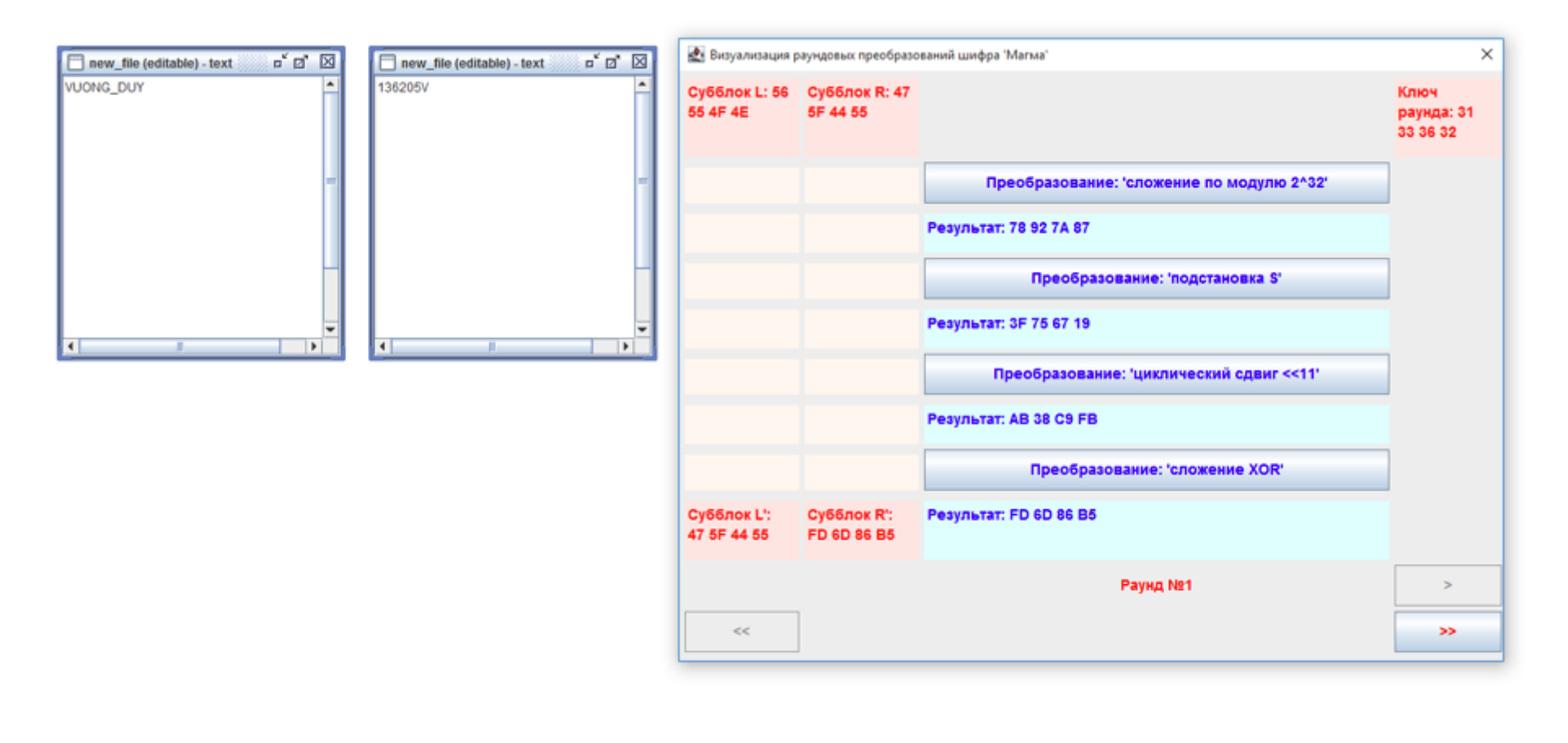
DES-EEE2

ГОСТ 28147-89 Магма: Расчет первого раунда шифрования



Исходные данные

ГОСТ 28147-89 Магма: Расчет первого раунда шифрования



Результат первого раунда шифрования

ГОСТ 28147-89 Магма: Ручной расчет первого раунда шифрования

Исходный текст								
V	U	O	N	G	_	D	U	Y
56	55	4F	4E	47	5F	44	55	59

Ключ (128 битов)															
1	3	6	2	0	5	V	1	3	6	2	0	5	V	1	3
31	33	36	32	30	35	56	31	33	36	32	30	35	56	31	33

00110001001100110011011000110010

Left

Right

56	55	4F	4E	47	5F	44	55

01000111010111110100010001010101

ГОСТ 28147-89 Магма: Ручной расчет первого раунда шифрования

Right 01000111010111110100010001010101

Key 1 00110001001100110011011000110010

Mod 2^{32}

01111000100100100111101010000111

78 | 92 | 7A | 87

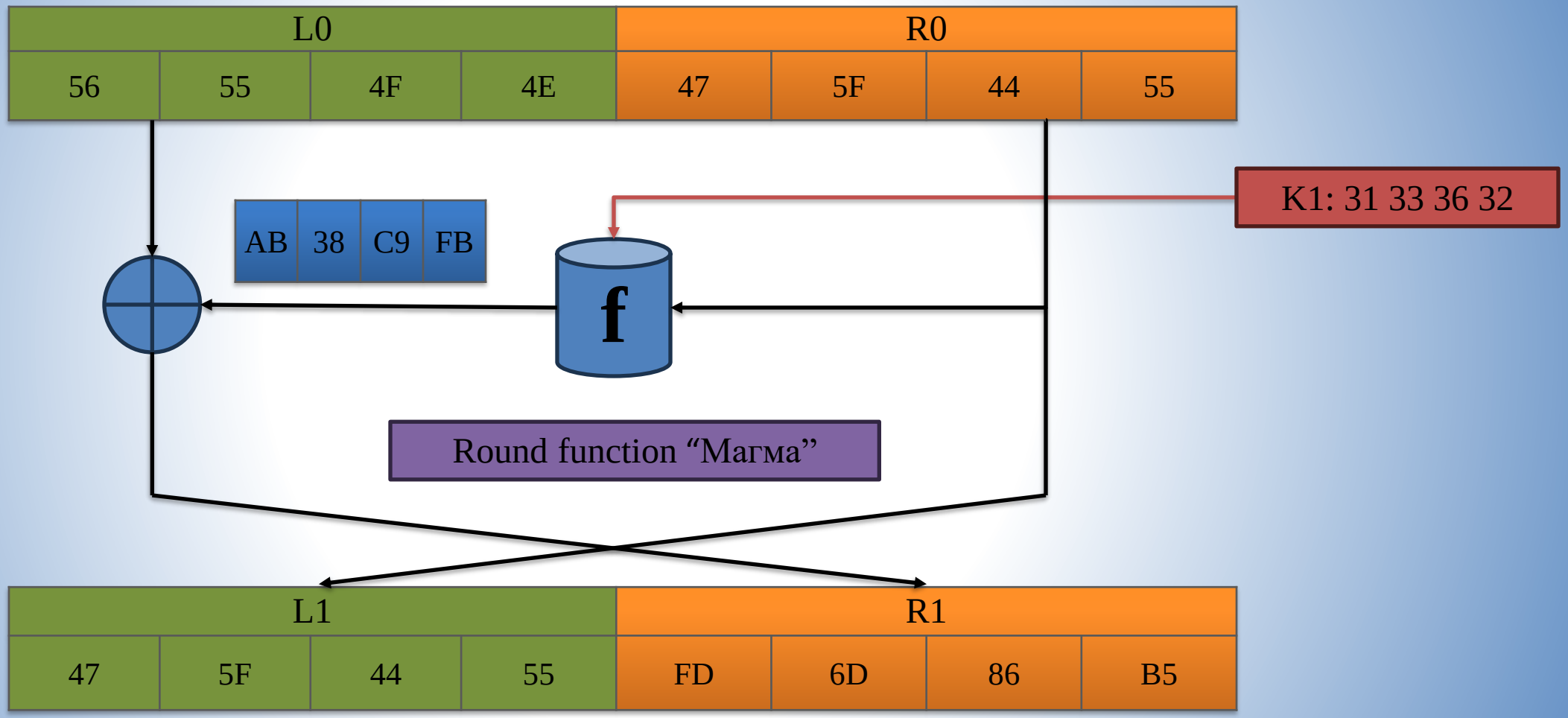
S - Box	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	12	4	6	2	10	5	11	9	14	8	13	7	0	3	15	1
2	6	8	2	3	9	10	5	12	1	14	4	7	11	13	0	15
3	11	3	5	8	2	15	10	13	14	1	7	4	12	9	6	0
4	12	8	2	1	13	4	15	6	7	0	10	5	3	14	9	11
5	7	15	5	10	8	1	6	13	0	9	3	14	11	4	2	12
6	5	13	15	6	9	2	12	10	11	7	8	1	4	3	14	0
7	8	14	2	5	6	9	1	12	15	4	11	0	13	10	3	7
8	1	7	14	13	0	5	8	3	4	15	10	6	9	12	11	2

3F | 75 | 67 | 19

<<11

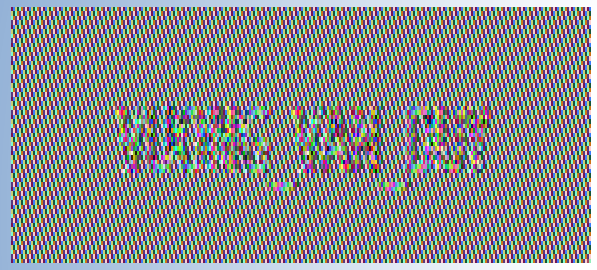
AB | 38 | C9 | FB

ГОСТ 28147-89 Магма: Ручной расчет первого раунда шифрования



ГОСТ 28147-89 Магма: Шифрование картинок

Результат шифровки режимом простой замены (ECB)



Исходная картинка

Результат шифровки режимом простой замены с зацеплением

Результаты сжатия

Картинка	Процент сжатия
Исходная	98%
ECB	11%
CBC	0%

Заключение

Были исследованы режимы **ECB** и **CBC** шифра **DES** и выявлены следующие основные характеристики:

- Симметричный блочный шифр
- Длина ключа – 64 бита (8 из которых – контрольные/проверочные)
- Размер блока – 64 бита
- В основе алгоритма лежит сеть Фейстеля с 16 раундами и рядом перестановок
- Было оценено время атаки грубой силой при известной части ключа для режимов ECB и CBC на примере текста длиной ~1100 символов, режим CBC показал лучшие результаты, что может быть связано с использованием различных значений для шифрования каждого блока

Было проведено исследование реализации шифра **3DES** в CrypTool2 путем построения моделей. В результате были выявлены два возможных режима работы модуля **TripleDES**:

- При длине ключа 16 байтов используется режим **DES-EDE2**, в котором применяется два различных ключа:первый ключ используется на первом и третьем этапе, а второй – на втором этапе.
- При длине ключа 24 байта используется режим **DES-EDE3**, в котором каждый из трех этапов использует отдельный ключ.
- В итоге, результаты работы встроенного модуля и созданных моделей полностью совпали.

Был исследован шифр **Магма ГОСТ 28147-89** и выявлены следующие основные характеристики данного шифра:

- симметричный блочный шифр
- длина ключа – 256 бит
- размер блока – 64 бита
- В основе алгоритма лежит сеть Фейстеля с 32 раундами, рядом перестановок и сдвигов

Кроме того, была проведена шифровка изображения в различных режимах работы алгоритма. Установлено, что при простом режиме замены, при использовании блоков с небольшим количеством ключей, сохраняются различимые очертания оригинального изображения. Однако в режиме замены с зацеплением, где результат текущего блока зависит от предыдущего, достигается большая энтропия. Это подтверждает, что попытка сжать зашифрованное изображение не приводит к значительным результатам.