

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

Лабораторная работа №5
ИЗУЧЕНИЕ ШИФРОВ AES и Кузнечик

Студент: _____ Выонг В.З, группа 1362

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

Санкт-Петербург 2025



Цель работы

Цель: Приобретение навыков работы с шифрами AES, «Кузнечик» ГОСТ 34.12-15

Задачи:

1. Изучить преобразования AES по шаблонной схеме AES Visualisation из CrypTool 2;
2. Провести исследование криптостойкости AES-128 в режиме CBC, используя CrypTool 2;
3. Изучить действия нарушителя при атаке предсказанием дополнения на шифр AES в режиме CBC;
4. Изучить алгоритм развертывания ключа шифра Кузнечик с помощью приложения ЛИТОРЕЯ;
5. Изучить раундовые преобразования шифра Кузнечик с помощью приложения ЛИТОРЕЯ.



Визуализация алгоритма зашифрования AES-256 в инфографике

Открытый текст (hex): 32 43 F6 A8 88 5A 30 8D 31 31 98 A2 E0 37 07 34

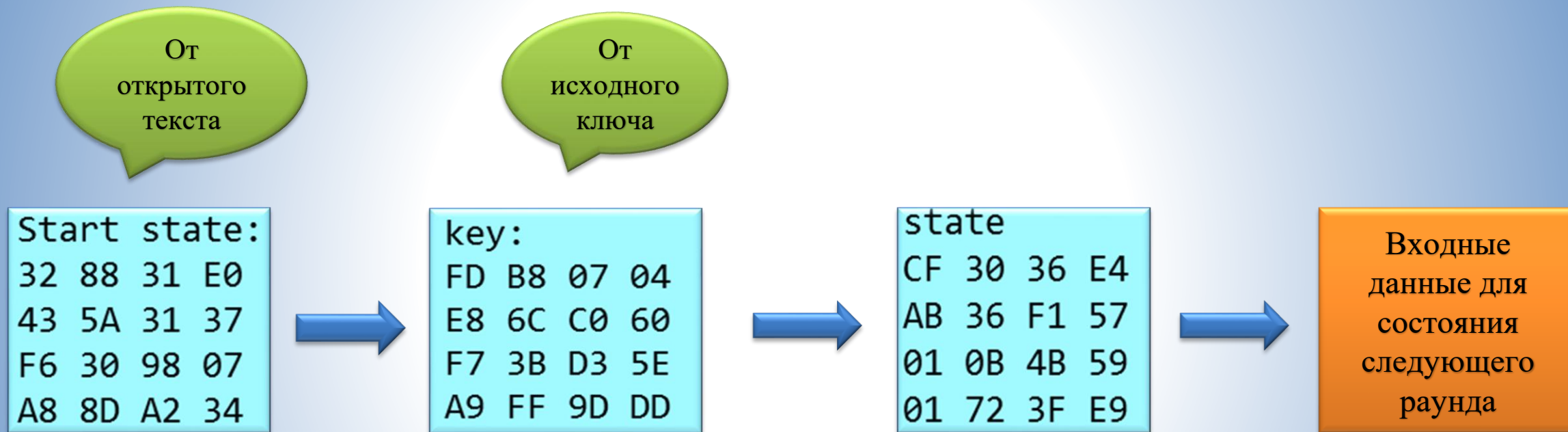
Ключ (hex): FD E8 F7 A9 B8 6C 3B FF 07 C0 D3 9D 04 60 5E DD 14 A3 D4 B6 33 45 4D 7C 5B 21 3A 5B 9A 0F 58 6C

	Key	State
0	FD E8 F7 A9 B8 6C 3B FF 07 C0 D3 9D 04 60 5E DD	CF AB 01 01 30 36 0B 72 36 F1 4B 3F E4 57 59 E9
1	14 A3 D4 B6 33 45 4D 7C 5B 21 3A 5B 9A 0F 58 6C	B9 F3 04 B9 74 22 E1 E2 80 56 5C F3 B0 AA 9A 74
2	8A 82 A7 11 32 EE 9C EE 35 2E 4F 73 31 4E 11 AE	50 A5 5B 0D 2B 80 2E E6 31 35 62 4A 06 AD 07 73
3	D3 8C 56 52 E0 C9 1B 2E BB E8 21 75 21 E7 79 19	1C 34 0D C5 AA 8C 8F C0 3D DB 88 8C 12 01 13 28
4	1C 34 73 EC 2E DA EF 02 1B F4 A0 71 2A BA B1 DF	63 03 44 9B 66 3E F1 7E BC F3 9B DC 9C B2 2A 3C
5	36 78 9E CC D6 B1 85 E2 6D 59 A4 97 4C BE DD 8E	E9 2B D9 B1 56 B8 56 77 16 8C CE E9 41 E8 B0 3A
6	B6 F5 6A C5 98 2F 85 C7 83 DB 25 B6 A9 61 94 69	35 35 8E 1B 62 AC C6 07 7B 1B 97 20 13 CD BD 8B
7	E5 97 BC 35 33 26 39 D7 5E 7F 9D 40 12 C1 40 CE	CF 86 F7 F7 43 E8 22 A2 1C D1 67 16 4A FB 1A 1E
8	C6 FC E1 0C 5E D3 64 CB DD 08 41 7D 74 69 D5 14	88 BD 77 73 E2 20 A7 A9 BD 08 4C D1 DB DE B3 2C
9	77 6E BF CF 44 48 86 18 1A 37 1B 58 08 F6 5B 96	7E D5 0D E4 DD 88 7E F3 EF A0 E3 83 8D 61 62 1C
10	94 C5 71 3C CA 16 15 F7 17 1E 54 8A 63 77 81 9E	B3 0A DB C4 AB 80 C0 37 42 6B C6 D2 C3 CE 0D 4A
11	8C 9B B3 C4 C8 D3 35 DC D2 E4 2E 84 DA 12 75 12	78 66 01 BD 46 31 B9 EA 2F 8F 55 ED 20 92 97 CC
12	7D 58 B8 6B B7 4E AD 9C A0 50 F9 16 C3 27 78 88	FB 25 FD 19 64 0B 01 7D A0 D8 C9 0F E0 59 AF 85
13	A2 57 0F 00 6A 84 3A DC B8 60 14 58 62 72 61 4A	8B E5 28 D2 E2 5A 8D B2 8E 0E 8D 19 F0 1F DD DD
14	7D B7 6E C1 CA F9 C3 5D 6A A9 3A 4B A9 8E 42 C3	40 09 33 00 52 52 02 E8 73 69 0E 7C 25 57 1F 17

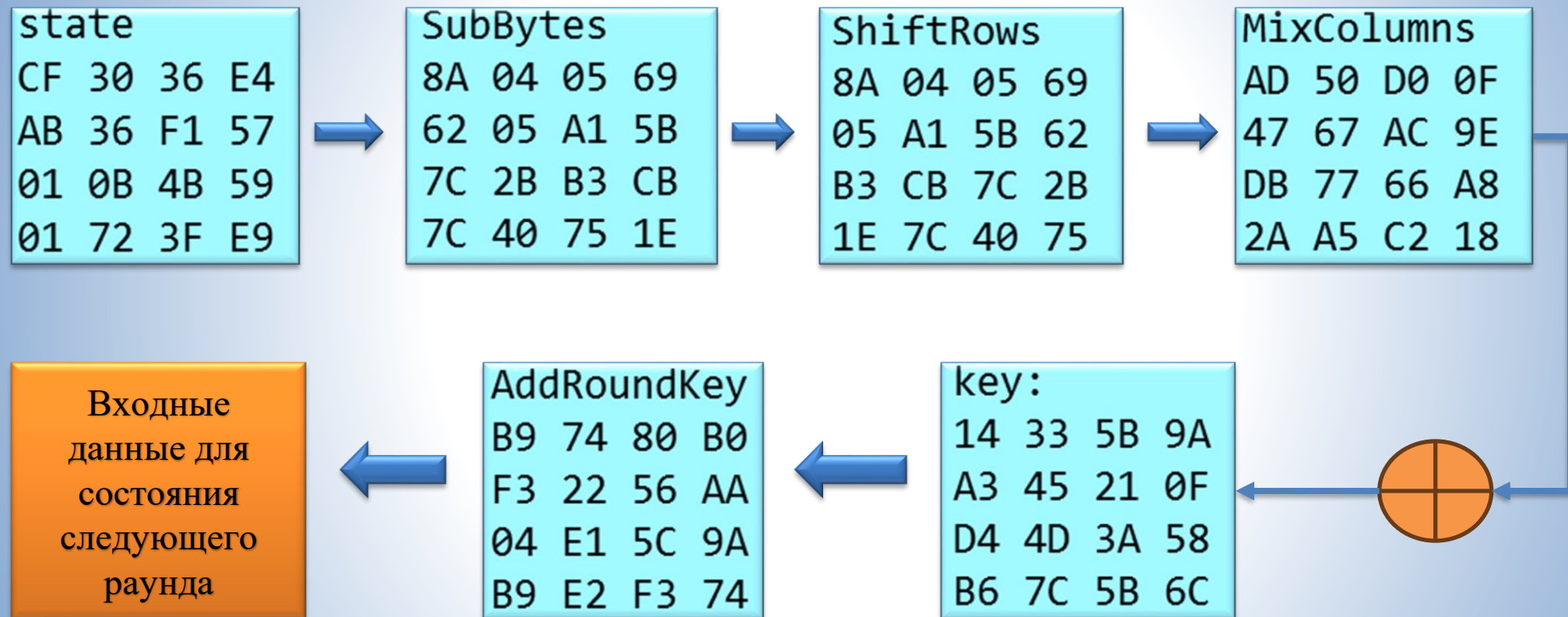
Шифровка (hex): 40 09 33 00 52 52 02 E8 73 69 0E 7C 25 57 1F 17



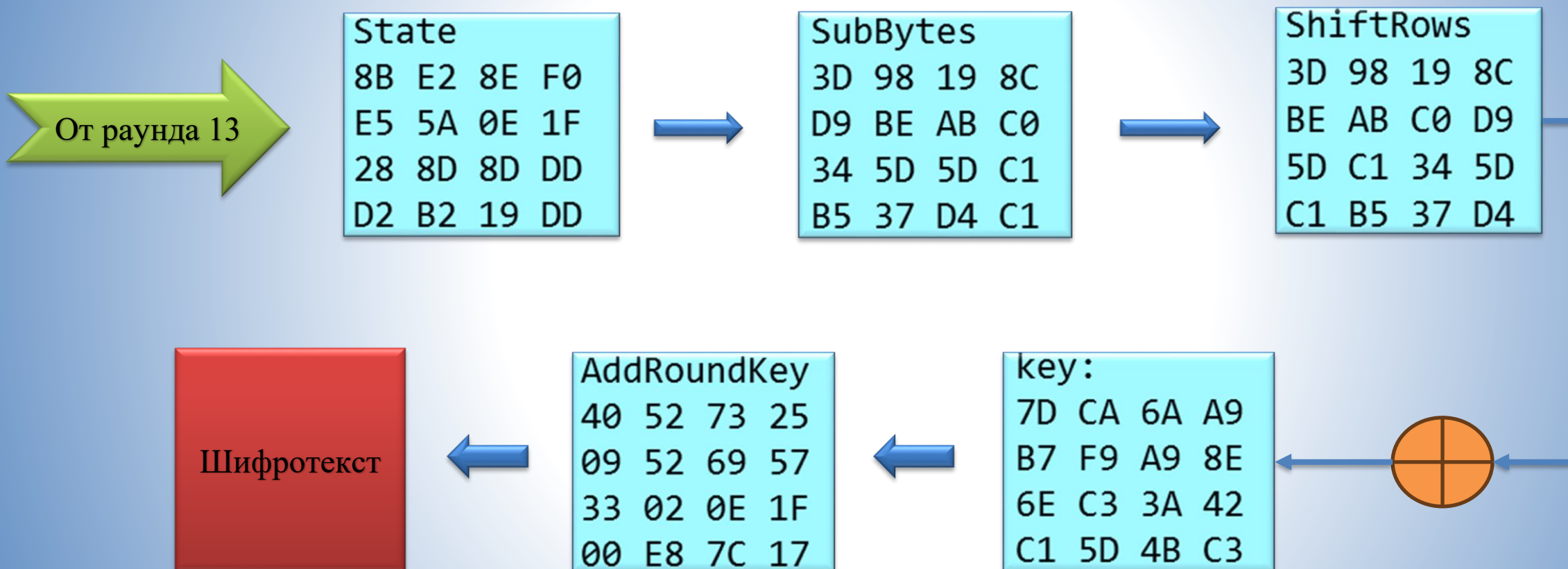
AES-256: Предварительный раунд



AES-256: Раунд AES (1-13)



AES-256: Заключительный раунд (раунд 14)



AES-256: Атаки "грубой силы"

Кол-во символов	Известные байты	Ожидаемое время
1116	14	1 с
	12	~2,5 ч
	10	~22,7 г

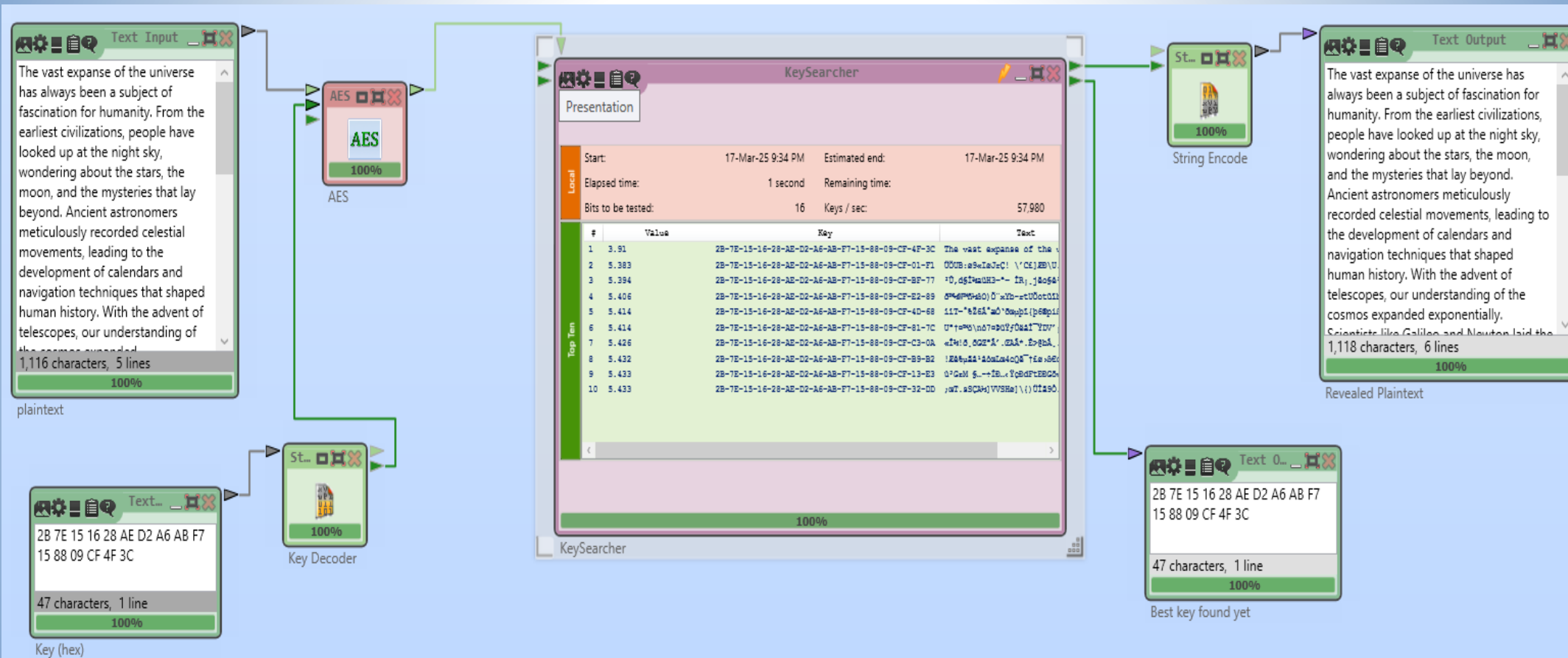
Таблица зависимости времени взлома от количества известных байт ключа



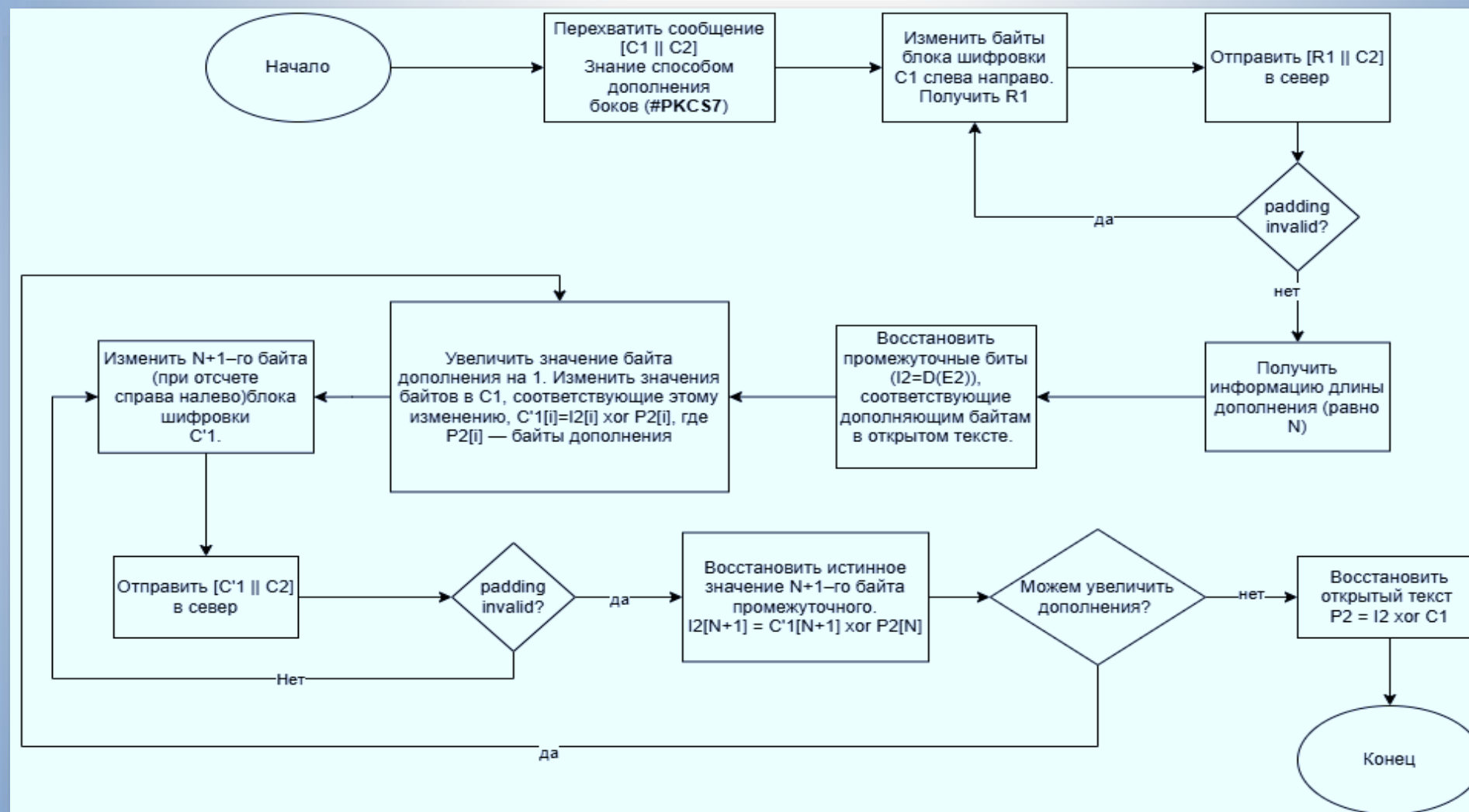
Столбчатая диаграмма зависимости времени взлома от количества процессорных ядер



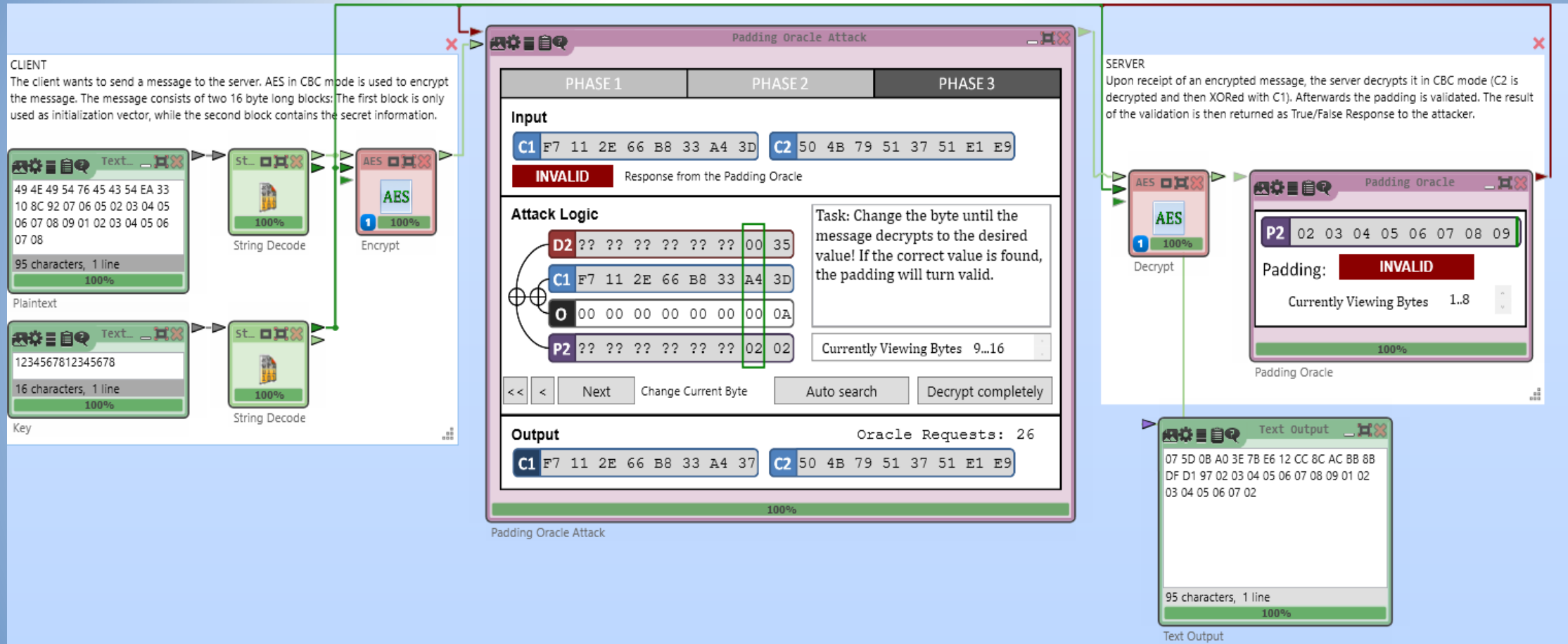
AES-256: Атаки "грубой силы"



AES: Инфографика действий нарушителя при атаке по дополнению



AES: Шаблон атаки по дополнению



Кузнечик ГОСТ 34.12-15: Развертывание ключа

Визуализация работы шифра 'Кузнечик' X

Секретный ключ

FD E8 F7 A9 B8 6C 3B FF 07 C0 D3 9D 04 60 5E DD 14 A3 D4 B6 33 45 4D 7C 5B 21 3A 5B 9A 0F 58 6C

OK Cancel

Секретный ключ:
FD E8 F7 A9 B8 6C 3B
FF 07 C0 D3 9D 04 60
5E DD 14 A3 D4 B6 33
45 4D 7C 5B 21 3A 5B
9A 0F 58 6C

Раундовый ключ 1
FD E8 F7 A9 B8 6C 3B
FF 07 C0 D3 9D 04 60
5E DD

Раундовый ключ 2
14 A3 D4 B6 33 45 4D
7C 5B 21 3A 5B 9A 0F
58 6C

Субблок L
AD 1E EA 2D E2 F0 CE
C8 35 C9 24 44 12 B0
B9 58

Субблок R
F6 87 AA 3C 2F 34 A9
F0 2F 1A 9D 5F BB E7
4C 6B

№ итерации развертывания ключа 7

Формирование ключа итерации:
C9 E8 81 9D C7 3B A5 AE 50 F5 B5 70 56 1A 6A 07

Преобразование: 'сложение XOR'
3F 6F 2B A1 E8 0F 0C 5E 7F EF
28 2F ED FD 26 6C

Преобразование: 'подстановка S'
1F B1 42 97 CB 4D 23 5D 57
52 81 4F E5 4B EF 9D

Преобразование: 'регистр сдвига L'
96 1F AE 89 5B 06 46 9C 4F
92 7B 0B 79 72 32 FE

Преобразование: 'сложение XOR'
F6 87 AA 3C 2F 34 A9 F0 2F
1A 9D 5F BB E7 4C 6B

<< >> >

Start left key:

AD 1E EA 2D E2 F0 CE C8 35 C9 24 44 12 B0 B9 58

Start Right key:

F6 87 AA 3C 2F 34 A9 F0 2F 1A 9D 5F BB E7 4C 6B

C_i:

C9 E8 81 9D C7 3B A5 AE 50 F5 B5 70 56 1A 6A 07

After xor C_i:

64 F6 6B B0 25 CB 6B 66 65 3C 91 34 44 AA D3 5F

After apply S_{Box}:

10 B4 6F AD 5C E4 6F 9A 7B 7F 0F E3 EA 38 49 87

After apply L:

3B 78 7A 12 4D 16 30 A9 59 C2 41 B4 AC 90 BD 47

Left key inter 7:

CD FF D0 2E 62 22 99 59 76 D8 DC EB 17 77 F1 2C


Right key inter 7:

AD 1E EA 2D E2 F0 CE C8 35 C9 24 44 12 B0 B9 58



Кузнечик ГОСТ 34.12-15: Раундовые преобразования

Визуализация работы шифра 'Кузнечик'

 Секретный ключ

FD E8 F7 A9 B8 6C 3B FF 07 C0 D3 9D 04 60 5E DD 14 A3 D4 B6 33 45 4D 7C 5B 21 3A 5B 9A 0F 58 6C

Блок данных (16 байт)

54 68 65 20 71 75 69 63 6B 20 62 72 6F 77 6E 20

OK Cancel

Визуализация раундовых преобразований шифра 'Кузнечик'

Блок данных: 3D 20 B6 5F 3E 17 86 AA E9 B8 9F 37 E7 CA 81 3D

Раундовый ключ: 79 F1 C9 F2 FD 49 05 47 B8 F4 32 05 97 A6 F2 1B

Преобразование: 'сложение XOR'

Результат X: 44 D1 7F AD C3 5E 83 ED 51 4C AD 32 70 6C 73 26

Преобразование: 'подстановка S'

Результат S: EA 1B 57 9F 40 5D A9 E5 70 FD 9F 02 32 9D 3D EF

Преобразование: 'регистр сдвига L'

Результат L: D4 8E DE 32 C8 E6 7E 10 49 89 E1 49 29 D3 F9 46

Раунд №7

<< >>

state:

3D 20 B6 5F 3E 17 86 AA E9 B8 9F 37 E7 CA 81 3D

After xor key:

44 D1 7F AD C3 5E 83 ED 51 4C AD 32 70 6C 73 26

After apply S_Box:

EA 1B 57 9F 40 5D A9 E5 70 FD 9F 02 32 9D 3D EF

After apply L:

D4 8E DE 32 C8 E6 7E 10 49 89 E1 49 29 D3 F9 46



Заключение

Был проведен анализ шифра AES и выявлены его основные характеристики. AES представляет собой симметричный блочный шифр с переменной длиной ключа: 128, 192 или 256 бит. Размер блока и размер раундовых ключей фиксированы и составляют 128 бит. Количество раундов зависит от длины ключа: 10 раундов для 128-битного ключа, 12 для 192-битного и 14 для 256-битного. Алгоритм основан на сети SP и в последнем раунде процедура MixColumns не выполняется.

Был проведён анализ времени, необходимого для атаки грубой силой, в случае частично известного ключа на примере текста длиной около 1100 символов при различных вычислительных ресурсах. Если 6 байт ключа остаются неизвестными, время подбора составляет от 6,4 до 22,7 лет. Одновременно время для атаки грубой силой будет эффективнее, если использовать больше процессорных ядер.

Также была рассмотрена атака на режим CBC шифра AES, а также построена схема алгоритма, описывающая действия потенциального злоумышленника. Оказалось, что в режиме CBC шифр AES очень уязвим для атак (без необходимости знать ключ), если злоумышленник обладает информацией о способе дополнения блока данных, а также имеет возможность перехватывать, модифицировать и пересылать зашифрованные данные получателю, а затем получать по побочным каналам реакцию получателя (сервера) на корректность дополнения.

Был проведён анализ шифра ГОСТ Р 34.12-2015 «Кузнечик», в результате чего выявлены его ключевые характеристики. Данный шифр представляет собой симметричный блочный алгоритм с длиной ключа 256 бит и размером блока 128 бит. В его основе лежит SP-сеть, состоящая из 10 раундов, где в последнем раунде выполняется только сложение с раундовым ключом. Также применяется сеть Фейстеля с 32 раундами для процесса развертывания ключа.

В процессе исследования и реализации алгоритма генерации раундовых ключей я обнаружил ошибку в программе Литорея. Похоже, что автор допустил неточность при реализации линейного преобразования L, а также ошибся в порядке передачи левых и правых блоков на следующий этап.

Также проведён расчёт результата раунда 7 шифрования, который подтвердил совпадение данных ручных и автоматизированных вычислений.



Ссылка на репозиторий проекта

Ссылка на репозиторий проекта (включая код, результаты, схемы и все, что связано с лабораторной работой): <https://github.com/VuongVanDuy/CRYPTOGRAPHY-LAB-5.git>