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

Лабораторная работа № 5

Изучение шифров AES и Кузнечик

Студентка: Усачева Дарья, группа 1384

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

Санкт-Петербург, 2024

Цель работы и задачи

Цель: Повысить свою компетенцию в области симметричных блочных шифров и в криптографии в целом.

Задачи:

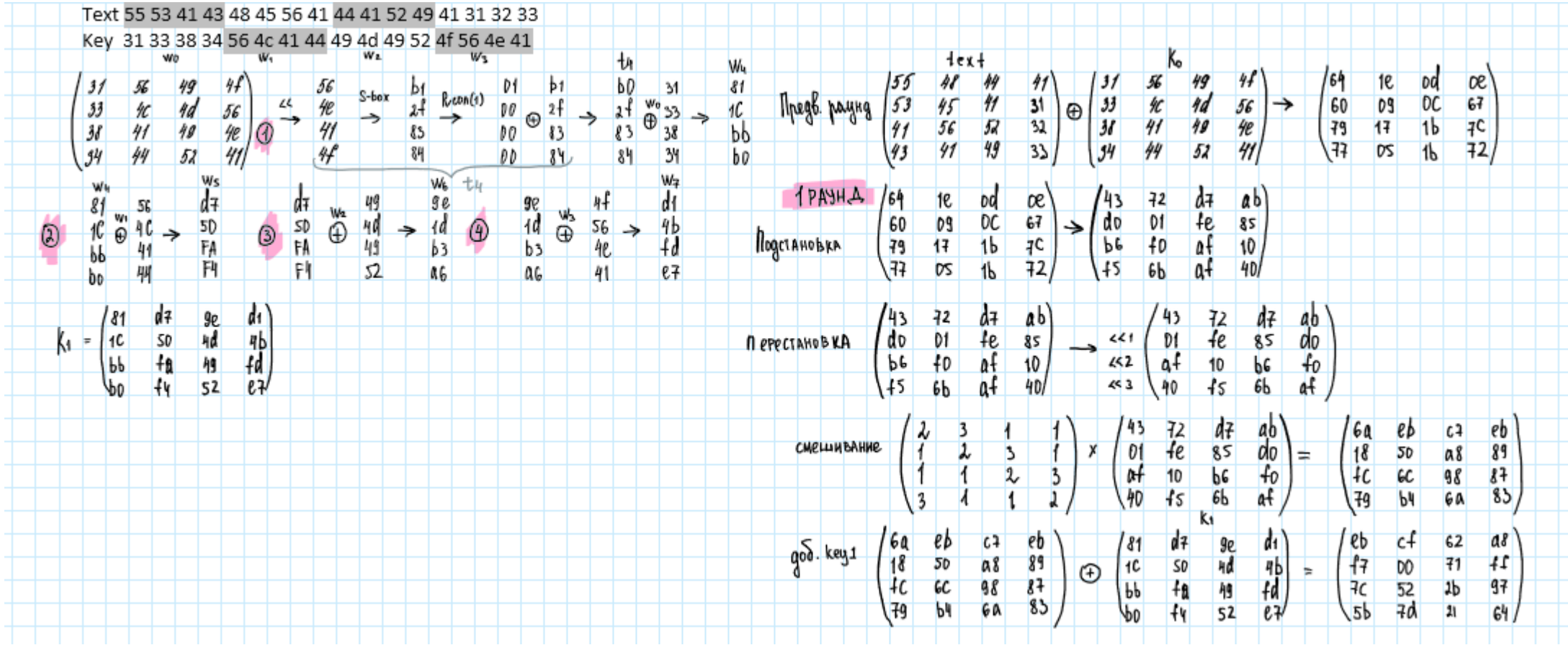
1. Изучить преобразования AES.
2. Провести исследование криптостойкости AES.
3. Изучить действия нарушителя при атаке предсказанием дополнения на шифр AES в режиме CBC.
4. Изучить алгоритм развертывания ключа шифра Кузнечик.
5. Изучить раундовые преобразования шифра Кузнечик.

Изучение преобразований AES

Ручной расчет

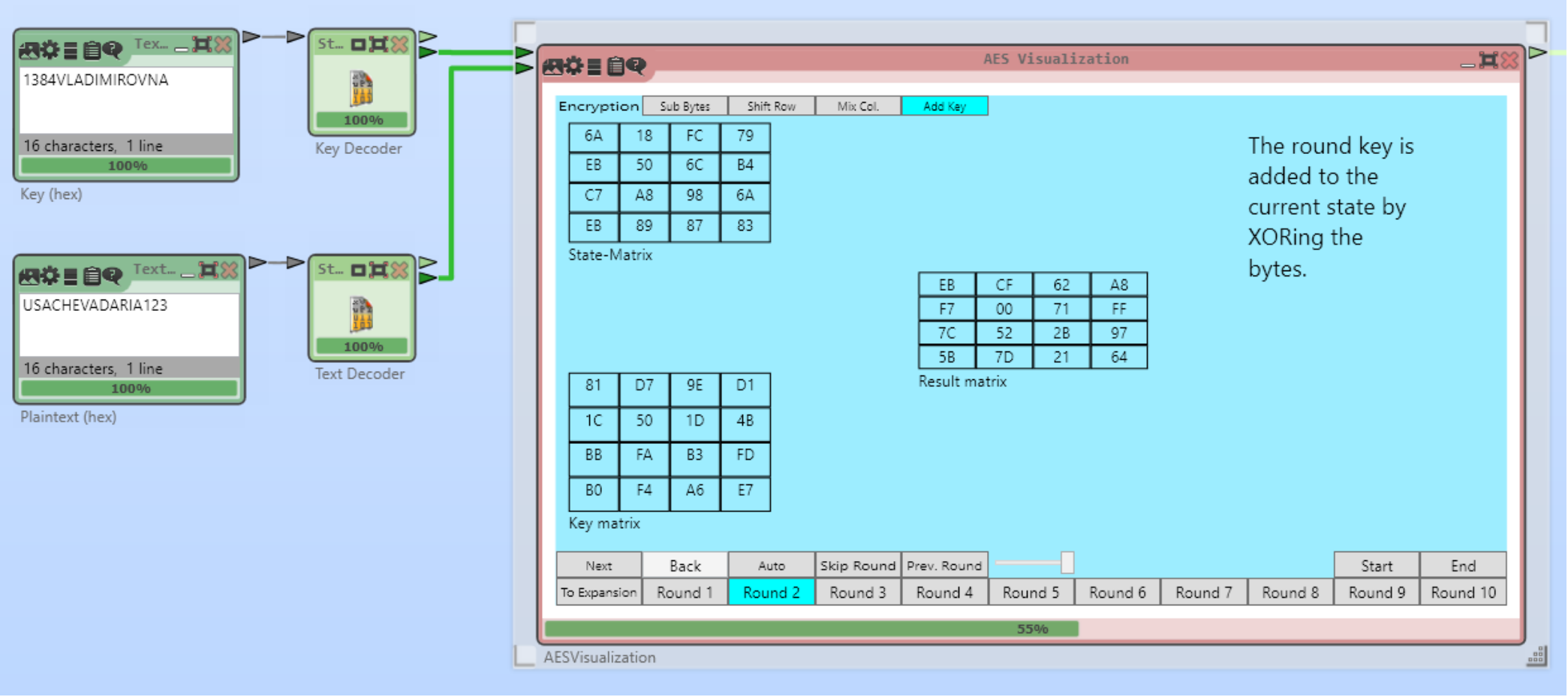
Открытый текст: USACHEVADARIA123

Ключ: 1384VLADIMIROVNA



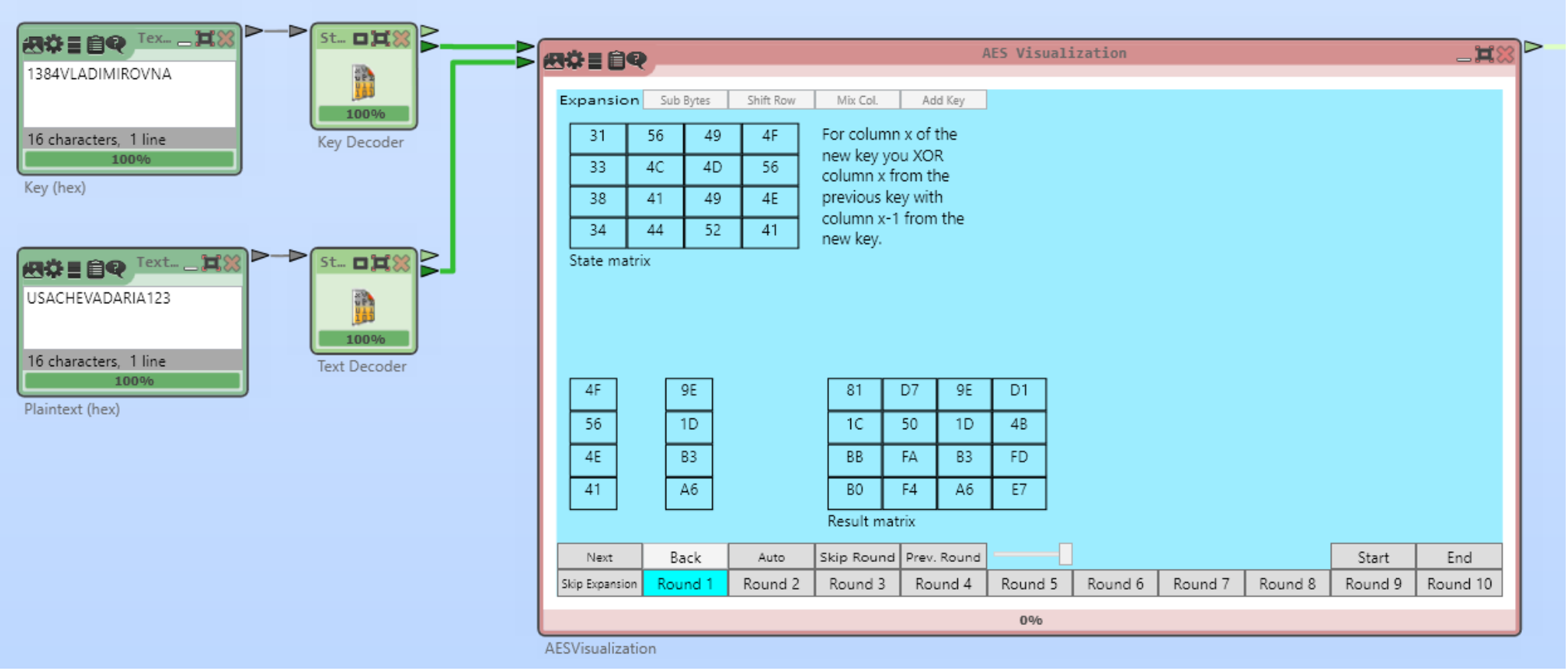
Результат раунда 1

Результат раунда 1 совпадает с результатом раунда 1 ручного расчета.



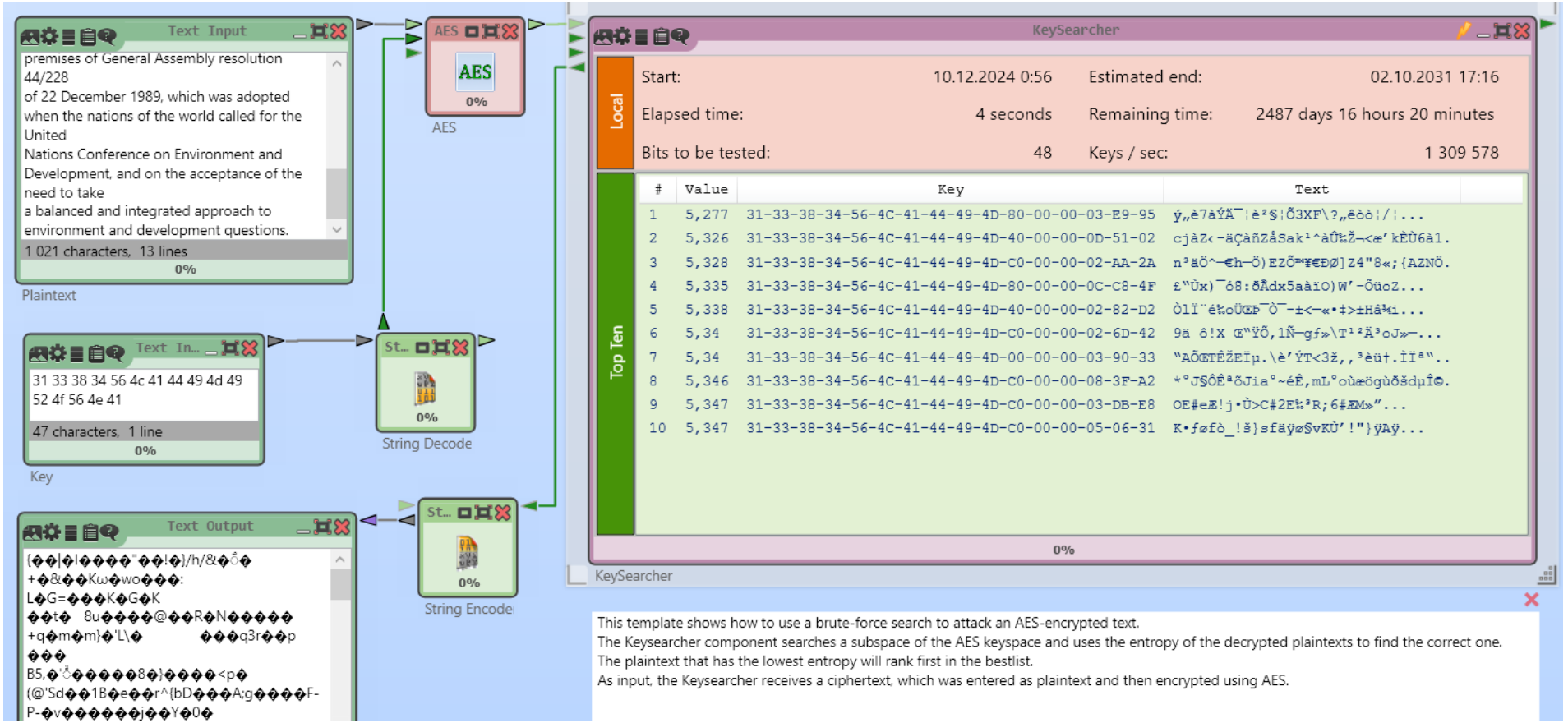
Ключ раунда 1

Ключ раунда 1 совпадает с результатом ручного расчета ключа 1.



Исследование криптостойкости AES

Шаблон атаки «грубой силы» CrypTool 2



Оценка времени атаки грубой силы

Результаты трудоемкости энтропийной атаки «грубой силы» для различных вариантов знаний о ключе и количестве задействованных процессорных ядер.

Кол-во известных байт	**Ожидаемые временные затраты**		
	1 ядро	2 ядра	4 ядра
n – 2	1 с	1 с	1 с
n – 4	2 ч 46 мин	1 час 39 мин	47 мин
n – 6	16.9 лет	9.5 лет	5.6 лет

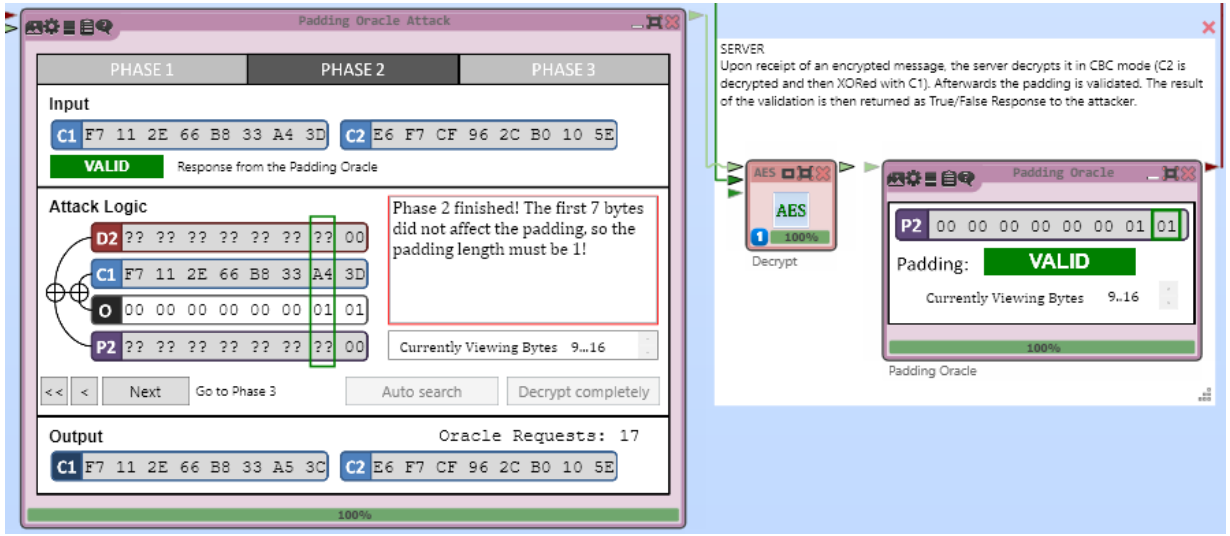
Оценка времени атаки грубой силы

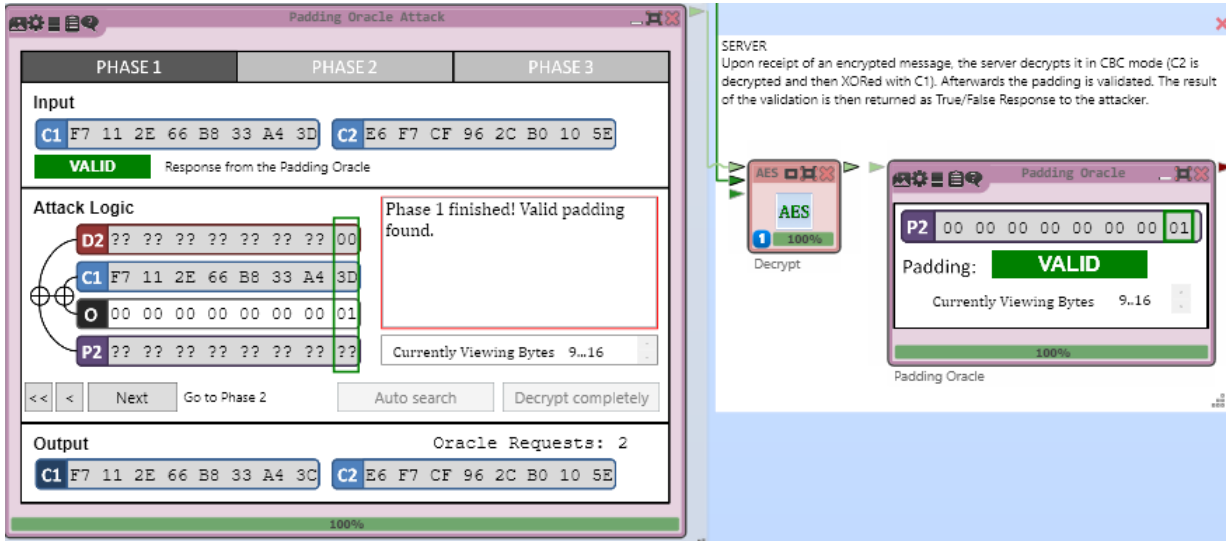
Результаты трудоемкости текстовой атаки «грубой силы» для различных вариантов знаний о ключе и количестве задействованных процессорных ядер.
Открытый текст DEARSIRSDIDYOUKNOWTHATILOVECATSTHANKS, оценочная функция DEARSIRS.
Как можно заметить, затрачиваемое время уменьшилось.

Кол-во известных байт	**Ожидаемые временные затраты**		
	1 ядро	2 ядра	4 ядра
n – 2	1 с	1 с	1 с
n – 4	1 ч 18 мин	45 мин	27 мин
n – 6	9.5 лет	5.2 лет	3.2 года

Изучение действий нарушителя при атаке предсказанием дополнения на шифр AES в режиме CBC.

Результаты 3 фаз атак





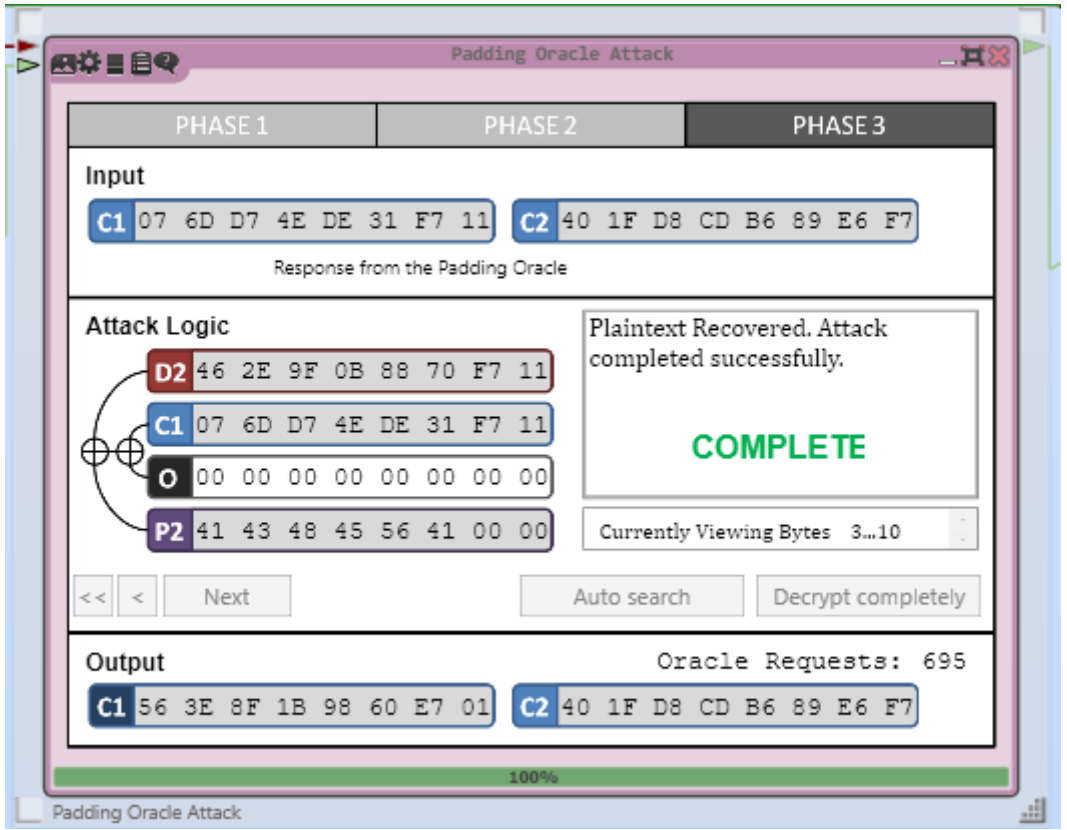


Схема алгоритма действия нарушителя

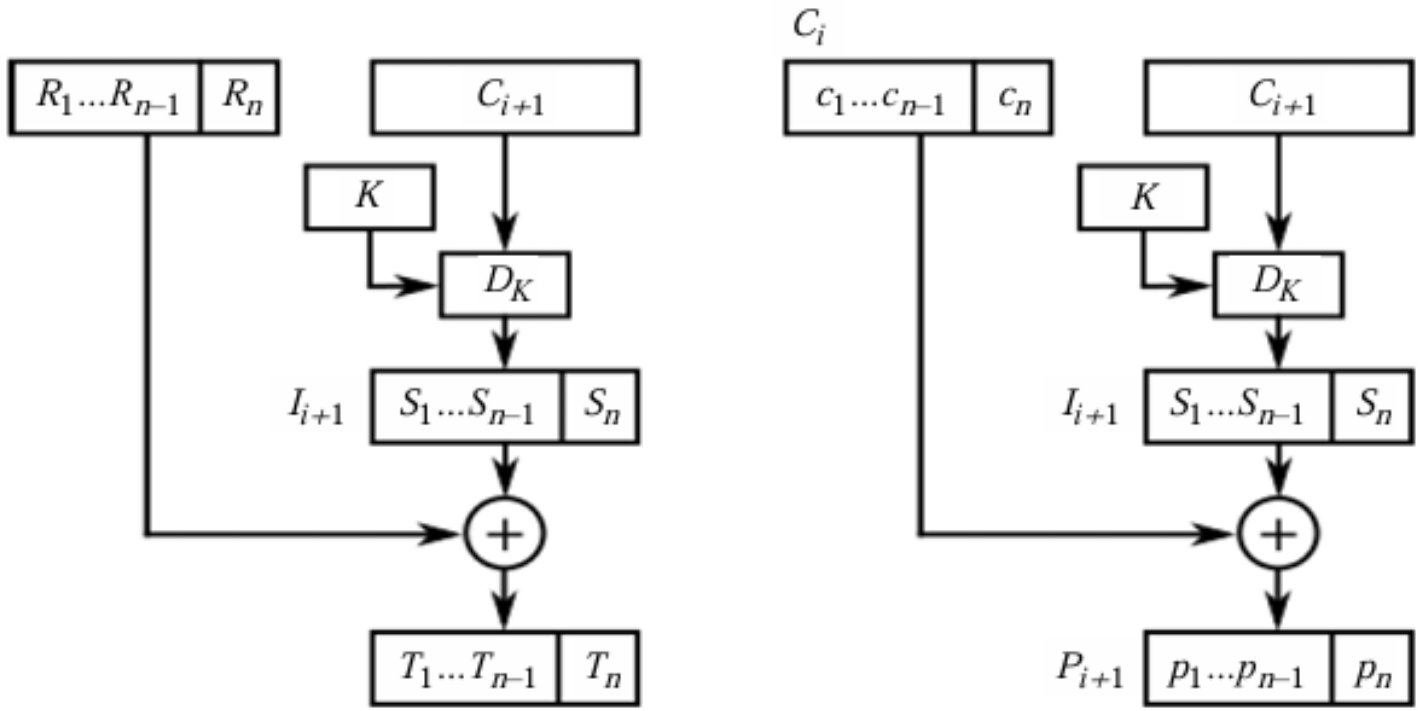


Рис. 5.3

Изучение алгоритма развертывания ключа шифра Кузнечик

Ручной расчет развертывания ключа

Ключ: 1384VLADIMIROVNA1384VLADIMIROVNA

Key 31 33 38 34 56 4c 41 44 49 4d 49 52 4f 56 4e 4131 33 38 34 56 4c 41 44 49 4d 49 52 4f 56 4e 41

Выбираем N(C)= 7+d = 9 C_9 = 09 be ef a9 01 cd cf 03 1a c1 d8 a6 44 0 fb 98

K_3 K_4

3c5ff1d7319ae77dc776221e3f7fd310	Bd1cef012b0cd271192fefe4e069fc14

1) X operation

K3 xor C9 = x

3c5ff1d7319ae77dc776221e3f7fd310
09be2efa901cdcf0312c4d8a6440fb98
35e1df2da1863b8df65a6f945b3f2888 X

2) S operation

S(x) = s

16cc	35	e1	df	2d	a1	86	3b	8d	f6	5a	6f	94	5b	3f	28	88
10cc	106	32	97	1	167	67	152	34	180	19	177	122	71	31	129	215
16cc	6a	20	61	1	a7	43	98	22	b4	13	b1	7a	47	1f	81	d7 S

3) L operation

L(s) = l

Так как L преобразование состоит из 16 итераций, выполним его с помощью программы из статьи на habr

result after L operation in iteration 9: dd8bbd500facf0104c1c67628922457a

4) L xor K4

6097525124a0226155338886694bb96e

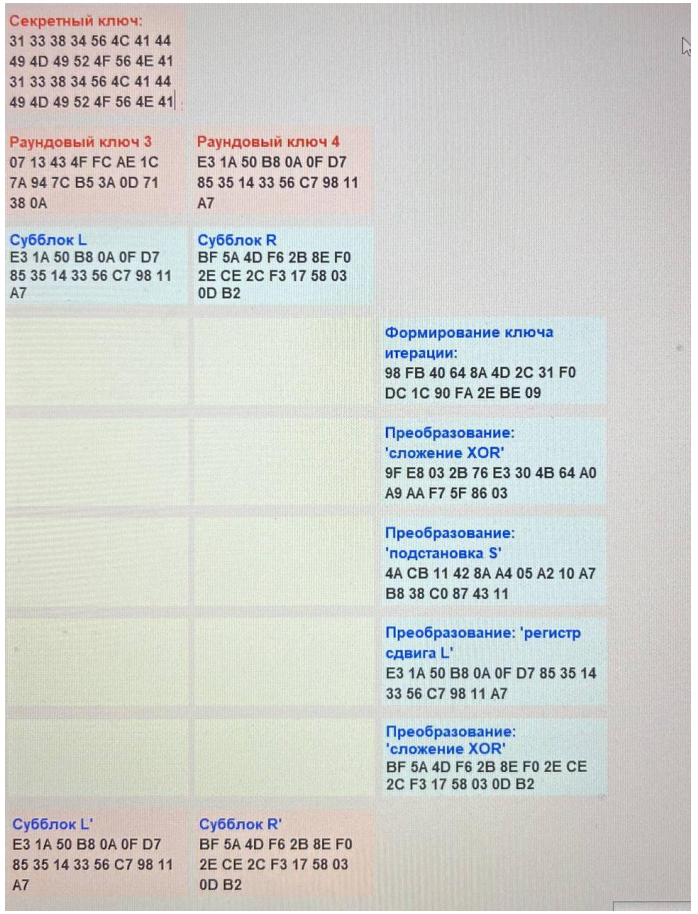
6097525124a0226155338886694bb96e	3c5ff1d7319ae77dc776221e3f7fd310

Результат развертывания ключа шифра

Результат выполнения итерации 9 не совпадает с результатом ручного расчета.

Проанализировав выводы работы приложения ЛИТОРЕЯ, заметим, что C9 задана неверно, она должна иметь вид: 09be2efa901cdcf0312c4d8a6440fb98.

В результате 16 сдвигов байт 09 должен вернуться на первую позицию. Однако в ЛИТОРЕЕ этого не произошло, что позволяет сделать вывод о неправильности реализации линейного преобразования.



Изучение раундовых преобразований шифра Кузнечик

Ручной расчет раунда 9

Открытый текст: USACHEVADARIA123

Ключ: 1384VLADIMIROVNA1384VLADIMIROVNA

K9= 3c3709b2988faccb5c2b39763660373a

Блок данных: V8=24c14f609b25b7724863ee01bbabe684

1) X operation

K9 xor V8 = x

3c3709b2988faccb5c2b39763660373a
24c14f609b25b7724863ee01bbabe684
18f646d203aa1bb91448d7778dcbd1be

2) S operation

S(x) = s

16cc	18	f6	46	d2	3	aa	1b	b9	14	48	d7	77	8d	cb	d1	be
10cc	23	180	72	131	17	56	187	163	147	242	254	126	34	228	27	149
16cc	17	b4	48	83	11	38	bb	a3	93	f2	fe	7e	22	e4	1b	95

3) L operation

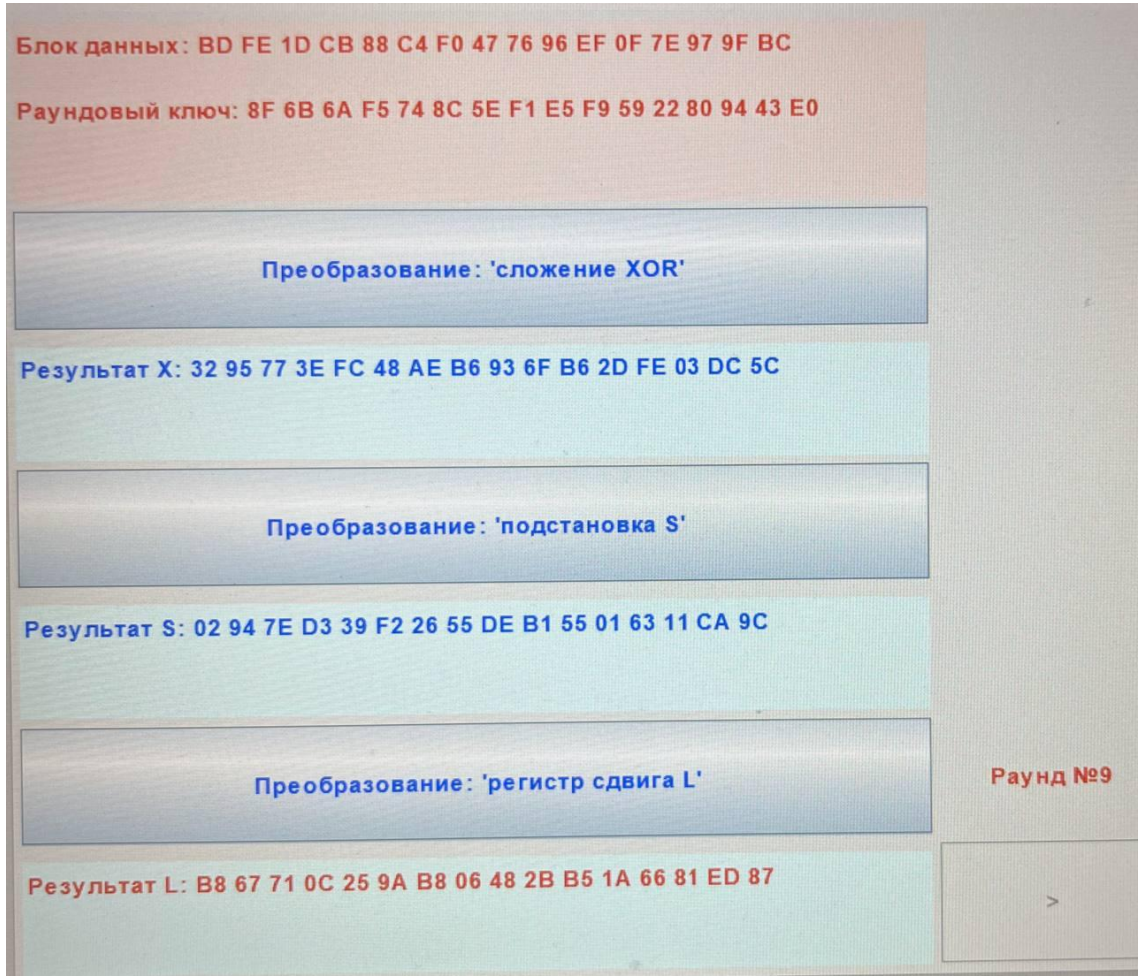
L(s) = l

Так как L преобразование состоит из 16 итераций, выполним его с помощью программы из статьи на habr

result after L operation l = 17b448831138bba393f2fe7e22e41b95

Результат раунда 9

Результат выполнения раунда 9 не совпадает с результатом ручного расчета. Объяснение этому представлено на слайде номер 16.



Заключение

1. Изучены преобразования AES по шаблонной схеме AES Visualisation.

Алгоритм выполняет 10,12,14 (для ключей длины 128, 192, 256 бит соответственно) раундов шифрования с выполнением различных обратимых преобразований (SubBytes, ShiftRows, MixColums, AddRoundKey). Выяснено, что раундовый ключ генерируется последовательно (слово за словом) при помощи преобразований RotWord, SubWord и раундовой константы Rcon(i).

2. Проведено исследование криптостойкости AES.

Были сделаны следующие выводы:

- Увеличение известной части секретного ключа ускоряет атаку, а рост числа процессорных ядер значительно сокращает её время.
- Использование специфических оценочных функций (например, “DEAR SIRS”) повышает эффективность атак по сравнению с применением энтропийных методов.

3. Изучены действия нарушителя при атаке предсказанием дополнения на шифр AES в режиме CBC.

В режиме CBC была исследована атака Padding Oracle Attack, включающая три фазы: поиск допустимого заполнения, определение его длины и побайтовое расшифрование.

4. Изучен алгоритм развертывания ключа шифра Кузнечик.

Выяснено, что каждая последующая пара раундовых ключей генерируется с использованием восьми итераций сети Фейстеля, где на каждой итерации генерируется константа и выполняются L,S,X преобразования.

5. Изучены раундовые преобразования шифра Кузнечик.

Алгоритм выполняет девять полных раундов с последовательными X, L, S преобразованиями. Заключительный десятый раунд включает в себя только X преобразование.