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

Лабораторная работа № 5

Изучение шифров AES, Кузнечик

Студент: _____ Чернякова Валерия, группа 1304

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

Санкт-Петербург 2024

Цель работы

Повысить компетенции в работе с методами симметричного шифрования: AES и Кузнечик. Исследовать на практике режимы работы данных шифров.

Задачи:

- Изучить преобразования AES
- Исследовать криптостойкость AES
- Изучить действия нарушителя при атаке с предсказанием дополнения AES CBC
- Изучить алгоритм развертывания ключа шифра Кузнечик
- Изучить раундовые преобразования шифра Кузнечик

Шифр «AES»

Задание

1. Изучить преобразования шифра AES с помощью демонстрационного приложения.
2. Выполнить вручную преобразования для одного раунда и вычисление раундового ключа при следующих исходных данных: а) открытый текст – свои фамилия_имя (транслитерация латиницей); б) ключ – номер группы_отчество.
3. Проверить полученные результаты с помощью приложения инспектора
4. Найти и запустить шаблон атаки в CrypTool 2: AES Analysis using Entropy(2).
5. Выбрать открытый текст (примерно 1000 знаков) и загрузить его в шаблон.
6. Провести атаку «грубой силы», когда известно n – 2, n – 4, n – 6 байт секретного ключа, используя в качестве оценочной функции энтропию и за действовав 1 ядро процессора. Зафиксировать затраты времени.
7. Выполнить атаку повторно с средним и максимальным количеством процессорных ядер. Зафиксировать затраты времени.
8. Сформировать текст со произвольным сообщением в формате «DEAR SIRS message THANKS» и загрузить его в шаблон.
9. Провести атаку «грубой силы», когда известно n – 2, n – 4, n – 6 байт секретного ключа, используя в качестве оценочной функции словосочетание DEAR SIRS и задействуя 1 ядро процессора. Зафиксировать затраты времени.
10. Выполнить атаку повторно со средним и максимальным количествами процессорных ядер. Зафиксировать затраты времени.
11. Найти и запустить шаблон атаки в CrypTool 2: Padding Oracle Attack on AES.
12. Подготовиться к атаке теоретически, т. е. изучить: а) комментарии к шаблону; б) действия атакующего злоумышленника.
13. Внедрить во второй блок исходного текста коды символов своего имени.
14. Выполнить 3 фазы атаки и сохранить итоговые скриншоты по окончании каждой фазы.
15. Убедиться, что атака удалась.

Исходные данные

Открытый текст:

M = chernyak_valeria

Ключ (64 бит):

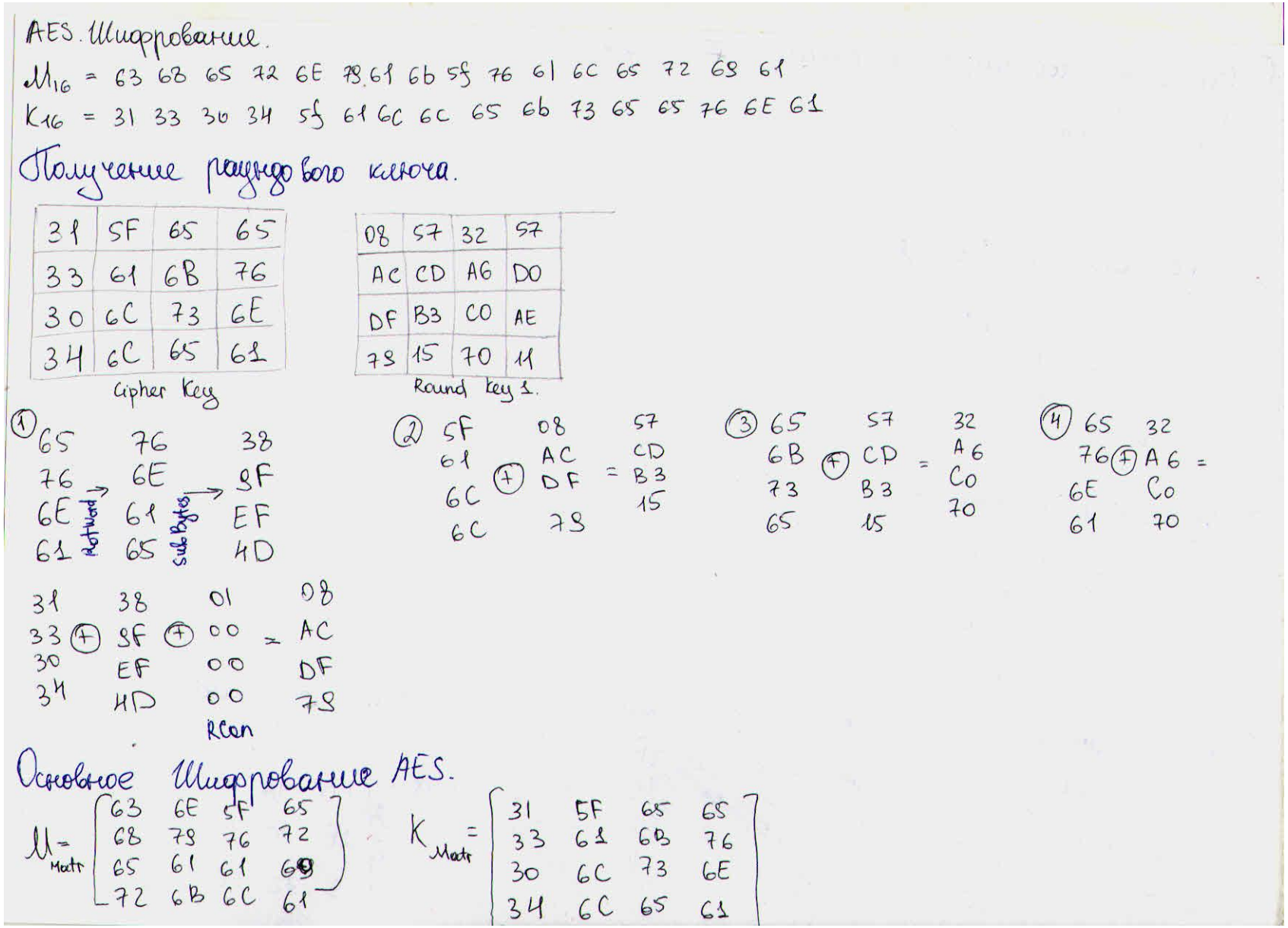
K = 1304_allekseevna

Байтовое представление:

M_{16} = 63 68 65 72 6e 79 61 6b 5f 76 61 6c 65 72 69 61

K_{16} = 31 33 30 34 5f 61 6c 6c 65 6b 73 65 65 76 6e 61

Ручные преобразования 1 раунда



AES. Шифрование.

M_{16} = 63 68 65 72 6E 79 61 6b 5f 76 61 6C 65 72 69 61

K_{16} = 31 33 30 34 5f 61 6C 6C 65 6b 73 65 65 76 6E 61

Получение раундового ключа.

31	5F	65	65
33	61	6B	76
30	6C	73	6E
34	6C	65	61

Cipher Key

08	57	32	57
AC	CD	AG	DO
DF	B3	CO	AE
79	15	70	11

Round key 1.

① 65 76 6E 61 → RotWord → 76 6E 61 65 → SubBytes → 38 9F EF 4D

② 5F 08 57 / 61 AC CD / 6C DF B3 / 6C 79 15 (⊕)

③ 65 57 32 / 6B CD A6 / 73 B3 C0 / 65 15 70 (⊕)

④ 65 32 / 76 A6 / 6E C0 / 61 70 (⊕) =

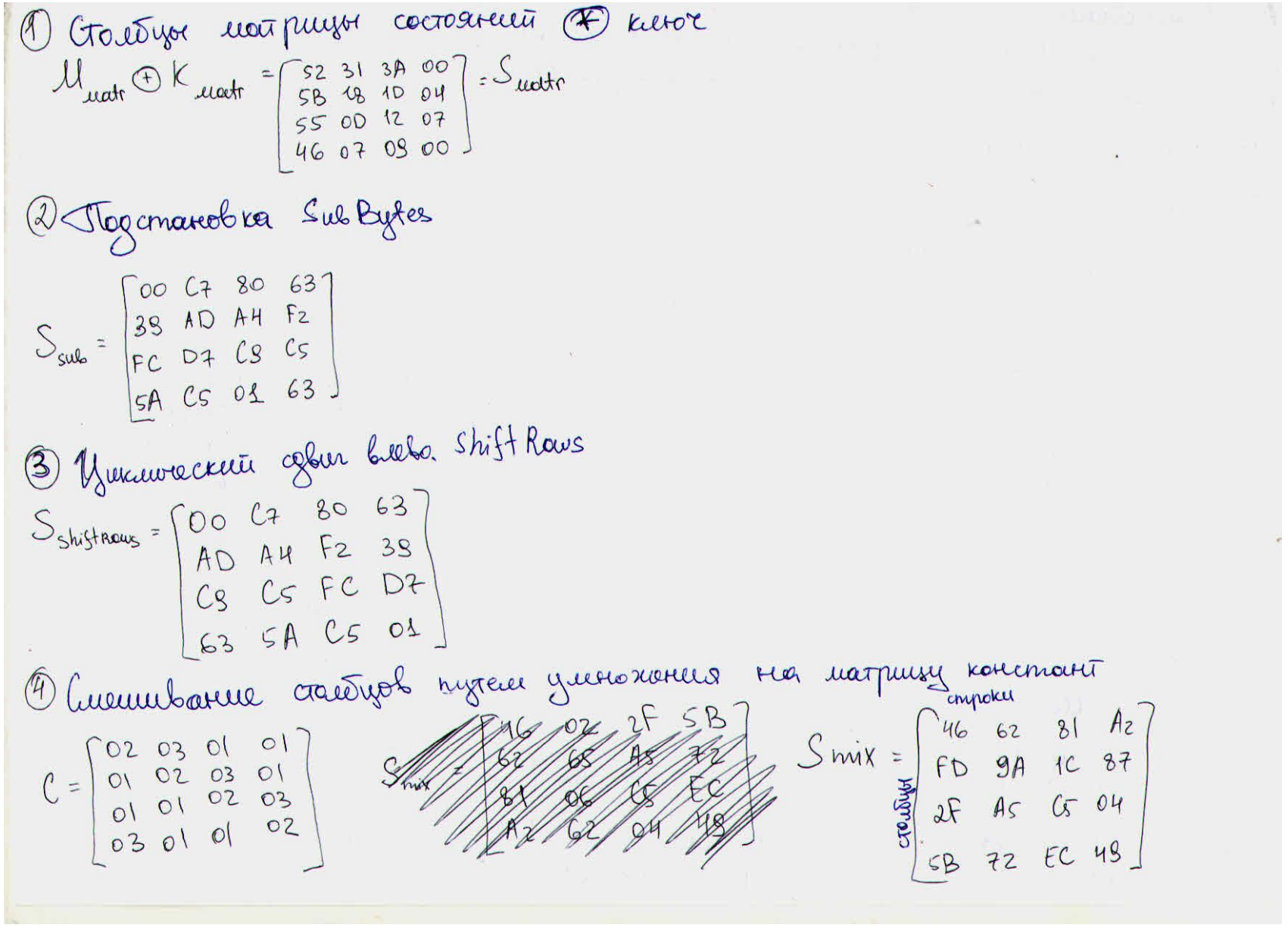
31 38 01 08 / 33 9F 00 AC / 30 EF 00 DF / 34 4D 00 79 (⊕ ⊕ = RCon)

Основное Шифрование AES.

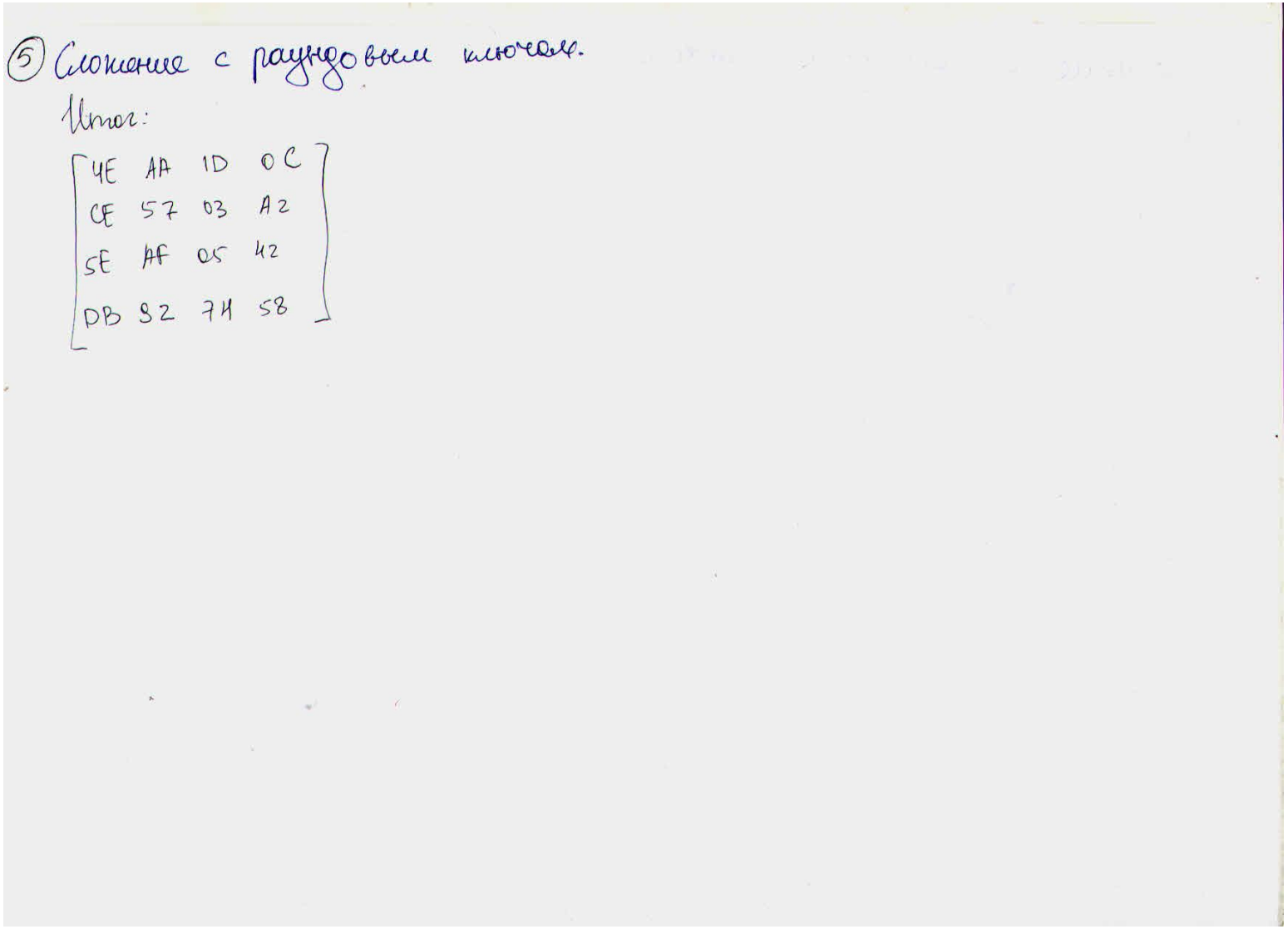
$M_{Matr} = \begin{bmatrix} 63 & 6E & 5F & 65 \\ 68 & 79 & 76 & 72 \\ 65 & 61 & 61 & 69 \\ 72 & 6B & 6C & 61 \end{bmatrix}$

$K_{Matr} = \begin{bmatrix} 31 & 5F & 65 & 65 \\ 33 & 61 & 6B & 76 \\ 30 & 6C & 73 & 6E \\ 34 & 6C & 65 & 61 \end{bmatrix}$

Ручные преобразования 1 раунда. Продолжение



Ручные преобразования 1 раунда. Конец

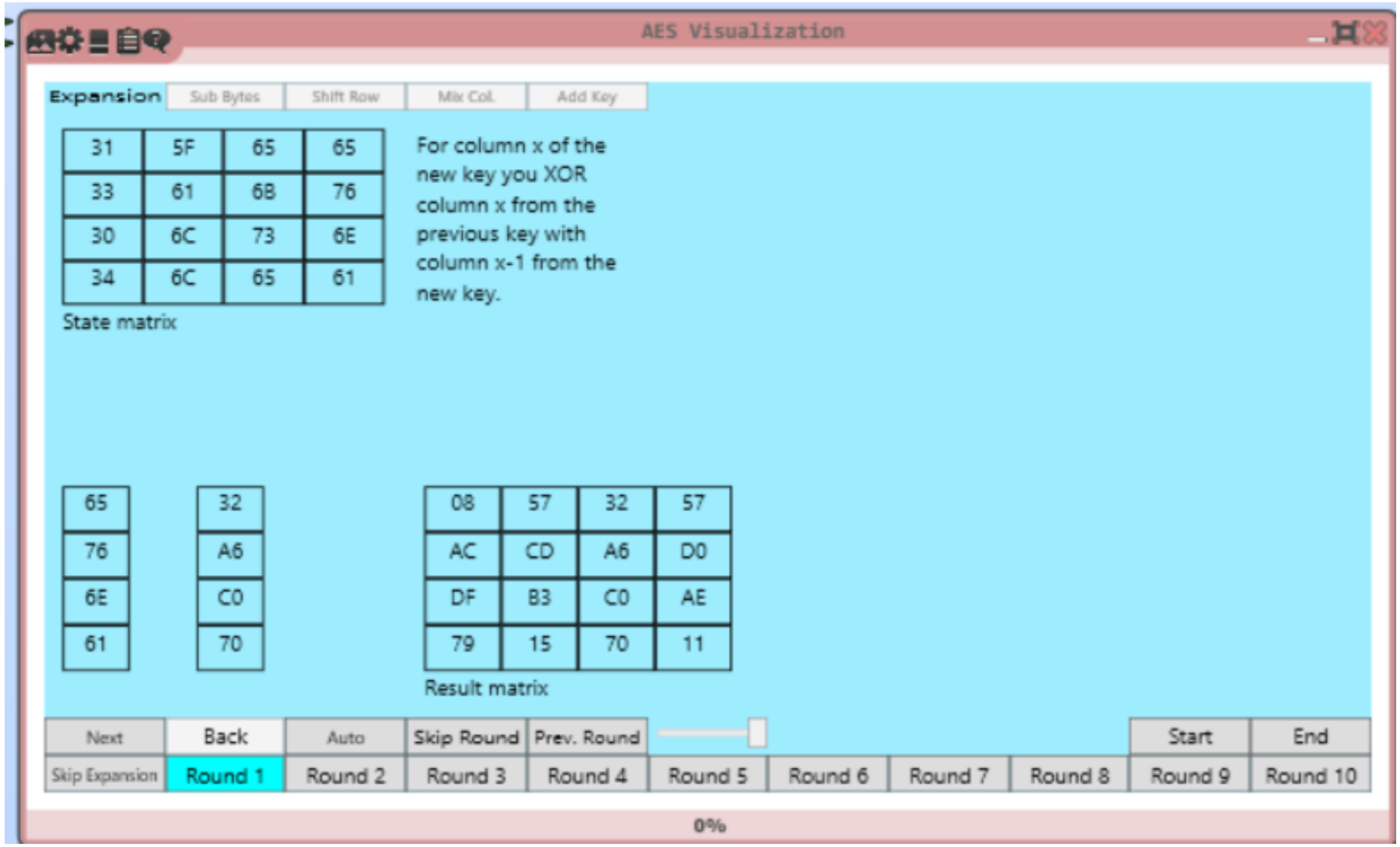


⑤ Сложение с раундовым ключом.

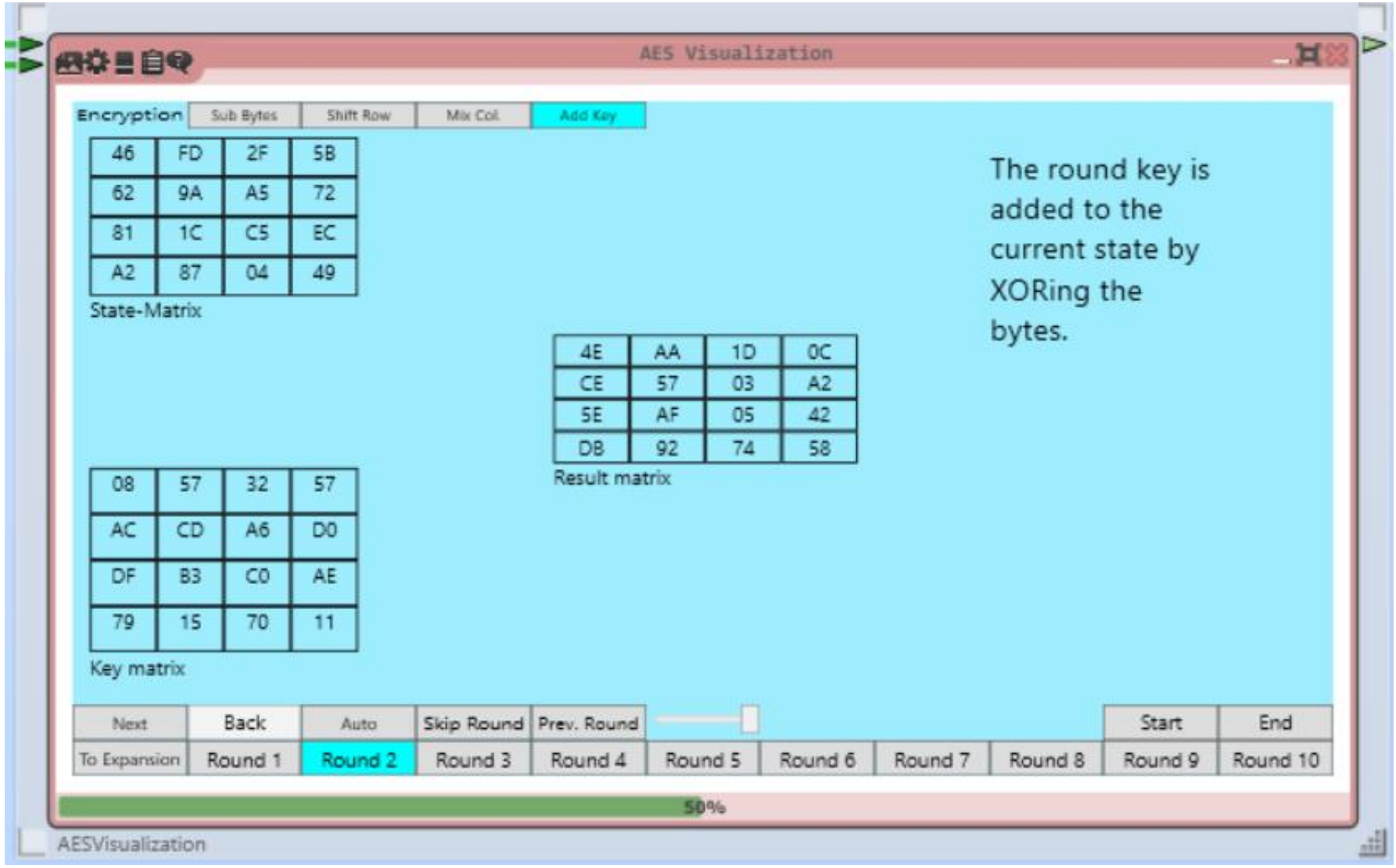
Итог:

$$\begin{bmatrix} 4E & AA & 1D & 0C \\ CE & 57 & 03 & A2 \\ 5E & AF & 05 & 42 \\ DB & 92 & 71 & 58 \end{bmatrix}$$

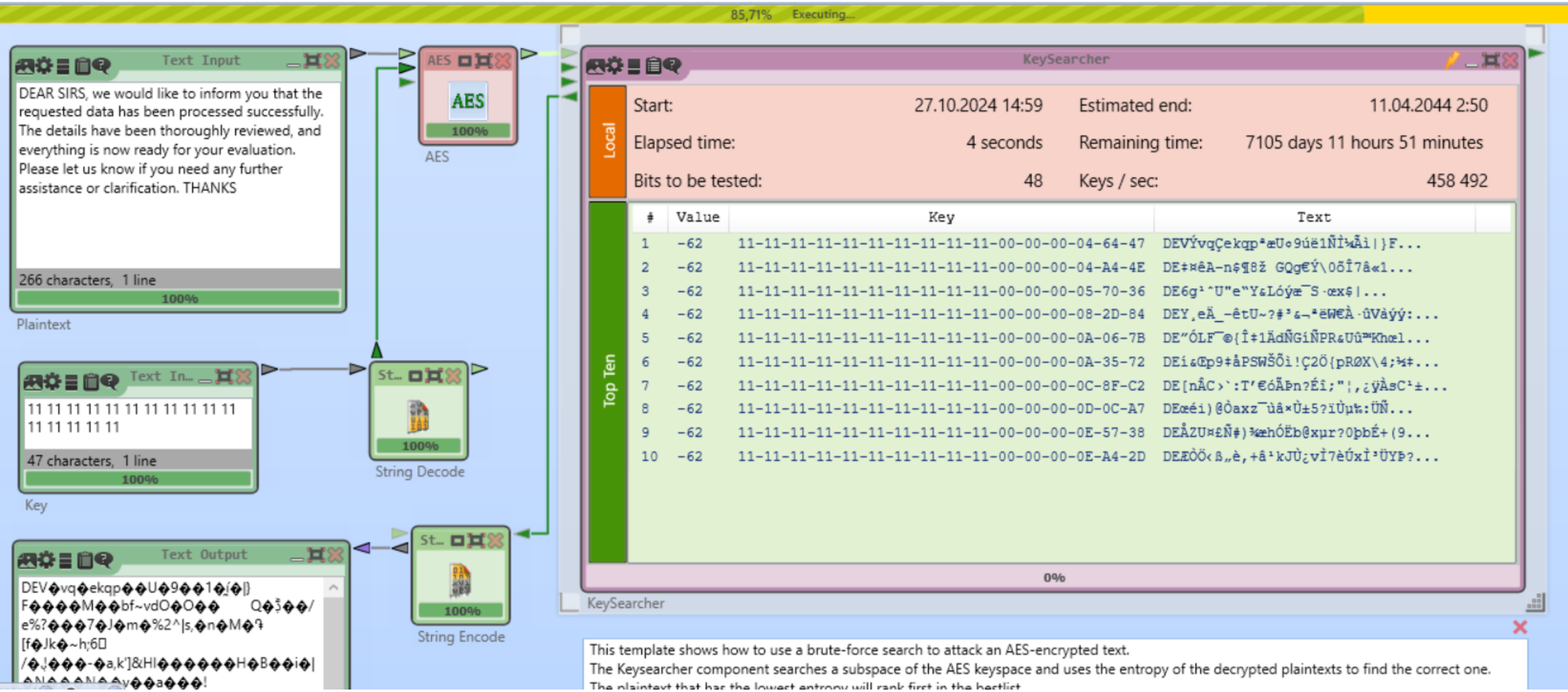
CrypTool 2. Ключ первого раунда



CrypTool 2. Матрица состояния после 1 раунда



AES. Атака грубой силы



AES. Атака грубой силы. Энтропия

Размер открытого текста – 1000 знаков.
Оценочная функция – энтропия.

Количество известных байт	Затраченное время	Количество ядер
14	< 1 секунды	1
12	≈ 4 часа	1
10	≈ 12400 дней	1
14	< 1 секунды	6
12	≈ 45 минут	6
10	≈ 2000 дней	6
14	< 1 секунды	12
12	≈ 30 минут	12
10	≈ 1000 дней	12

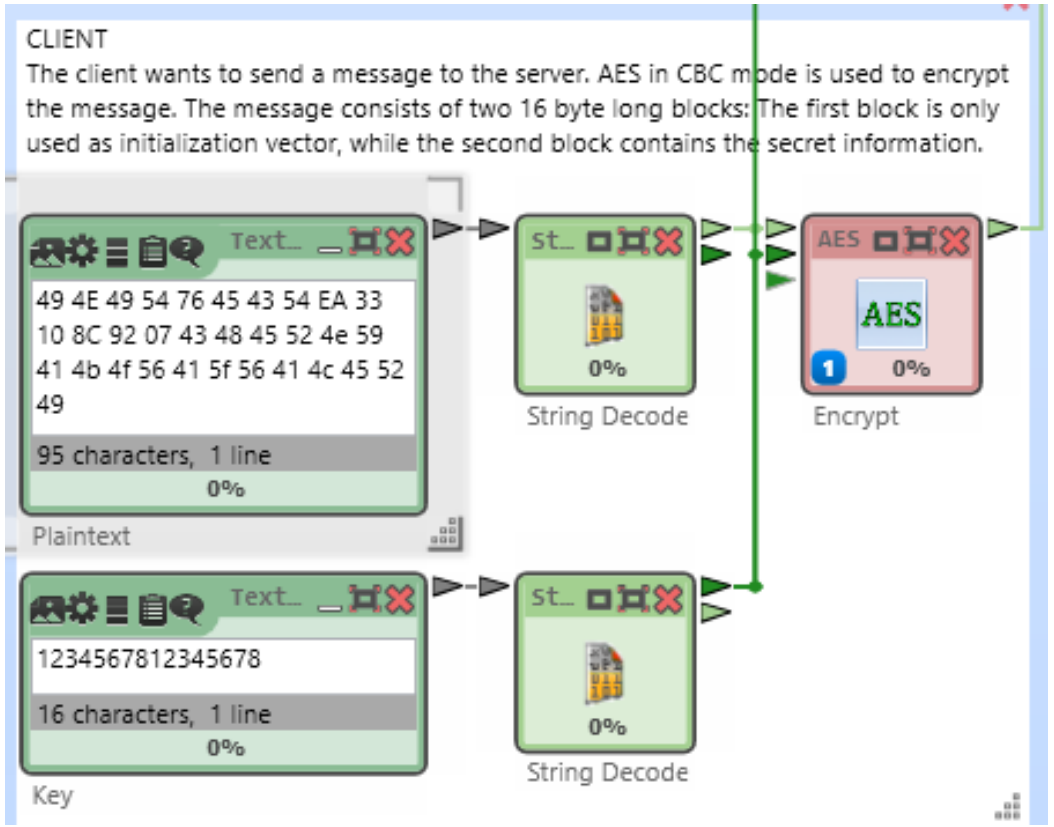
AES. Атака грубой силы. DEAR SIRS

Размер открытого текста – 1000 знаков.
Оценочная функция – DEAR SIRS.

Количество известных байт	Затраченное время	Количество ядер
14	< 1 секунды	1
12	≈ 2 часа 30 минут	1
10	≈ 7100 дней	1
14	< 1 секунды	6
12	≈ 30 минут	6
10	≈ 1500 дней	6
14	< 1 секунды	12
12	≈ 18 минут	12
10	≈ 850 дней	12

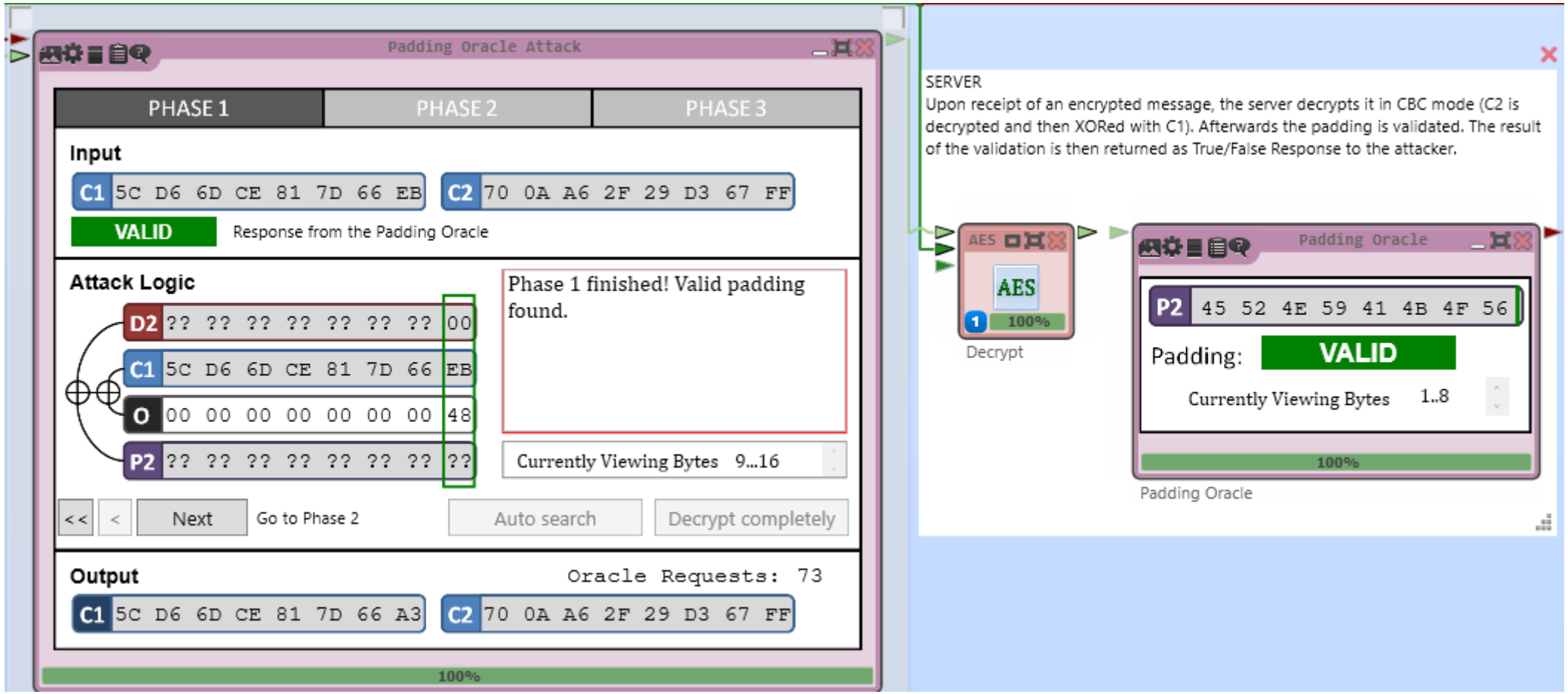
AES. Атака предсказанием дополнения на шифр в режиме CBC

В исходный текст внедрена фамилия и имя:
chernyakova_valeri
43 48 45 52 4e 59 41 4b 4f 56 41 5f 56 41 4c 45 52 49



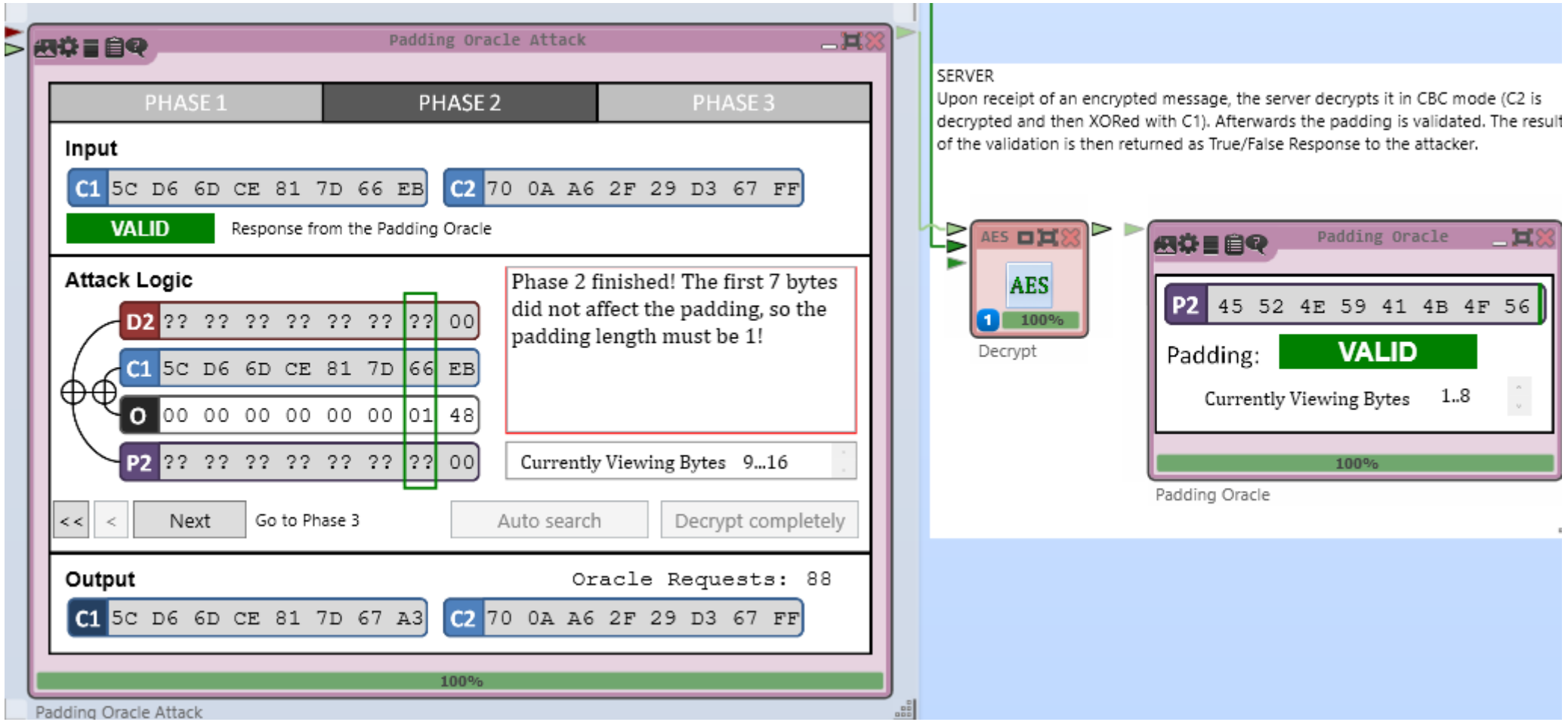
AES. Атака предсказанием дополнения на шифр в режиме CBC. 1 фаза

Поиск допустимого дополнения



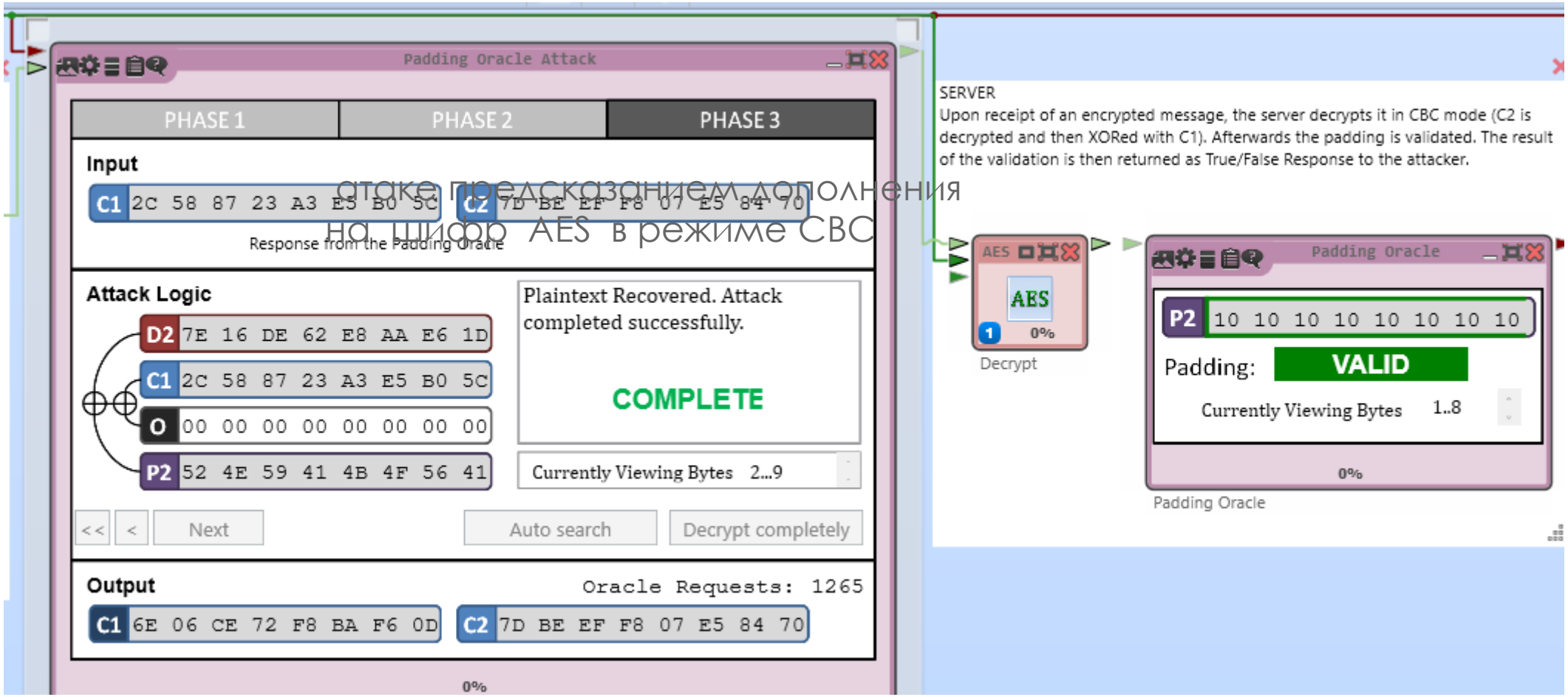
AES. Атака предсказанием дополнения на шифр в режиме CBC. 2 фаза

Поиск первого байта дополнения -> определение допустимой длины дополнения

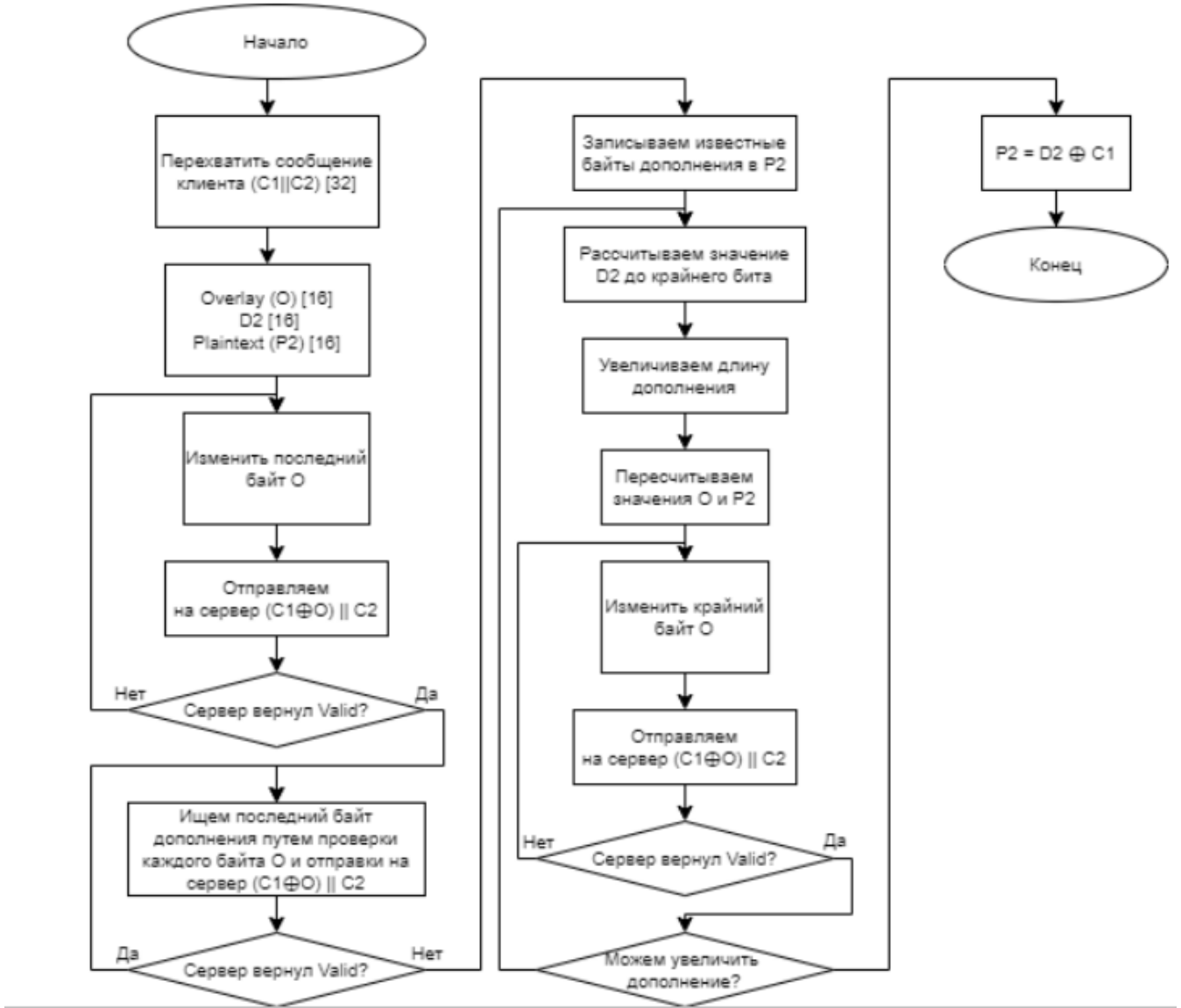


AES. Атака предсказанием дополнения на шифр в режиме CBC. 3 фаза

Расшифровка сообщения по байтам



AES. Схема действия нарушителя при атаке по дополнению



Шифр «Кузнечик»

Задание

1. Изучить алгоритм развертывания ключа шифра Кузнечик с помощью приложения ЛИТОРЕЯ. В качестве секретного ключа выбрать использованный в п. 1, В качестве материала для итерационного ключа выбрать константу N+2, где N - последняя цифра в номере студенческого билета.
2. Изучить раундовые преобразования шифра Кузнечик с помощью приложения ЛИТОРЕЯ. В качестве блока данных и секретного ключа выбрать использованные в п. 1. а в качестве эталонного раунда - раунд с номером N+2, где N - последняя цифра в номере студенческого билета.

Исходные данные

Открытый текст M = “chernyakova_valeria”

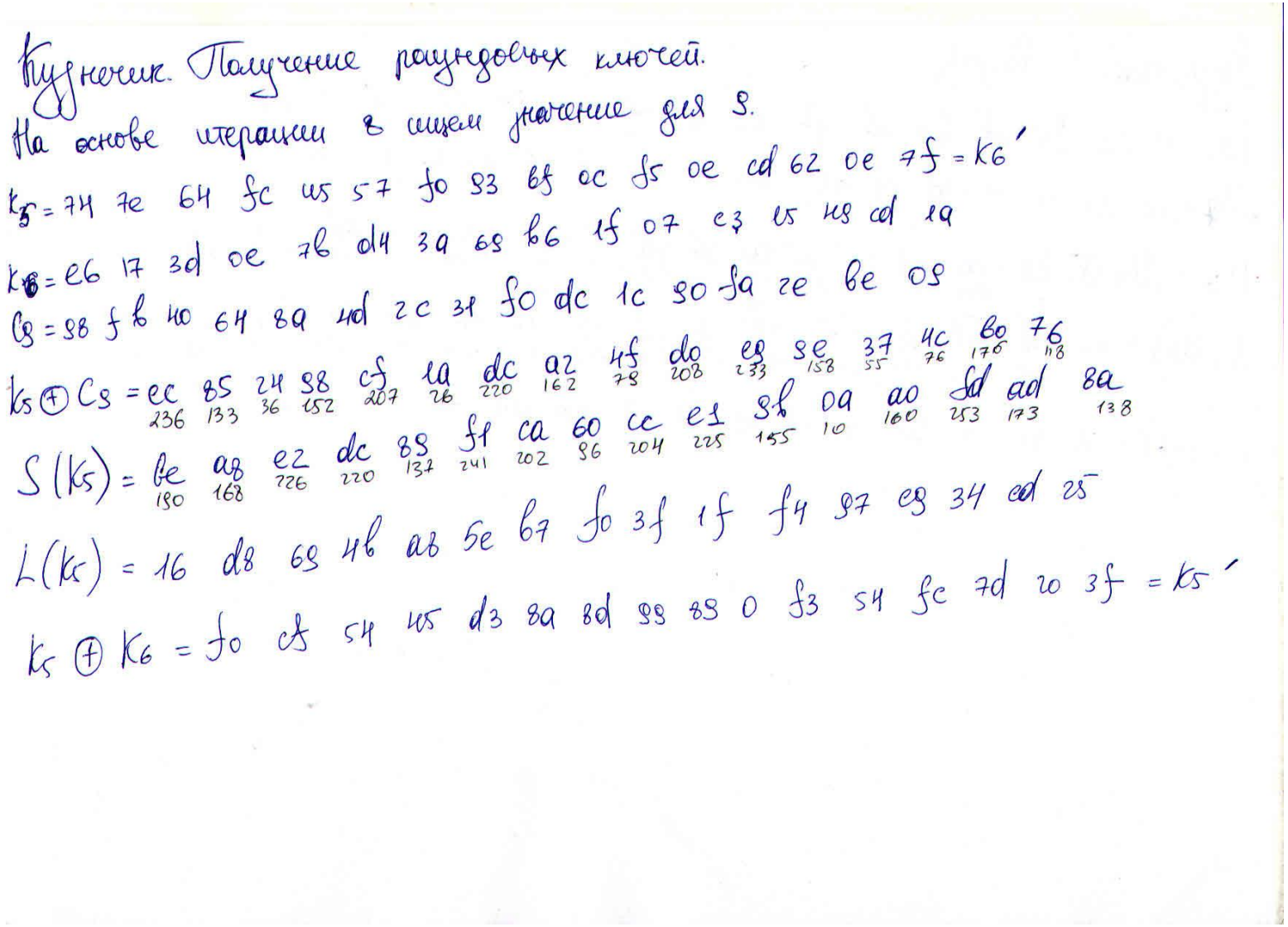
Ключ K = “1304_alekseevna”

Байтовое представление:

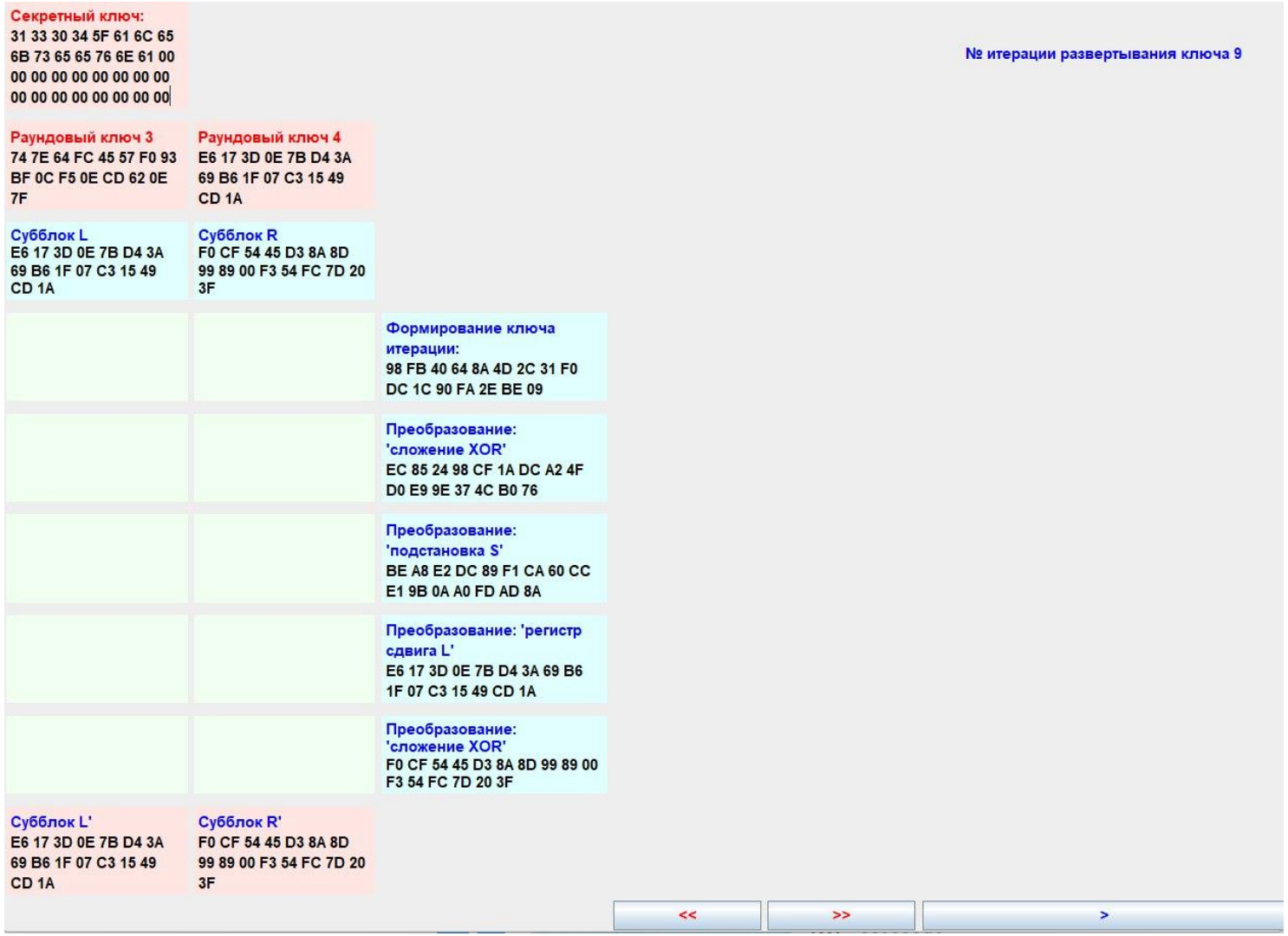
M16 = 63 68 65 72 6e 79 61 6b

K16 = 31 33 30 34 5f 61 6c 65 6b 73 65 65 76 6e 61 00

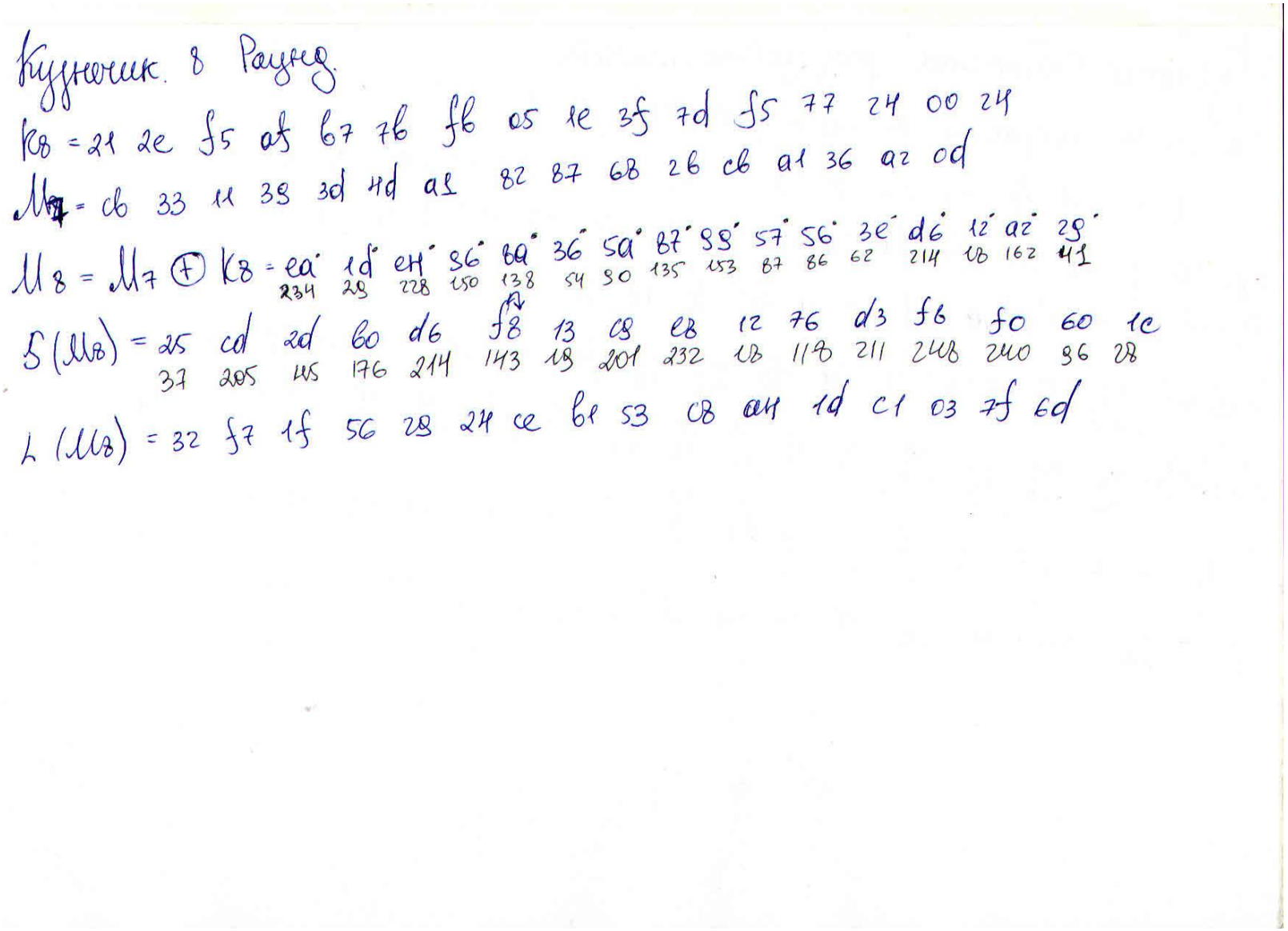
Развертывание ключа. Итерация 9



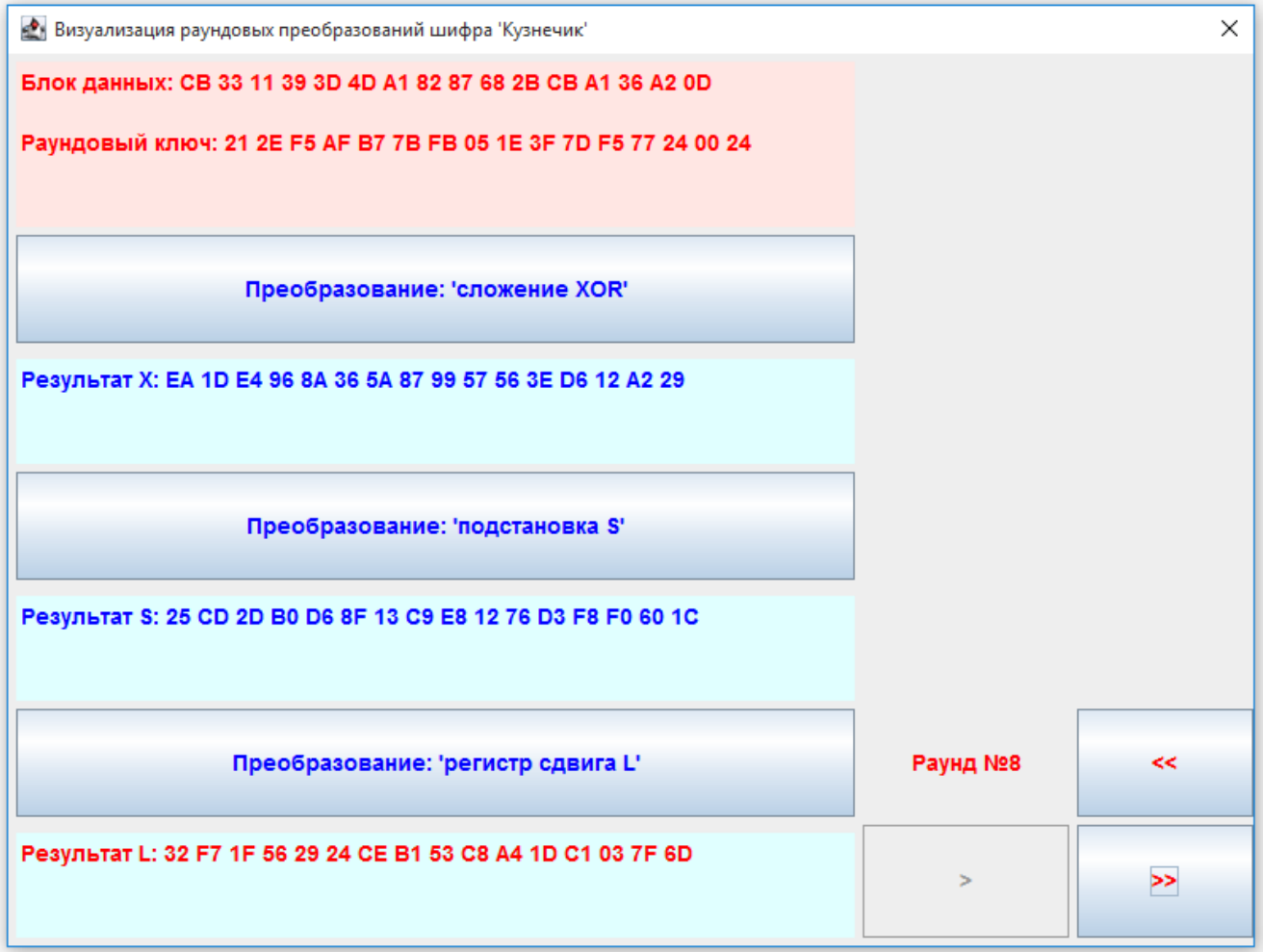
ЛИТОРЕЯ. Развертывание ключа. Раунд 9



Шифрование. Раунд 8



ЛИТОРЕЯ. Шифрование. Раунд 8



Заключение

Изучен шифр AES и выявлены следующие характеристики:

- Блоковый симметричный шифр, размер блока 128 бит. Шифр основан на подстановочно-перестановочной сети. Количество раундов следующее:
  - 10 для 128-битного ключа
  - 12 для 192-битного ключа
  - 14 для 256-битного ключа

Исследована криптостойкость шифра AES и выявлено следующее:

- Как шифрование, так и дешифрование AES распараллеливаемо. Благодаря этому атака грубой силы с использование большего количества ядер более эффективна.
- Облегчить взлом может использование в качестве оценочной функции части выражения исходного текста (вместо энтропии) и знание части ключа.
- Для шифра AES в режиме работы CBC была проведена атака с предсказанием дополнения в среде CrypTool2. Данная атака позволила достаточно быстро расшифровать один из блоков сообщения без знания самого ключа шифрования.

Заключение. Продолжение

Изучен шифр Кузнечик и выявлены следующие характеристики:

- Симметричный блочный шифр, длина ключа – 256 бит, размер блока – 128 бит.
- В основе алгоритма - SP-сеть из 10 раундов, в последнем раунде осуществляется только сложение с раундовым ключом, - и сеть Фейстеля с 32 раундами для развертывания ключа.