

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:

$M = \text{chernyak_valeria}$

Ключ (64 бит):

$K = \text{1304_allekseevna}$

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.

$M_{16} = 63\ 68\ 65\ 72\ 6E\ 78\ 61\ 6B\ 5F\ 76\ 61\ 6C\ 65\ 72\ 68\ 61$

$K_{16} = 31\ 33\ 30\ 34\ 5F\ 61\ 6C\ 6C\ 65\ 6B\ 73\ 65\ 65\ 76\ 6E\ 61$

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
78	15	70	11

Round Key 1.

①

65	76	38
76	6E	8F
6E	61	EF
61	65	4D

Rotated Sub Bytes

31	38	01	08
33	8F	00	AC
30	EF	00	DF
34	4D	00	78

Rcon

②

5F	08	57
61	AC	CD
6C	DF	B3
6C	78	15

+

③

65	57	32
6B	CD	AG
73	B3	CO
65	15	70

+

④

65	32
76	AG
6E	CO
61	70

+

Основное Шифрование AES.

$M_{\text{Matrix}} = \begin{bmatrix} 63 & 6E & 5F & 65 \\ 68 & 78 & 76 & 72 \\ 65 & 61 & 61 & 68 \\ 72 & 6B & 6C & 61 \end{bmatrix}$

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

Ручные преобразования 1 раунда. Продолжение

① Столбцы матрицы состоящий \oplus ключ

$$M_{\text{matr}} \oplus K_{\text{matr}} = \begin{bmatrix} 52 & 31 & 3A & 00 \\ 5B & 18 & 1D & 04 \\ 55 & 0D & 12 & 07 \\ 46 & 07 & 08 & 00 \end{bmatrix} = S_{\text{matr}}$$

② Подстановка Sub Bytes

$$S_{\text{sub}} = \begin{bmatrix} 00 & C7 & 80 & 63 \\ 38 & AD & A4 & F2 \\ FC & D7 & C8 & C5 \\ 5A & C5 & 01 & 63 \end{bmatrix}$$

③ Циклический сдвиг вправо Shift Rows

$$S_{\text{shiftrows}} = \begin{bmatrix} 00 & C7 & 80 & 63 \\ AD & A4 & F2 & 38 \\ C8 & C5 & FC & D7 \\ 63 & 5A & C5 & 01 \end{bmatrix}$$

④ Смешивание столбцов путем умножения на матрицу констант

$$C = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix}$$

$$S_{\text{mix}} = \begin{bmatrix} 16 & 02 & 2F & 5B \\ 62 & 68 & A5 & 72 \\ 81 & 06 & C5 & EC \\ A2 & 62 & 04 & 48 \end{bmatrix}$$

$$S_{\text{mix}} = \begin{bmatrix} 46 & 62 & 81 & A2 \\ FD & 9A & 1C & 87 \\ 2F & A5 & C5 & 04 \\ 5B & 72 & EC & 48 \end{bmatrix}$$

Ручные преобразования 1 раунда. Конец

⑤ Сложение с раундовыми ключами.

Итого:

4E	AA	1D	0C
CE	57	03	A2
5E	AF	05	42
DB	82	7H	58

CrypTool 2. Ключ первого раунда

The screenshot shows the 'AES Visualization' window. The 'Expansion' tab is selected, displaying the key schedule for Round 1. The 'State matrix' is a 4x4 grid of hex values. The 'Result matrix' is a 4x4 grid of hex values. The 'Key schedule' section shows the calculation of the new key for Round 1 by XORing the previous key with the new key's column x-1.

Expansion Sub Bytes Shift Row Mix Col. Add Key

For column x of the new key you XOR column x from the previous key with column x-1 from the new key.

State matrix

31	5F	65	65
33	61	68	76
30	6C	73	6E
34	6C	65	61

Key schedule

65	32
76	A6
6E	C0
61	70

Result matrix

08	57	32	57
AC	CD	A6	D0
DF	83	C0	AE
79	15	70	11

Next Back Auto Skip Round Prev. Round Start End

Skip Expansion **Round 1** Round 2 Round 3 Round 4 Round 5 Round 6 Round 7 Round 8 Round 9 Round 10

0%

CrypTool 2. Матрица состояния после 1 раунда

The screenshot shows the AES Visualization tool interface. The title bar is "AES Visualization". The main window has a light blue background. At the top, there are icons for settings, a list, and a help icon. Below the icons, there are tabs for "Encryption", "Sub Bytes", "Shift Row", "Mix Col", and "Add Key". The "Encryption" tab is selected. The main area displays three 4x4 matrices: the State-Matrix, the Key matrix, and the Result matrix. The State-Matrix is a 4x4 grid of hexadecimal values. The Key matrix is a 4x4 grid of hexadecimal values. The Result matrix is a 4x4 grid of hexadecimal values. To the right of the matrices, there is a text box that says "The round key is added to the current state by XORing the bytes." At the bottom, there is a control bar with buttons for "Next", "Back", "Auto", "Skip Round", "Prev. Round", "Start", and "End". Below these buttons is a progress bar showing "50%". The bottom status bar says "AESVisualization".

Encryption

Sub Bytes

Shift Row

Mix Col

Add Key

46	FD	2F	5B
62	9A	A5	72
81	1C	C5	EC
A2	87	04	49

State-Matrix

4E	AA	1D	0C
CE	57	03	A2
5E	AF	05	42
DB	92	74	58

Result matrix

08	57	32	57
AC	CD	A6	D0
DF	B3	C0	AE
79	15	70	11

Key matrix

The round key is added to the current state by XORing the bytes.

Next

Back

Auto

Skip Round

Prev. Round

Start

End

To Expansion

Round 1

Round 2

Round 3

Round 4

Round 5

Round 6

Round 7

Round 8

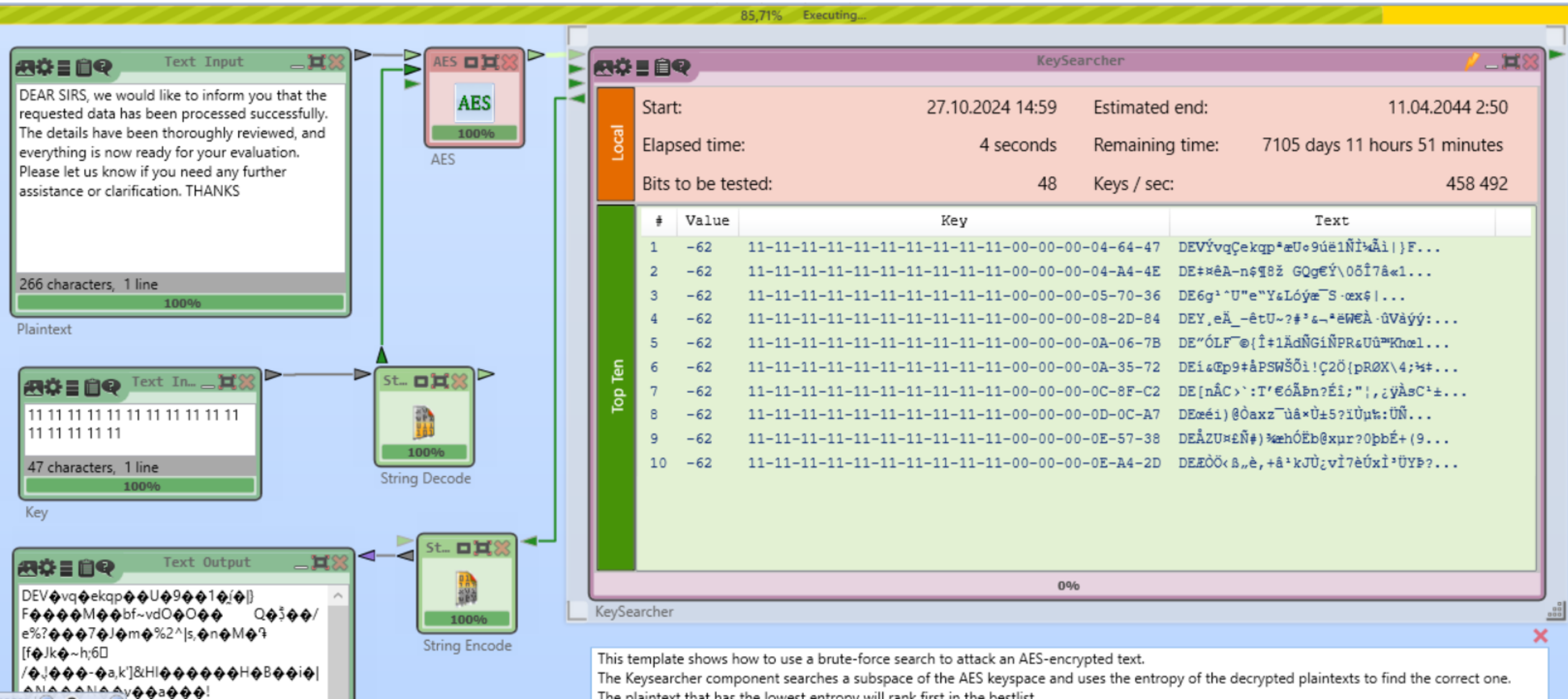
Round 9

Round 10

50%

AESVisualization

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

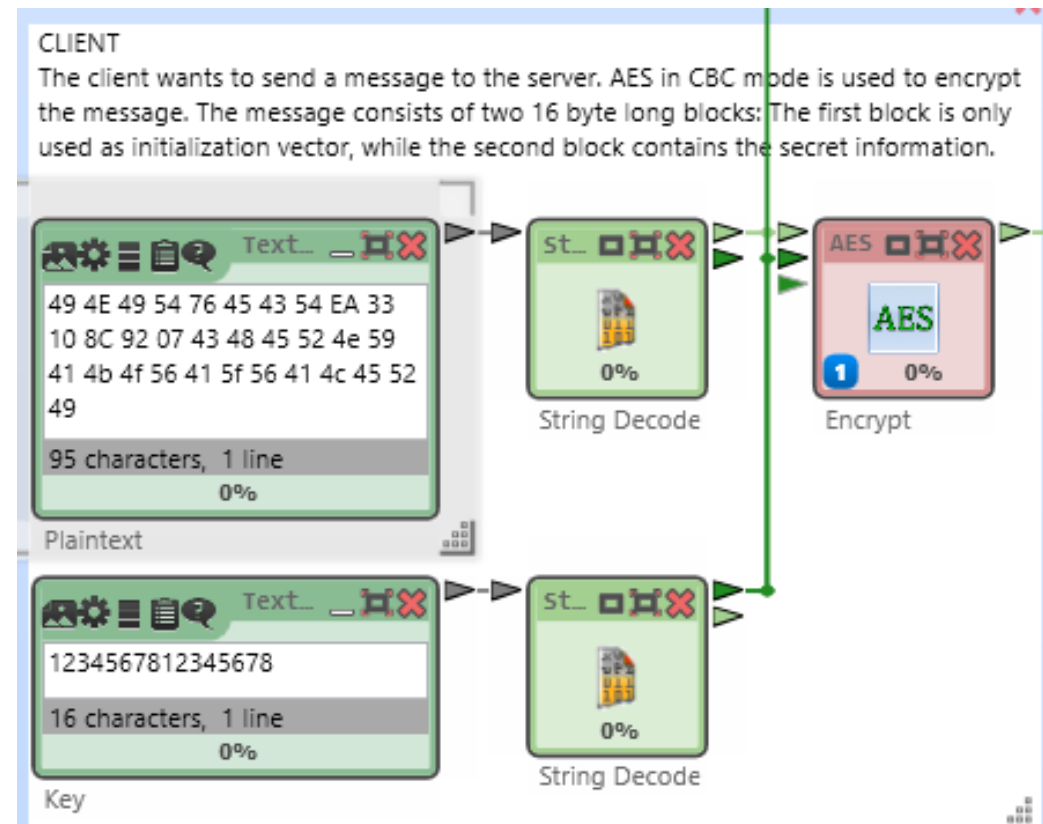
Размер открытого текста – 1000 знаков.

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

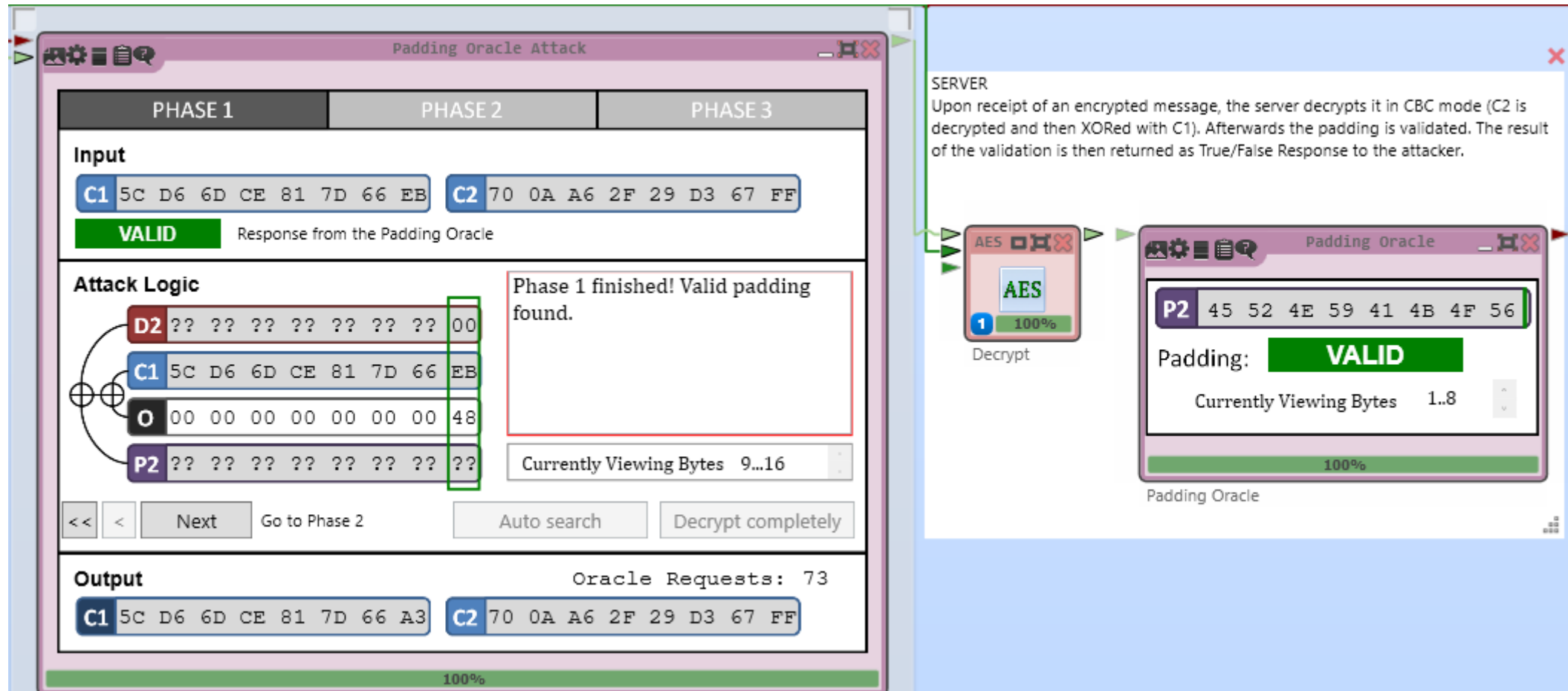
AES. Атака предсказанием дополнения на шифр в режиме CBC

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



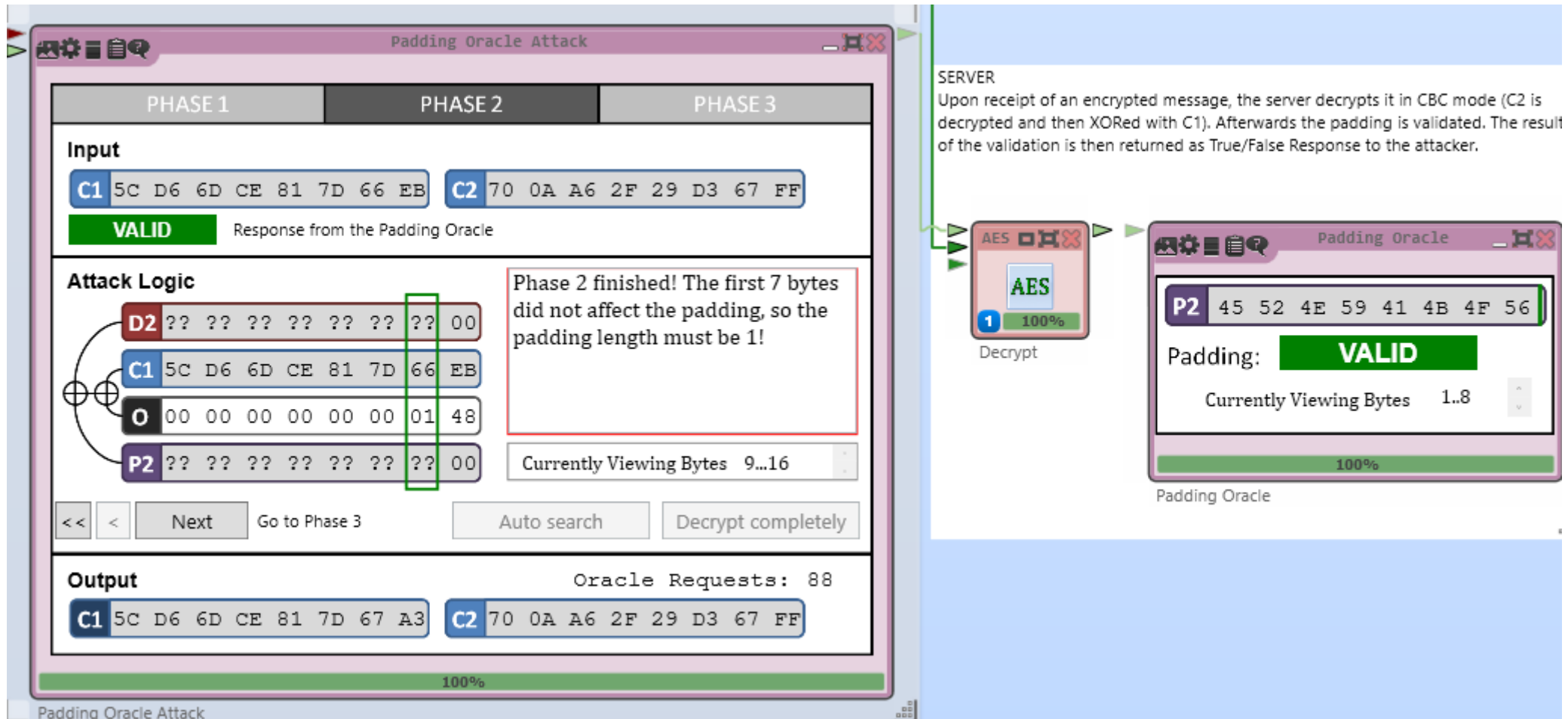
AES. Атака предсказанием дополнения на шифр в режиме CBC. 1 фаза

Поиск допустимого дополнения



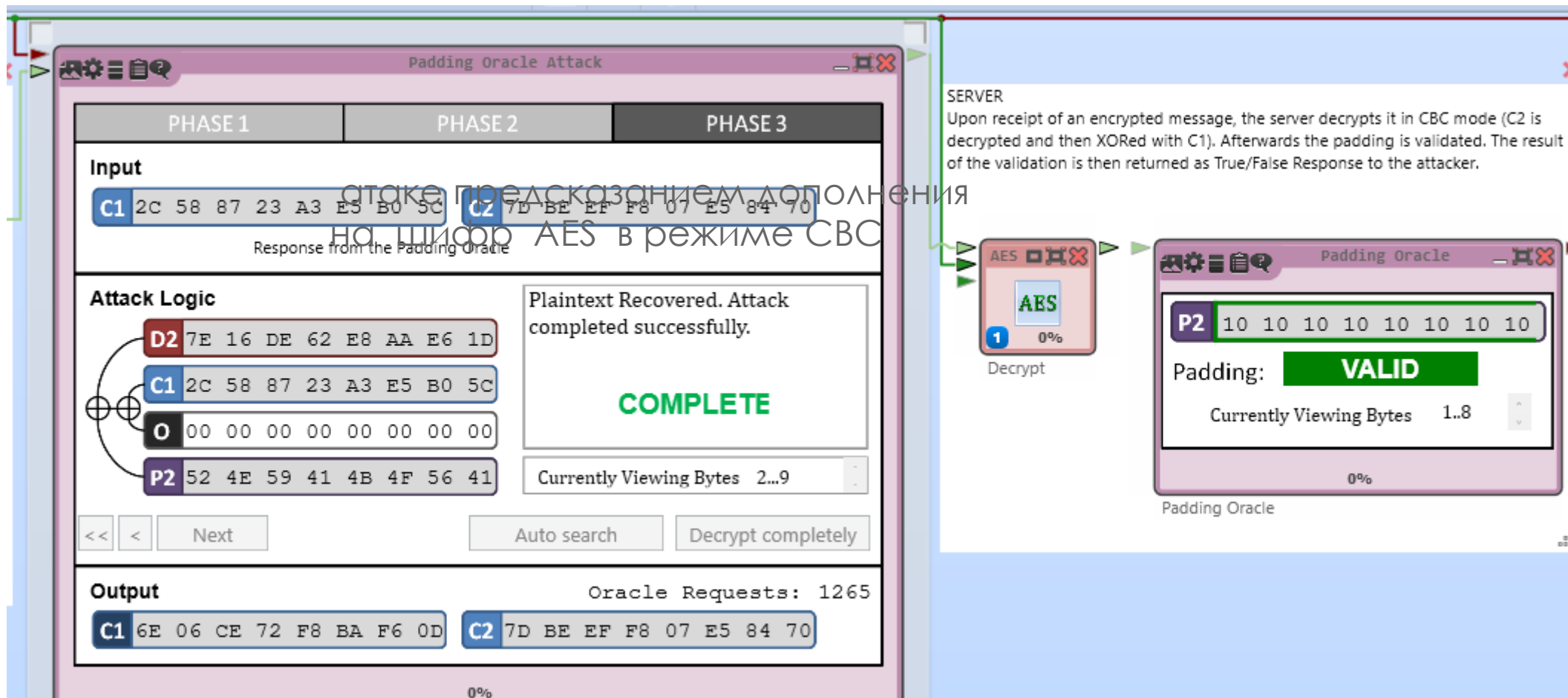
AES. Атака предсказанием дополнения на шифр в режиме CBC. 2 фаза

Поиск первого байта дополнения -> определение допустимой длины дополнения

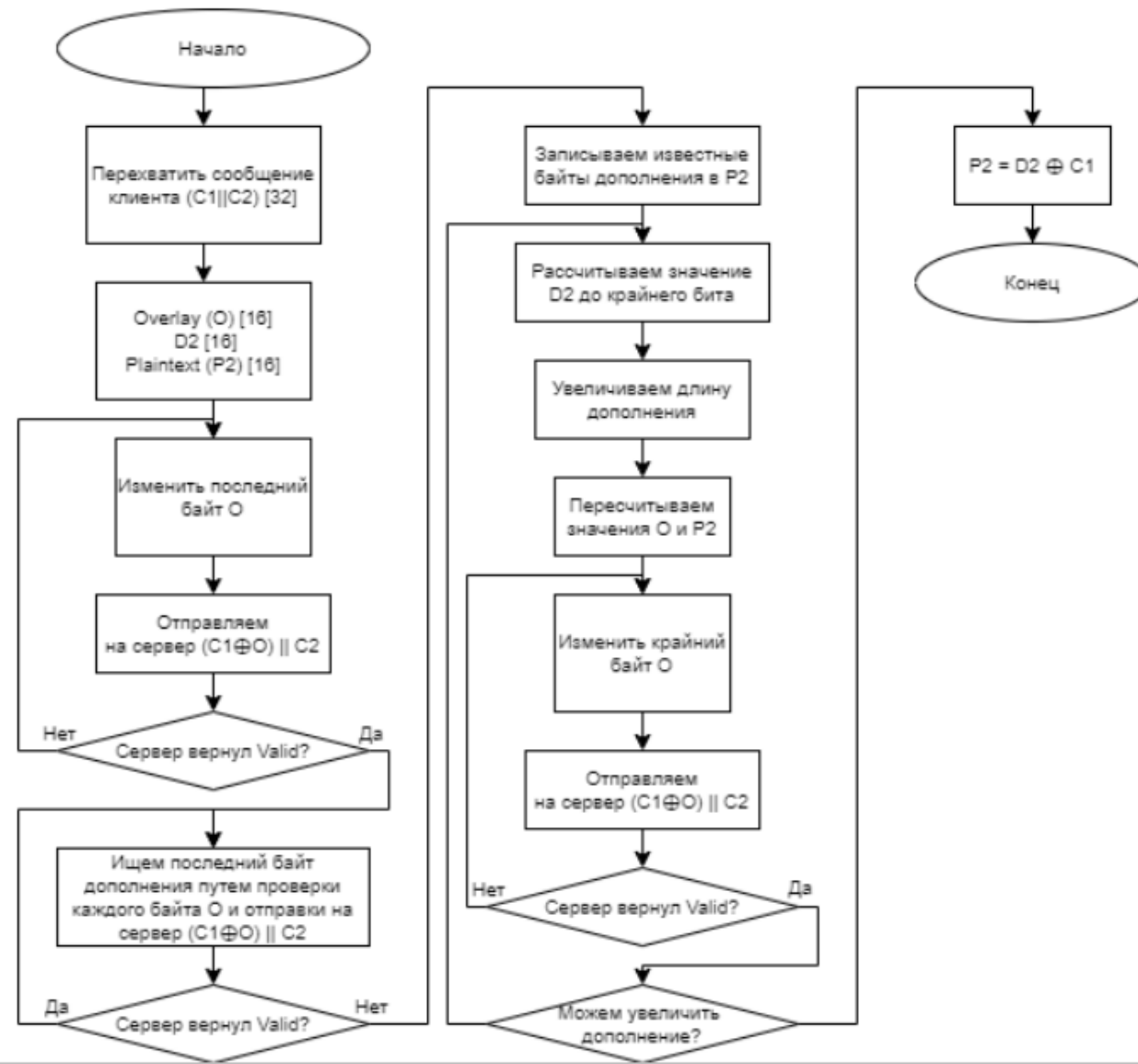


AES. Атака предсказанием дополнения на шифр в режиме CBC. 3 фаза

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

Получение раундовых ключей.

На основе итерации в ищем значение для S .

$K_5 = 74\ 7e\ 64\ fc\ 45\ 57\ f0\ 83\ b5\ 0c\ f5\ 0e\ cd\ 62\ 0e\ 7f = K_6'$

$K_6 = e6\ 17\ 3d\ 0e\ 7b\ d4\ 3a\ 68\ b6\ 1f\ 07\ e3\ 45\ 48\ cd\ 1a$

$C_8 = 88\ fb\ 40\ 64\ 8a\ 4d\ 2c\ 3f\ f0\ dc\ 1c\ 80\ fa\ 2e\ be\ 08$

$K_5 \oplus C_8 =$

ee	85	24	88	c5	1a	dc	a2	4f	do	eg	se	37	4c	60	76
236	133	36	152	207	26	220	162	78	208	233	158	55	76	170	118

$S(K_5) =$

be	a8	e2	dc	88	ff	ca	60	ce	e1	8b	0a	ao	fd	ad	8a
180	168	226	220	137	241	202	86	204	225	155	10	160	253	173	138

$L(K_5) = 16\ d8\ 68\ 4b\ ab\ 5e\ b7\ f0\ 3f\ 1f\ f4\ 87\ e8\ 34\ cd\ 25$

$K_5 \oplus K_6 = f0\ c5\ 54\ 45\ d3\ 8a\ 8d\ 88\ 88\ 0\ f3\ 54\ fc\ 7d\ 20\ 3f = K_5'$

ЛИТОРЕЯ. Развертывание ключа. Раунд 9

Секретный ключ:
31 33 30 34 5F 61 6C 65
6B 73 65 65 76 6E 61 00
00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00

Раундовый ключ 3
74 7E 64 FC 45 57 F0 93
BF 0C F5 0E CD 62 0E
7F

Субблок L
E6 17 3D 0E 7B D4 3A
69 B6 1F 07 C3 15 49
CD 1A

Раундовый ключ 4
E6 17 3D 0E 7B D4 3A
69 B6 1F 07 C3 15 49
CD 1A

Субблок R
F0 CF 54 45 D3 8A 8D
99 89 00 F3 54 FC 7D 20
3F

Формирование ключа
итерации:
98 FB 40 64 8A 4D 2C 31 F0
DC 1C 90 FA 2E BE 09

Преобразование:
'сложение XOR'
EC 85 24 98 CF 1A DC A2 4F
D0 E9 9E 37 4C B0 76

Преобразование:
'подстановка S'
BE A8 E2 DC 89 F1 CA 60 CC
E1 9B 0A A0 FD AD 8A

Преобразование: 'регистр
сдвига L'
E6 17 3D 0E 7B D4 3A 69 B6
1F 07 C3 15 49 CD 1A

Преобразование:
'сложение XOR'
F0 CF 54 45 D3 8A 8D 99 89 00
F3 54 FC 7D 20 3F

Субблок L'
E6 17 3D 0E 7B D4 3A
69 B6 1F 07 C3 15 49
CD 1A

Субблок R'
F0 CF 54 45 D3 8A 8D
99 89 00 F3 54 FC 7D 20
3F

№ итерации развертывания ключа 9

<<

>>

>

Шифрование. Раунд 8

Ключевой. 8 Раунд.

$K_8 = 21\ 2e\ f5\ a5\ b7\ 7b\ fb\ 05\ 1e\ 3f\ 7d\ f5\ 77\ 24\ 00\ 24$

$M_7 = cb\ 33\ 11\ 38\ 3d\ 4d\ a1\ 82\ 87\ 68\ 2b\ cb\ a1\ 36\ a2\ 0d$

$M_8 = M_7 \oplus K_8 =$

ea	1d	en	86	ba	36	5a	87	88	57	56	3e	d6	12	a2	28
234	28	228	150	138	54	80	135	153	87	86	62	214	1b	162	41

$S(M_8) =$

25	cd	2d	60	d6	f8	13	08	e8	12	76	d3	f6	f0	60	1c
37	205	115	176	214	143	18	201	232	1b	11b	211	248	240	86	28

$L(M_8) = 32\ f7\ 1f\ 56\ 28\ 24\ ce\ b1\ 53\ 0b\ a4\ 1d\ c1\ 03\ 7f\ 6d$

ЛИТОРЕЯ. Шифрование. Раунд 8

Визуализация раундовых преобразований шифра 'Кузнечик'

Блок данных: CB 33 11 39 3D 4D A1 82 87 68 2B CB A1 36 A2 0D

Раундовый ключ: 21 2E F5 AF B7 7B FB 05 1E 3F 7D F5 77 24 00 24

Преобразование: 'сложение XOR'

Результат X: EA 1D E4 96 8A 36 5A 87 99 57 56 3E D6 12 A2 29

Преобразование: 'подстановка S'

Результат S: 25 CD 2D B0 D6 8F 13 C9 E8 12 76 D3 F8 F0 60 1C

Преобразование: 'регистр сдвига L'

Результат L: 32 F7 1F 56 29 24 CE B1 53 C8 A4 1D C1 03 7F 6D

Раунд №8

<< >>

Заключение

Изучен шифр AES и выявлены следующие характеристики:

- Блочный 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 использованием 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.