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

Лабораторная работа №5
ИЗУЧЕНИЕ ШИФРОВ AES и Кузнечик

Студент: _____ Порошина Алина, группа 0361

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

Санкт-Петербург 2024

Цель работы

Цель работы: Приобретение знаний и умений в работе с шифрами AES и Кузнечик.

Задачи:

- Изучить преобразования AES.
- Провести исследование криптостойкости AES.
- Изучить действия нарушителя при атаке с предсказанием дополнения AES CBC.
- Изучить алгоритм развертывания ключа шифра Кузнечик.
- Изучить раундовые преобразования шифра Кузнечик.

AES: Исходные данные и результат со значением раундового ключа

Раундовый ключ и результат раунда

BB	A5	97	3B
88	2C	7C	35
11	09	37	68
16	B2	D5	49

Key matrix

B4	2B	F8	62
D2	1C	01	A1
F9	8A	3D	CE
C7	A9	78	FC

Result matrix

Исходный и раундовый ключи

50	53	41	49
4F	48	5F	4E
52	49	41	41
4F	4E	4C	52

State matrix

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

49	6C
4E	DB
41	5A
52	76

7E	2D	6C	25
CC	84	DB	95
52	1B	5A	1B
74	3A	76	24

Result matrix

AES: Ручные расчеты для первого раунда

Блок	P	O	R	O	S	H	I	N	A	_	A	L	I	N	A	R
HEX	50	4F	52	4F	53	48	49	4E	41	5F	41	4C	49	4E	41	52

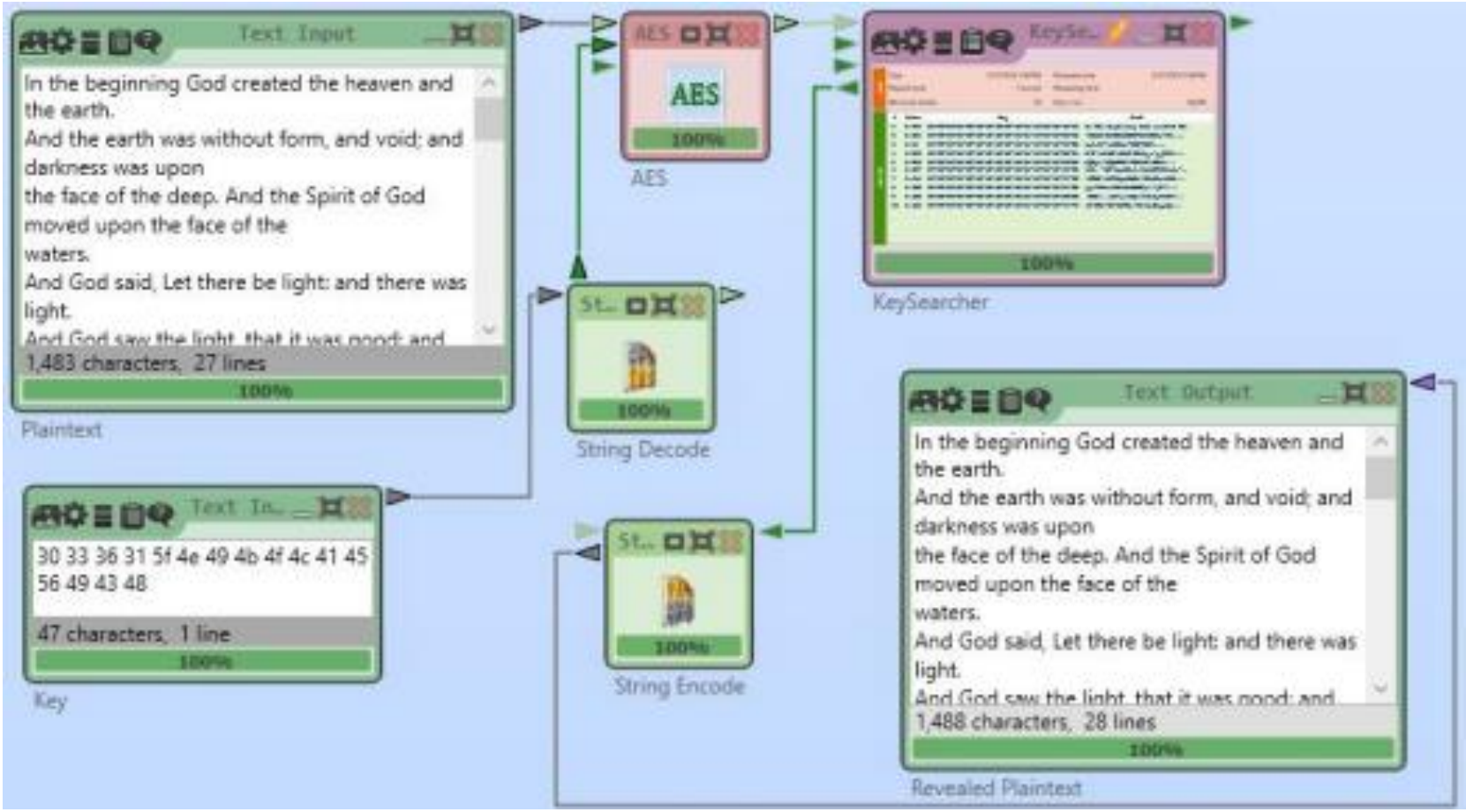
Ключ	0	3	6	1	_	R	O	M	A	N	O	V	N	A	A	P
HEX	30	33	36	31	5F	52	4F	4D	41	4E	4F	56	4E	41	41	50

Ключ, записанный в матрицу 4x4				Циклический сдвиг последнего столбца, замена по таблице, сложение с раундовой константой			Xor столбца со столбцом предыдущего ключа																	
30	5F	41	4E	41	83	82	7E	2D	6C	25	95	2A	28	56	7B	17	32	A9	D3	D7	81	FA	ED	DF	A3	0A	02
33	52	4E	41	41	83	83	CC	84	DB	95	1B	AF	AF	63	E7	3C	A9	3E	B2	B2	D1	36	0A	A3	26	F7	F7
36	4F	4F	41	50	53	53	52	1B	5A	1B	24	36	36	64	7F	25	3E	23	26	26	42	3D	18	26	3D	27	27
31	4D	56	50	4E	2F	2F	74	3A	76	24	25	3F	3F	4B	71	07	23	32	23	23	68	19	1E	3D	DF	9E	9E
83	79	94	4B	B9	56	46	C5	BC	28	63	A6	24	04	C1	7D	55	36	FA	2D	6D	AC	D1	84	B2	ED	55	D5
26	10	1A	B9	66	33	33	15	05	1F	A6	50	53	53	46	43	5C	FA	B6	4E	4E	08	4B	17	ED	47	A0	A0
65	58	40	66	CC	4B	4B	2E	76	36	50	97	88	88	A6	D0	E6	B6	D8	61	61	C7	17	F1	47	38	07	07
F6	EF	F1	CC	4B	B3	B3	45	AA	5B	97	63	FB	FB	BE	14	4F	D8	36	05	05	BB	AF	E0	38	B2	37	37
79	A8	2C	9E	19	D4	CF	B6	1E	32	AC	49	3B	0D	BB	A5	97	3B										
A8	E3	F4	19	61	EF	EF	47	A4	50	49	5F	CF	CF	88	2C	7C	35										
C0	D7	26	61	FB	0F	0F	CF	18	3E	5F	9C	DE	DE	11	09	37	68										
8C	23	C3	FB	9E	0B	0B	87	A4	67	9C	AC	91	91	16	B2	D5	49										

0361
HOLD ON

AES: Атака грубой силой

Для атаки по известной части открытого текста использовался текст “DEARSIRSWEAREGLADTOINVITEYOUTHANKS”

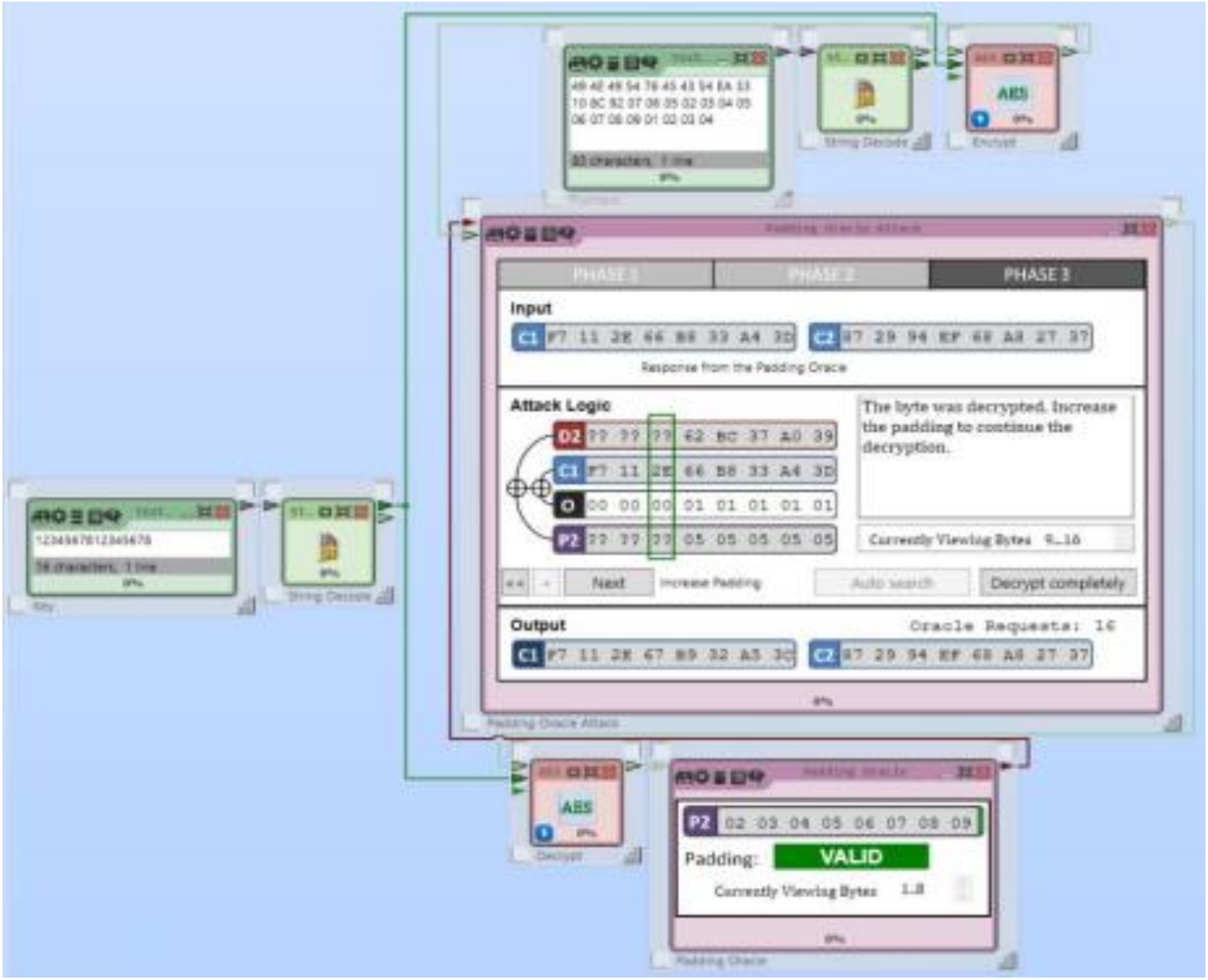


AES: Атака грубой силой

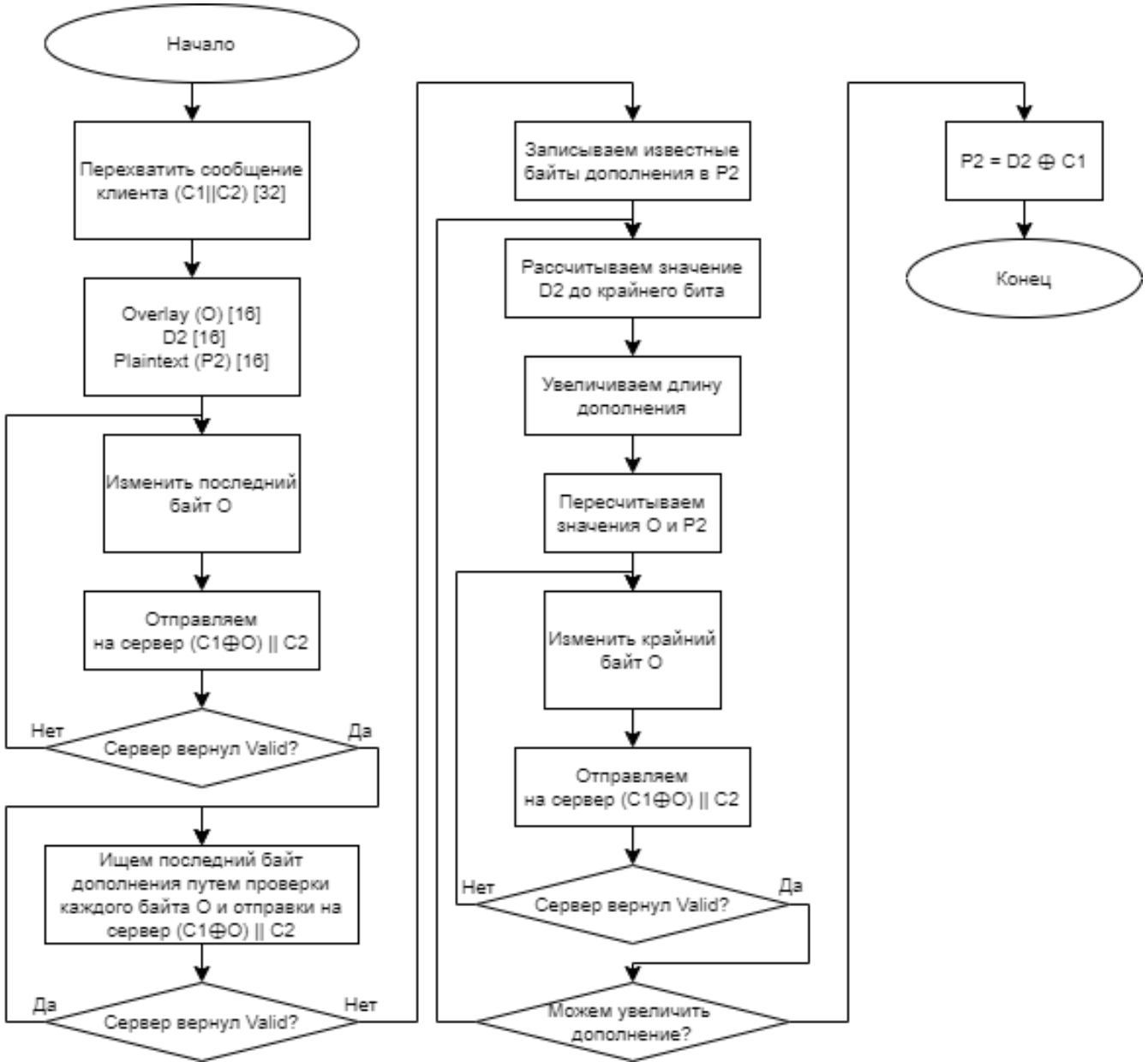
Количество неизвестных байт ключа	Ожидаемое время атаки грубой силой
2	2 с
4	4,5 ч
6	34 г
2 ядра	
6	16,9 г
3 ядра	
6	15 г

Количество неизвестных байт ключа	Ожидаемое время атаки грубой силой
Известный открытый текст	
2	2 с
4	4,5 ч
6	34 г
Известный открытый текст 3 ядра	
6	9,4 г

AES:Шаблон атаки по дополнению

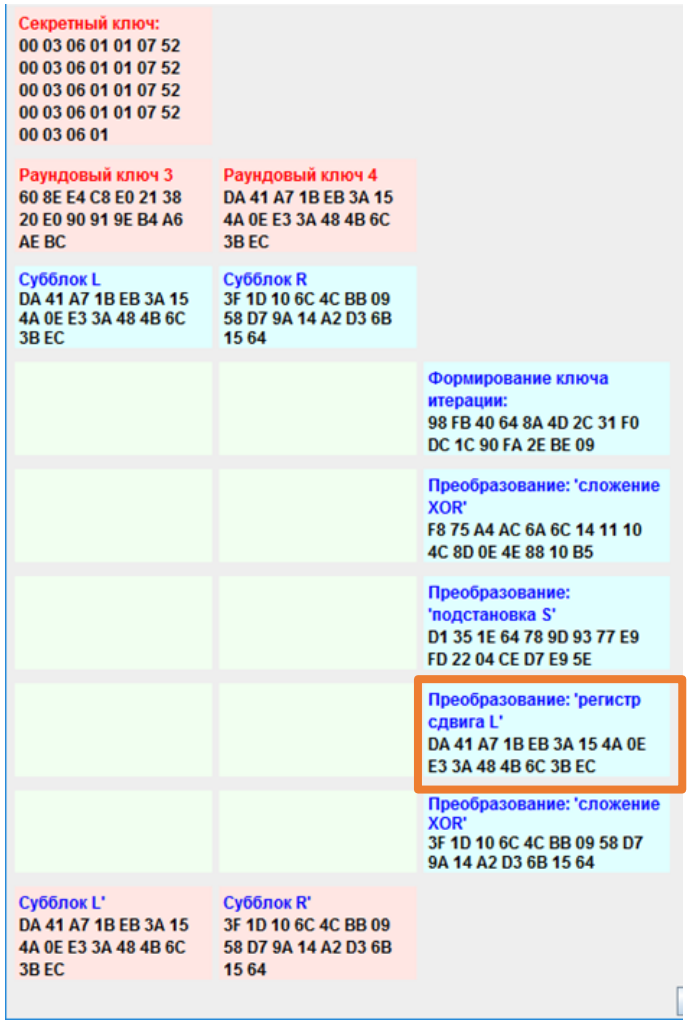


AES: Схема действий нарушителя при атаке по дополнению



ГОСТ Р 34.12.2015 Кузнечик: Развертывание ключа

9 итерация развертывания ключа




```
L: b'da41a71beb3a154a0ee33a484b6c3bec'; R: b'3f1d106c4cbb0958d79a14a2d36b1564'
Iter const: b'447cac8052ddd8824a92a5b083e5550b'
After XOR: b'7b61bcec1e66d1da9d08b112508e406f'
After S: b'80a169be5f9a1baa33fb45f0b5b9ebb1'
After L: b'92ae5221a5555928ee1c9f1832c99145'
b'48eff53a4e6f4c62e0ffa55079a5aaa9'
```

0361
HOLD ON

ГОСТ Р 34.12.2015 Кузнечик: Раундовые преобразования

9 раунд шифрования


```
XOR: b'504c544e541a494d475e461e494d4751'
S: b'b5fd08ce08f12a3aab5d485f2a3aab70'
L: b'619516e46dab50650fc88d4ad03cdf1e'
```

0361
HOLD ON

Выводы

Заключение AES:

• Был исследован шифра AES и выявлены следующие основные характеристики шифра: симметричный блочный шифр, длина ключа варьируется в зависимости от версии: 128, 192 и 256 бит, размер блока - 128 бит. Число раундов зависит от длины ключа: 10 для ключа 128 бит, 12 для 192 и 14 для 256. В основе алгоритма - SP-сеть, в последнем раунде отсутствует одна из процедур (MixColumns), что не влияет на безопасность шифра.

• Для первого раунда были проведены расчеты ключа (0A551A4C29672B62642D6C2F80CB8EC6) и результата раунда (8F688A9C21547F672F51169D93E37495), результаты автоматизированных и ручных расчетов совпали.

• Было оценено время атаки грубой силой при известной части ключа на примере текста длиной ~1500 символов при разном количестве машинных ресурсов: в случае 6 неизвестных байтов ключа, результат варьируется от 15 до 34 лет. При атаке по известному открытому тексту результаты улучшаются до диапазона от 9.4 до 34 лет.

• Была исследована атака по дополнению на AES в режиме CBC и построена схема алгоритма действий нарушителя.

Заключение ГОСТ Р 34.12.2015 Кузнечик:

• Был исследован шифр ГОСТ Р 34.12.2015 Кузнечик и выявлены следующие основные характеристики данного шифра: 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.

• Был проведен расчет результата 11 итерации развертывания ключа (3bb1de4aadf0216bbc9d4ba9b2a51acb), результаты ручных и автоматизированных расчетов совпали. Была выявлена ошибка вывода блока после L-преобразования в программе “Литорея” в визуализации развертывания ключа.

• Был проведен расчет результата первого раунда шифрования (8022ca157f861eaf9e086fbeaa1e8967), результаты ручных и автоматизированных расчетов совпали.

Спасибо за внимание!
Готова ответить на ваши вопросы.