

**МИНОБРНАУКИ РОССИИ**  
**САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ**  
**ЭЛЕКТРОТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ**  
**«ЛЭТИ» ИМ. В.И. УЛЬЯНОВА (ЛЕНИНА)**  
**Кафедра МО ЭВМ**

**ОТЧЕТ**  
**по лабораторной работе №5**  
**по дисциплине «Криптография и защита информации»**  
**ТЕМА: ИЗУЧЕНИЕ И ИССЛЕДОВАНИЕ ШИФРОВ AES и Кузнечик.**

Студент гр. 0303

Калмак Д.А.

Преподаватель

Племянников А.К.

Санкт-Петербург

2023

## **Цель работы.**

Изучить и исследовать шифры AES и Кузнечик.

## **Порядок выполнения работы.**

1. Изучить преобразования AES по шаблонной схеме AES Visualisation из CrypTool 2 с учетом рекомендаций Методического пособия из задания раздела 5.1 (на с. 26).

2. Провести исследование криптостойкости AES с учетом рекомендаций Методического пособия из задания раздела 5.3 (на с. 28)

3. Изучить действия нарушителя при атаке предсказанием дополнения на шифр в режиме CBC с учетом рекомендаций Методического пособия из задания раздела 5.4 (на с. 29)

4. 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. При выполнении задания полезно изучить статью <https://habr.com/ru/articles/459004/>

5. 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.

## Выполнение работы.

### 1. Шифр AES

#### 1.1 Преобразования AES по шаблонной схеме AES Visualisation

Исходный текст: KALMAKDANIIL

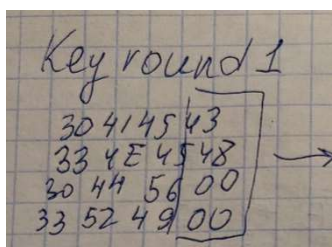
В hex виде: 4B 41 4C 4D 41 4B 44 41 4E 49 49 4C 00 00 00 00

Ключ: 0303ANDREEVICH

В hex виде: 30 33 30 33 41 4E 44 52 45 45 56 49 43 48 00 00

1. Определим ключ первого раунда  $K_1$

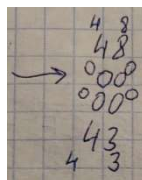
Ключ длиной 128 бит. Запишем ключ в матрицу состояний.



Handwritten matrix for Key round 1:

30	41	45	43
33	4E	45	48
30	44	56	00
33	52	49	00

Возьмем последний столбец и первый элемент перенесем в конец, а остальные элементы поднимем.



Handwritten circular shift of the last column:

4	3
48	
00	00
00	00
43	
4	3

С помощью таблицы подстановок S-box сделаем замену, при этом необходимо каждое число разделить на две цифры, где левая – номер строки, а правая – номер столбца.

	X0	X1	X2	X3	X4	X5	X6	X7	X8	X9	XA	XB	XC	XD	XE	XF
0X	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	A8	76
1X	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2X	87	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3X	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4X	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5X	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6X	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7X	51	A3	40	8F	92	9D	38	F5	BC	86	DA	21	10	FF	F3	D2
8X	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9X	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	08	DB
AX	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
BX	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
CX	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	48	BD	88	8A
DX	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
EX	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
FX	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

52  
→ 63  
63  
1A

Проведем XOR с константой, которая зависит от номера раунда.

Раунд	Константа (RCon)	Раунд	Константа (RCon)
1	(01 00 00 00) <sub>16</sub>	6	(20 00 00 00) <sub>16</sub>
2	(02 00 00 00) <sub>16</sub>	7	(40 00 00 00) <sub>16</sub>
3	(04 00 00 00) <sub>16</sub>	8	(80 00 00 00) <sub>16</sub>
4	(08 00 00 00) <sub>16</sub>	9	(1B 00 00 00) <sub>16</sub>
5	(10 00 00 00) <sub>16</sub>	10	(36 00 00 00) <sub>16</sub>

01 52  
→ 00 63  
00 63  
00 1A

53  
63  
63  
1A

Проведем XOR полученного столбца с каждым столбцом матрицы состояний ключа и получим ключ первого раунда  $K_1$

30 53 → 63  
33 63 → 50  
30 63 → 53  
33 1A → 29

41 63 → 22  
4E 50 → 1E  
44 53 → 17  
52 29 → 7B

45 22 → 67  
45 1E → 5B  
56 17 → 41  
49 7B → 32

43 67 → 24  
48 5B → 13  
00 41 → 41  
00 32 → 32

63 22 67 24  
50 1E 5B 13  
53 17 41 41  
29 7B 32 32

KEY 1

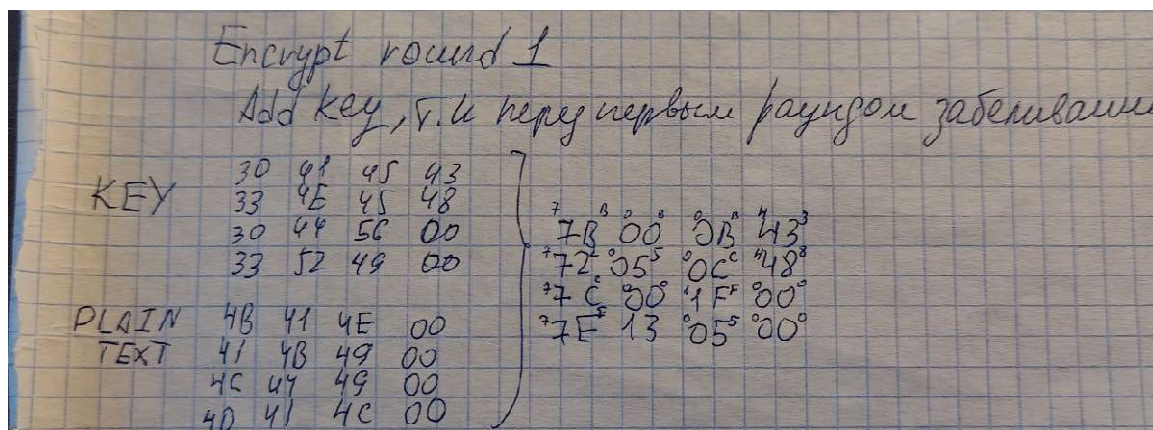
Полученный ключ совпадает с ключом, полученным в Cryptool 2.

63	22	67	24
50	1E	5B	13
53	17	41	41
29	7B	32	32

Result matrix

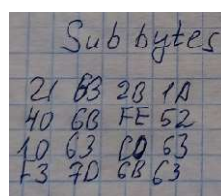
## 2. Произведем первый раунд зашифровки исходного текста

Перед первым раундом применяется дополнительное забеливание с использованием ключа, поэтому произведем XOR матрицы ключа и матрицы исходного текста.



С помощью таблицы подстановок S-box произведем процедуру SubBytes, при этом необходимо каждое число разделить на две цифры, где левая – номер строки, а правая – номер столбца.

	X0	X1	X2	X3	X4	X5	X6	X7	X8	X9	XA	XB	XC	XD	XE	XF
0X	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1X	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2X	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3X	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4X	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5X	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6X	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7X	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8X	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9X	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
AX	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
BX	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
CX	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
DX	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
EX	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
FX	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16





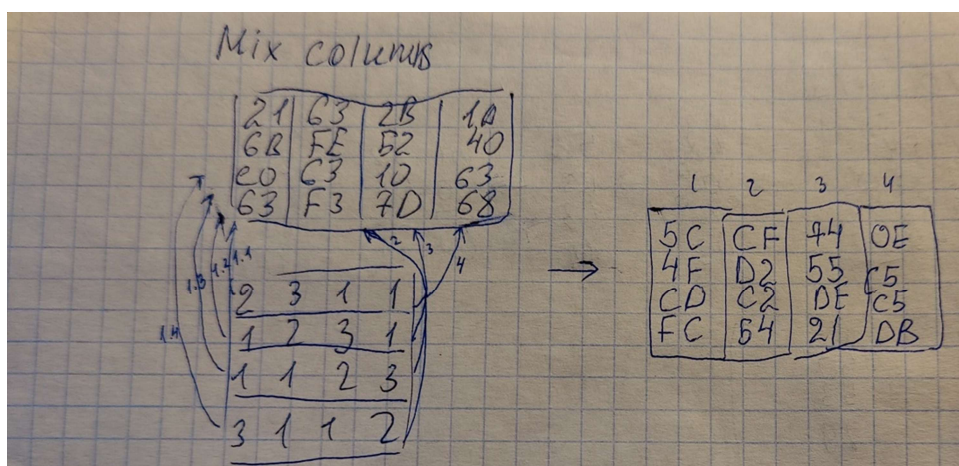
Произведем операцию ShiftRow, а именно циклический сдвиг влево: не сдвигать первую строку, циклически сдвинуть на один влево вторую, на два – третью, на три – четвертую.

Shift row

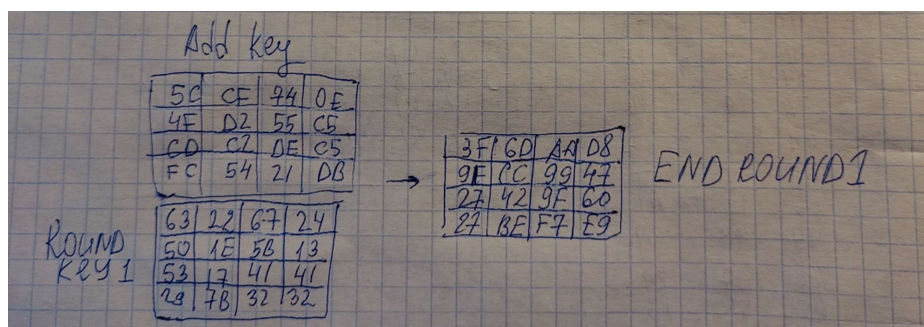
21	63	2B	1A
6B	FE	52	40
C0	63	1D	63
63	F3	7D	68

Произведем операцию MixColumns, а именно умножение матрицы констант на каждый столбец полученной матрицы, причем умножение в поле Галуа по основанию  $2^8$  - в  $GF(2^8)$ , сложение по модулю два (XOR).

02	03	01	01
01	02	03	01
01	01	02	03
03	01	01	02



Произведем операцию AddRoundKey, а именно XOR матрицы раундового ключа  $K_1$  и полученной матрицы, и получим шифротекст после первого раунда.

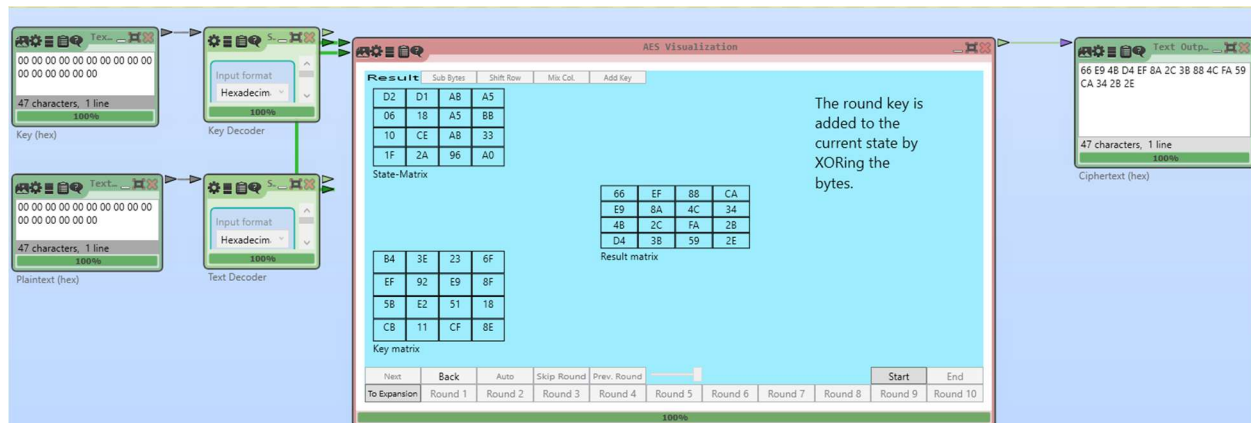


Полученный шифротекст совпадает с шифротекстом, полученным в Cryptool 2.

3F	6D	AA	D8
9F	CC	99	47
27	42	9F	60
27	BE	F7	E9

Result matrix

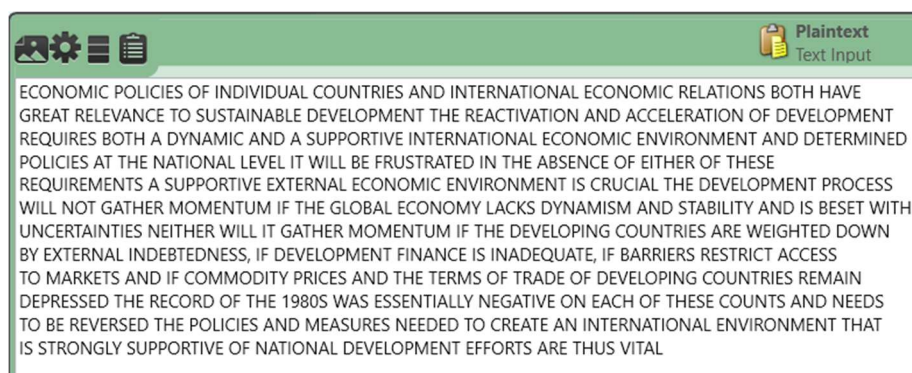
Проведем шифрование AES с помощью ключа, состоящего из нулей, и исходного текста, состоящего из нулей.



Шифротекст не состоит из нулей благодаря операциям, производимым в алгоритме.

## 1.2 Исследование криптостойкости AES

Выбран исходный текст на английском языке, в котором количество символов больше тысячи.



Выбран ключ: 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11



Для AES оценено время проведения атаки «грубой силы» с оценочной функцией энтропия в случаях, когда известна часть ключа с 14 байтами, 12

байтами и 10 байтами и задействовано разное число ядер процессора: одно, четыре и восемь.

Известный ключ, байт	Время проведения атаки грубой силы с 1 ядром	Время проведения атаки грубой силы с 4 ядрами	Время проведения атаки грубой силы с 8 ядрами
14 байт	1 секунда	1 секунда	1 секунда
12 байт	1 час 39 минут	30 минут	19 минут
10 байт	4971 день 20 часов 7 минут	1343 дня 15 часов 52 минуты	994 дня 10 часов 51 минута

Выбран исходный текст в виде DEAR SIRS message THANKS.



Выбран ключ: 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11



Для AES оценено время проведения атаки «грубой силы» с оценочной функцией словосочетание DEAR SIRS в случаях, когда известна часть ключа с 14 байтами, 12 байтами и 10 байтами и задействовано разное число ядер процессора: одно, четыре и восемь.

Известный ключ, байт	Время проведения атаки грубой силы с 1 ядром	Время проведения атаки грубой силы с 4 ядрами	Время проведения атаки грубой силы с 8 ядрами
14 байт	1 секунда	1 секунда	1 секунда
12 байт	1 час 39 минут	30 минут	19 минут
10 байт	4971 день 20 часов 7 минут	1343 дня 15 часов 52 минуты	994 дня 10 часов 51 минута

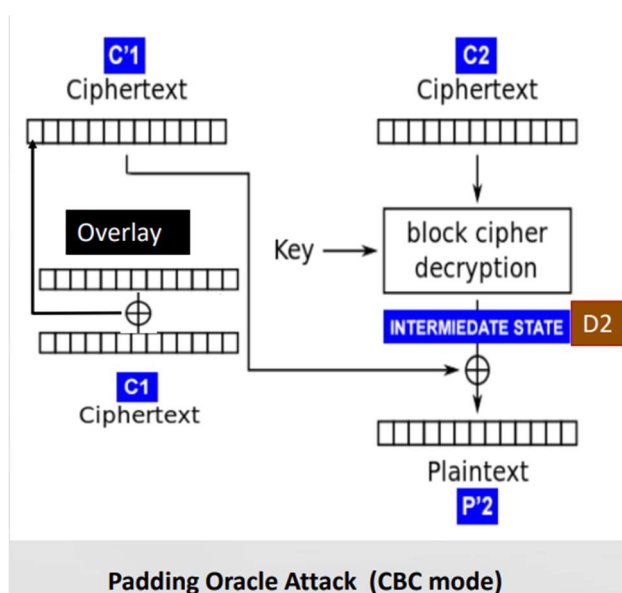


14 байт	1 секунда	1 секунда	1 секунда
12 байт	37 минут	12 минут	11 минут
10 байт	1714 дней 21 час 23 минуты	552 дня 18 часов 49 минут	473 дня 15 часов 42 минуты

Исходя из полученных данных, время проведения атаки грубой силы растет экспоненциально. При этом время проведения атаки грубой силы уменьшается с увеличением числа процессоров и отношение времени растет с уменьшением длины известной части ключа. Время проведения атаки грубой силы больше с использованием оценочной функции энтропии, чем с использованием оценочной функции словосочетания из исходного текста.

### 1.3 Изучение действий нарушителя при атаке предсказанием дополнения на шифр в режиме CBC

В атаке предсказанием дополнения на шифр в режиме CBC предполагается, что нарушитель имеет возможность изменять и отправлять блоки зашифрованного сообщения серверу с целью его расшифровки. Он также может определить ответ сервера о правильности дополнения последнего блока шифротекста. Начало расшифровки сообщения нарушителем происходит с последнего блока шифротекста.



Нарушитель хочет расшифровать  $C2$ , зная правило дополнения блока открытого текста  $P2$ . Для этого он изменяет блок шифротекста, передает измененный блок  $C1'$  и анализирует реакцию сервера-получателя на корректность дополнения:

$$P2' = D2 \oplus C1'$$

Знание реакции сервера-получателя позволяет восстановить

$$D2 = P2' \oplus C1'$$

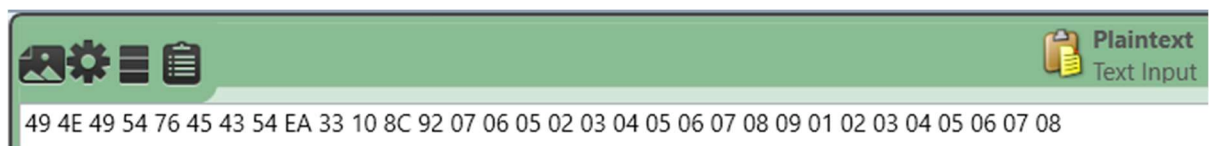
Расшифровка производится по правилу

$$P2 = D2 \oplus C1$$

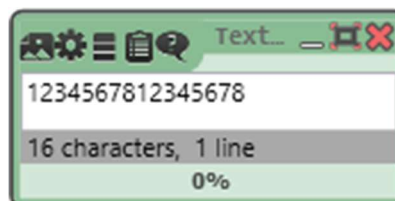
В Cryptool 2 атака предсказанием дополнения реализована в три фазы:

1. Нахождение длины дополнения.
2. Подбор дополнения.
3. Расшифровка текста.

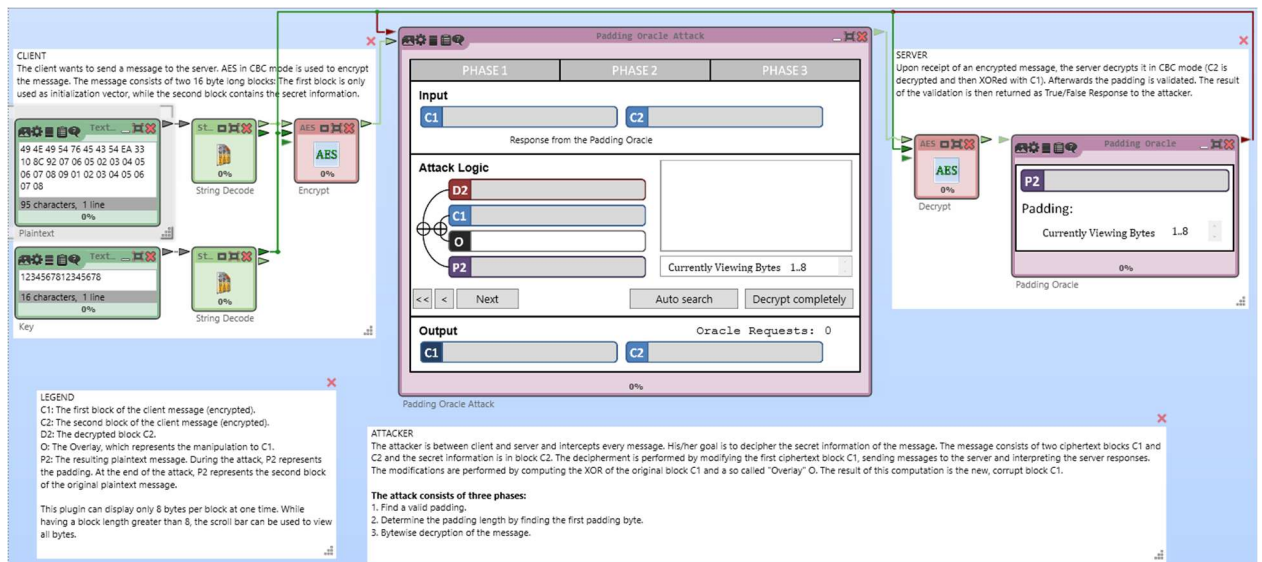
Исходный текст:



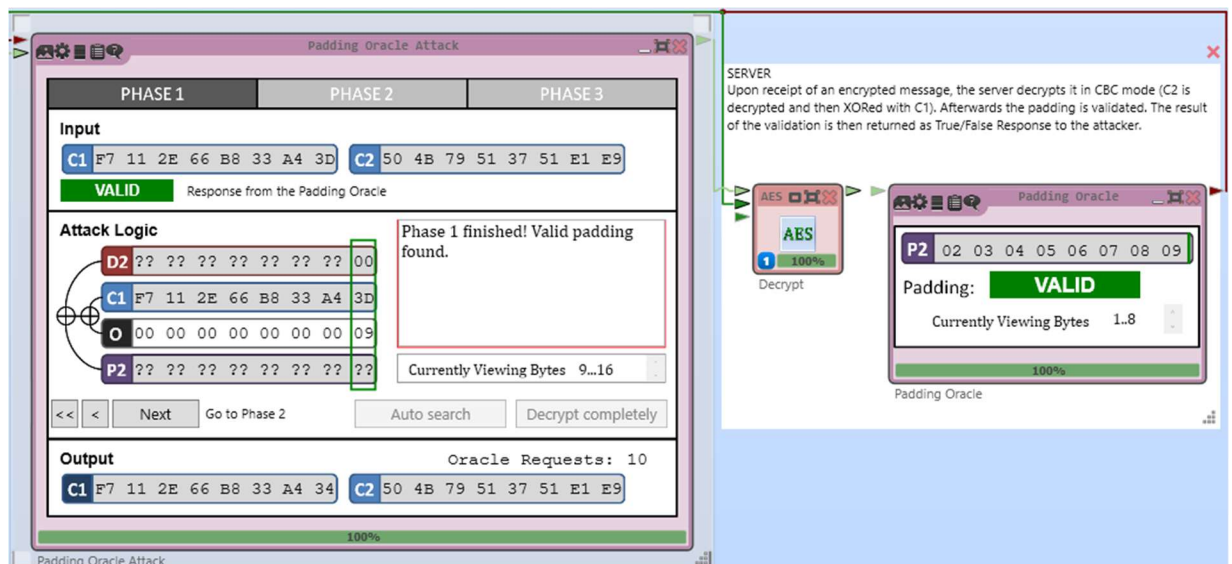
Выбран ключ:



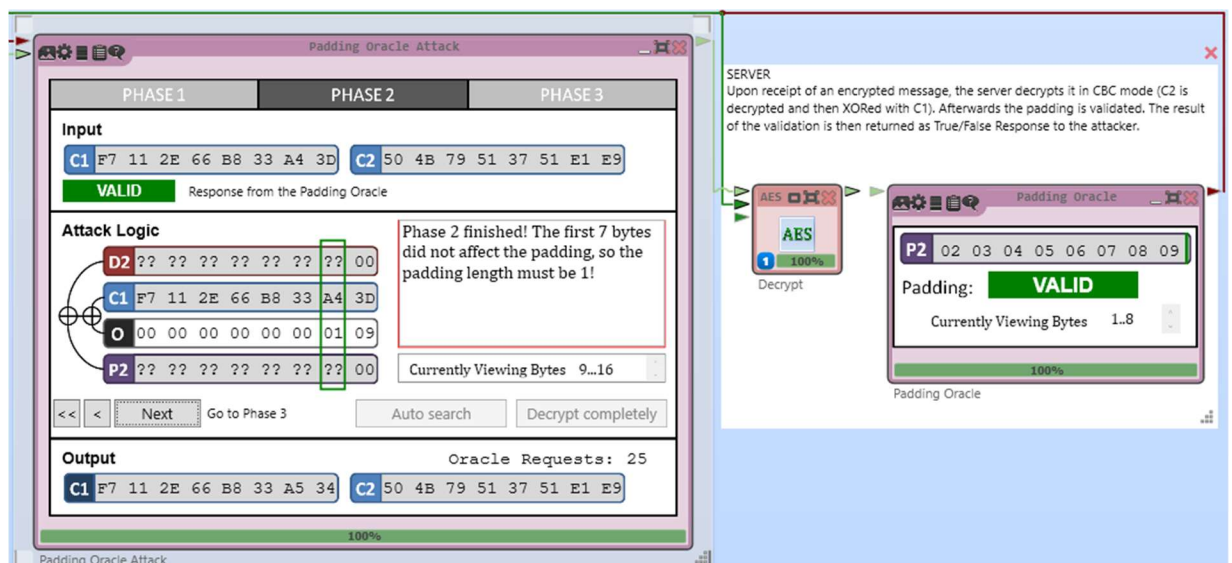
Шаблон атаки предсказанием дополнения на шифр в режиме CBC в Cryptool 2.



## Фаза 1.



## Фаза 2.



**Padding Oracle Attack**

PHASE 1      PHASE 2      PHASE 3

**Input**

C1 A4 07 6D D7 4E DE 31 F7      C2 BC 61 65 65 8B 20 50 50

Response from the Padding Oracle

**Attack Logic**

D2 A7 03 68 D1 49 D6 38 F6  
 C1 A4 07 6D D7 4E DE 31 F7  
 0 00 00 00 00 00 00 00  
 P2 03 04 05 06 07 08 09 01

Plaintext Recovered. Attack completed successfully.

**COMPLETE**

Currently Viewing Bytes 2...9

Output      Oracle Requests: 143

C1 B7 13 78 C1 59 C6 28 E6      C2 BC 61 65 65 8B 20 50 50

100%

**SERVER**

Upon receipt of an encrypted message, the server decrypts it in CBC mode (C2 is decrypted and then XORed with C1). Afterwards the padding is validated. The result of the validation is then returned as True/False Response to the attacker.

**AES**

Decrypt

**Padding Oracle**

P2 10 10 10 10 10 10 10 10

Padding: **VALID**

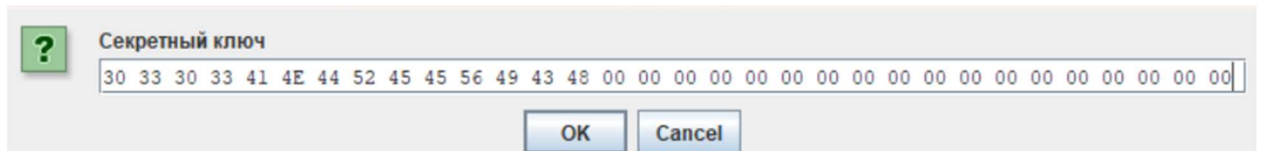
Currently Viewing Bytes 1..8

100%

Padding Oracle

## 2.1 Алгоритм развертывания ключа шифра Кузнечик с помощью приложения ЛИТОРЕЯ

В hex виде: 30 33 30 33 41 4E 44 52 45 45 56 49 43 48 00 00 00 00 00 00 00  
00 00 00 00 00 00 00 00 00 00



Так как зачетная книжка оканчивается на 7, то рассмотрим итерацию 9.

На вход итерации приходят раундовые ключи 3 и 4.



Раундовый ключ 3	Раундовый ключ 4
1C 11 32 E6 D2 BD 28	D9 E9 D0 CA B8 B0 7A
86 80 25 C6 1D 2A 41	4F 9B 3B 6D B7 27 71
B9 2B	95 8F

Ключ 3 принимаем за субблок L, а ключ 4 за субблок R.

Субблок L	Субблок R
1C 11 32 E6 D2 BD 28	D9 E9 D0 CA B8 B0 7A
86 80 25 C6 1D 2A 41	4F 9B 3B 6D B7 27 71
B9 2B	95 8F

Итерационный ключ на 9 итерации равен:

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

Производим XOR L с итерационным ключом.

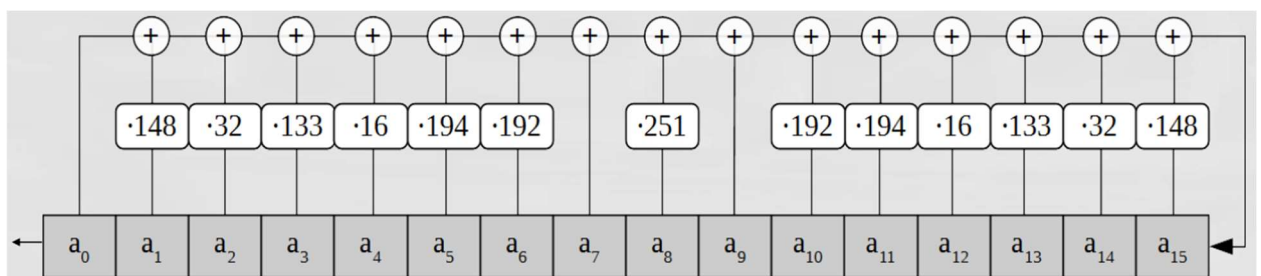
Преобразование: 'сложение  
XOR'  
84 EA 72 82 58 F0 04 B7 70 F9  
DA 8D D0 6F 07 22

Производим подстановку S с помощью таблицы.

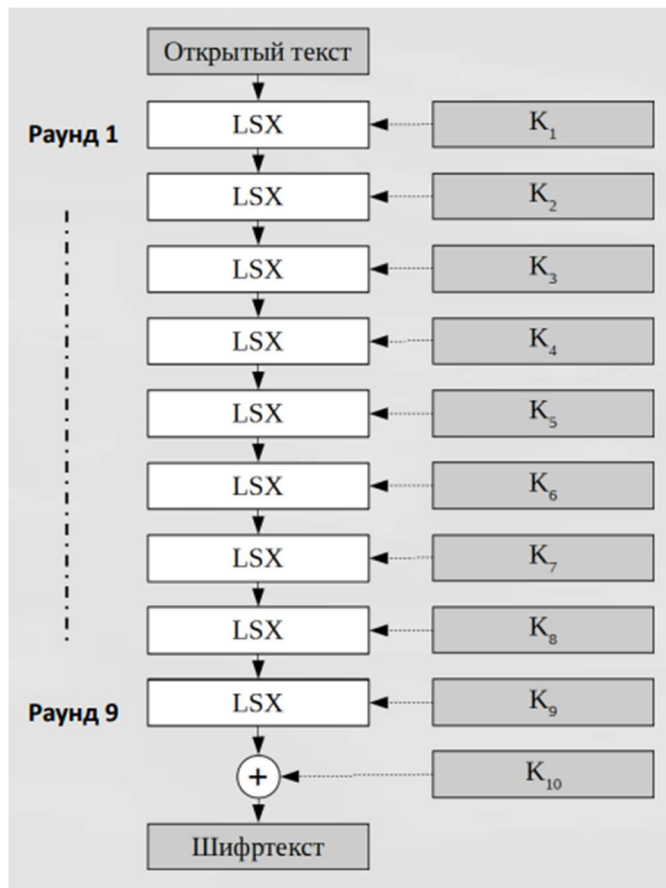
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	252	238	221	17	207	110	49	22	251	196	250	213	35	197	4	77
16	233	119	240	219	147	46	153	186	23	54	241	187	20	205	95	193
32	249	24	101	90	226	92	239	33	129	28	60	66	139	1	142	79
48	5	132	2	174	227	106	143	160	6	11	237	152	127	212	211	31
64	235	52	44	81	234	200	72	171	242	42	104	162	253	58	206	204
80	181	112	14	86	8	12	118	18	191	114	19	71	156	183	93	135
96	21	161	150	41	16	123	154	199	243	145	120	111	157	158	178	177
112	50	117	25	61	255	53	138	126	109	84	198	128	195	189	13	87
128	223	245	36	169	62	168	67	201	215	121	214	246	124	34	185	3
144	224	15	236	222	122	148	176	188	220	232	40	80	78	51	10	74
160	167	151	96	115	30	0	98	68	26	184	56	130	100	159	38	65
176	173	69	70	146	39	94	85	47	140	163	165	125	105	213	149	59
192	7	88	179	64	134	172	29	247	48	55	107	228	136	217	231	137
208	225	27	131	73	76	63	248	254	141	83	170	144	202	216	133	97
224	32	113	103	164	45	43	9	91	203	155	37	208	190	229	108	82
240	89	166	116	210	230	244	180	192	209	102	175	194	57	75	99	182

Преобразование:  
'подстановка S'  
3E 25 19 24 BF 59 CF 2F 32 66  
AA 22 E1 B1 16 65

Производим линейное преобразование L. L представимо в виде регистра сдвига с обратной связью, который движется 16 раз. Регистр реализуется над полем Галуа по модулю неприводимого многочлена  $x^8 + x^7 + x^6 + x + 1$ .



### Схема раундовых преобразований:



Так как зачетная книжка оканчивается на 7, то рассмотрим раунд 9.  
На вход приходит блок данных:

Блок данных: 39 58 8F D2 3A 94 40 9C 67 FA 69 17 3E 5F 5C 6F

Раундовый ключ 9.

Раундовый ключ: C3 14 9C DD CF 86 C9 75 3E 3E 81 1E BA 7C 0F C2

Производим XOR блока данных с раундовым ключом.

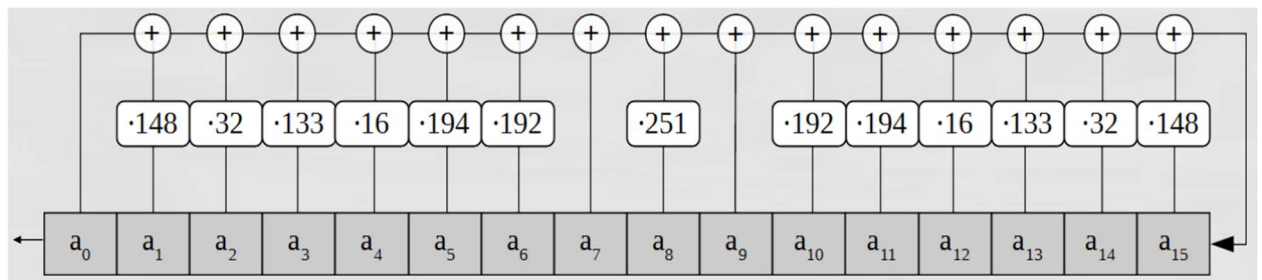
Результат X: FA 4C 13 0F F5 12 89 E9 59 C4 E8 09 84 23 53 AD

Производим подстановку S с помощью таблицы.

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	252	238	221	17	207	110	49	22	251	196	250	213	35	197	4	77
16	233	119	240	219	147	46	153	186	23	54	241	187	20	205	95	193
32	249	24	101	90	226	92	239	33	129	28	60	66	139	1	142	79
48	5	132	2	174	227	106	143	160	6	11	237	152	127	212	211	31
64	235	52	44	81	234	200	72	171	242	42	104	162	253	58	206	204
80	181	112	14	86	8	12	118	18	191	114	19	71	156	183	93	135
96	21	161	150	41	16	123	154	199	243	145	120	111	157	158	178	177
112	50	117	25	61	255	53	138	126	109	84	198	128	195	189	13	87
128	223	245	36	169	62	168	67	201	215	121	214	246	124	34	185	3
144	224	15	236	222	122	148	176	188	220	232	40	80	78	51	10	74
160	167	151	96	115	30	0	98	68	26	184	56	130	100	159	38	65
176	173	69	70	146	39	94	85	47	140	163	165	125	105	213	149	59
192	7	88	179	64	134	172	29	247	48	55	107	228	136	217	231	137
208	225	27	131	73	76	63	248	254	141	83	170	144	202	216	133	97
224	32	113	103	164	45	43	9	91	203	155	37	208	190	229	108	82
240	89	166	116	210	230	244	180	192	209	102	175	194	57	75	99	182

**Результат S: AF FD DB 4D F4 F0 79 9B 72 86 CB C4 3E 5A 56 9F**

Производим линейное преобразование L и получим шифротекст после девятого раунда. L представимо в виде регистра сдвига с обратной связью, который движется 16 раз. Регистр реализуется над полем Галуа по модулю неприводимого многочлена  $x^8 + x^7 + x^6 + x + 1$ .



**Результат L: 9D 20 D3 A8 BF D7 04 24 7F 01 CB DF A8 68 31 7B**



## **Выводы.**

Таким образом, были исследованы шифры AES и Кузнечик.

1. Шифр AES. Симметричный, текст шифруется блоками 128 бит, ключ может быть 128, 192, 256 бит с 10, 12, 14 раундами соответственно, раундовый-128 бит. Содержит операции AddRoundKey, SubBytes, ShiftRows, MixColumns.

1.1 Вручную определен ключ первого раунда, произведен первый раунд зашифровки исходного текста. Произведенные действия совпадают с Cryptool 2.

1.2 Время проведения атаки грубой силы растет экспоненциально, когда известна только часть ключа. Время проведения атаки грубой силы уменьшается с увеличением числа процессоров и отношение времени растет с уменьшением длины известной части ключа. Использование оценочной функции словосочетания из исходного текста уменьшает время атаки грубой силы в сравнении с оценочной функцией энтропии.

1.3 Изучена атака предсказанием дополнения на шифр в режиме CBC. Нарушителю достаточен сервер, который возвращает ответ о правильности дополнения последнего блока.

## **2. Шифр Кузнечик.**

2.1 Ключ 256 бит. По алгоритму расширения ключа из исходного ключа получается 10 раундовых ключей по 128 бит. Первые два ключа получаются разбиением на две равные части исходного. Каждые последующие пары ключей получаются последовательным преобразованием пары субблоков через восемь итераций сети Фейстеля. В итерации используется итерационный ключ, который получается в результате линейного преобразования порядкового номера. Получены промежуточные субблоки девятой итерации.

2.2 Шифр симметричный, текст шифруется блоками 128 бит. Раундовые преобразования представляют собой SP-сеть с набором преобразований L, S, X. Количество раундов – 9, десятый ключ используется в операции XOR с результатом девяти раундов. Выполнен девятый раунд шифрования.

## ПРИЛОЖЕНИЕ А

### ЗАМЕЧАНИЯ К ПРОГРАММЕ ЛИТОРЕЯ

1. Проблемы с отрисовкой в визуализации развертывания ключей:  
наслаивание, обновление субблоков на вход раньше конца итерации,  
отсутствие очистки результатов с предыдущих итераций.

<b>Секретный ключ:</b> 30 33 30 33 41 4E 44 52 45 45 56 49 43 48 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		
<b>Раундовый ключ 3</b> D5 58 11 AE 76 41 1F BC 04 10 11 24 98 99 67 12	<b>Раундовый ключ 4</b> 15 AB AA BE FA FA B4 42 86 EE 6D 5B A5 D3 9F F1	
<b>Субблок L</b> 15 AB AA BE FA FA B4 42 86 EE 6D 5B A5 D3 9F F1	<b>Субблок R</b> 5C 8D 8B 62 76 B7 20 C8 33 E9 46 EA 46 30 23 F4	
		<b>Формирование ключа итерации:</b> 98 FB 40 64 8A 4D 2C 31 F0 0C 1C 90 FA 2F BF 09
		<b>Преобразование: 'сложение XOR'</b> 84 EA 72 82 58 F0 04 B7 70 F9 0A 80 00 6F 07 22
		<b>Преобразование: 'подстановка S'</b> 3E 25 19 24 BF 59 CF 2F 32 66 AA 22 F1 B1 16 65
		<b>Преобразование: 'регистр сдвига L'</b> D9 E9 D0 CA B8 B0 7A 4F 9B 3B 6D B7 27 71 95 8F
		<b>Преобразование: 'сложение XOR'</b> 5C 8D 8B 62 76 B7 20 C8 33 F9 46 FA 46 30 23 F4
<b>Субблок L'</b> 15 AB AA BE FA FA B4 42 86 EE 6D 5B A5 D3 9E F1	<b>Субблок R'</b> 5C 8D 8B 62 76 B7 20 C8 33 E9 46 EA 46 30 23 E4	
<b>Субблок L'</b> 15 AB AA BE FA FA B4 42 86 EE 6D 5B A5 D3 9F F1		

<b>Секретный ключ:</b> 30 33 30 33 41 4E 44 52 45 45 56 49 43 48 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00			№ итерации развертывания ключа 10
<b>Раундовый ключ 3</b> 1C 11 32 E6 D2 BD 28 86 80 25 C6 1D 2A 41 B9 2B	<b>Раундовый ключ 4</b> D9 E9 D0 CA B8 B0 7A 4F 9B 3B 6D B7 27 71 95 8F		
<b>Субблок L</b> D9 E9 D0 CA B8 B0 7A 4F 9B 3B 6D B7 27 71 95 8F	<b>Субблок R</b> 5C 8D 8B 62 76 B7 20 C8 33 E9 46 EA 46 30 23 E4		
		<b>Формирование ключа итерации:</b> 2A DE DA F2 3E 95 A2 3A 17 B5 18 A0 5E 61 C1 0A	
		<b>Преобразование: 'сложение XOR'</b> 76 53 51 90 48 22 82 F2 24 5C 5E 4A 18 51 E2 EE	
		<b>Преобразование: 'подстановка S'</b> 8A 56 70 E0 F2 65 24 74 E2 9C 5D 68 17 70 67 6C	
		<b>Преобразование: 'регистр сдвига L'</b> D9 E9 D0 CA B8 B0 7A 4F 9B 3B 6D B7 27 71 95 8F	
		<b>Преобразование: 'сложение XOR'</b> 5C 8D 8B 62 76 B7 20 C8 33 E9 46 EA 46 30 23 E4	

<b>Секретный ключ:</b> 30 33 30 33 41 4E 44 52 45 45 56 49 43 48 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		№ итерации развертывания ключа 11
<b>Раундовый ключ 3</b> 1C 11 32 E6 D2 BD 28 86 80 25 C6 1D 2A 41 B9 2B	<b>Раундовый ключ 4</b> D9 E9 D0 CA B8 B0 7A 4F 9B 3B 6D B7 27 71 95 8F	
<b>Субблок L</b> 5C 8D 8B 62 76 B7 20 C8 33 E9 46 EA 46 30 23 E4	<b>Субблок R</b> BE 19 58 4C B8 10 43 9B 5D C8 5E E0 A8 2F 09 6A	
		<b>Формирование ключа итерации:</b> 2A DE DA F2 3E 95 A2 3A 17 B5 18 A0 5E 61 C1 0A
		<b>Преобразование:</b> 'сложение XOR' 76 53 51 90 48 22 82 F2 24 5C 5E 4A 18 51 E2 EE
		<b>Преобразование:</b> 'подстановка S' 8A 56 70 E0 F2 65 24 74 E2 9C 5D 68 17 70 67 6C
		<b>Преобразование: 'регистр сдвига L'</b> 1C 11 32 E6 D2 BD 28 86 80 25 C6 1D 2A 41 B9 2B
		<b>Преобразование:</b> 'сложение XOR' BE 19 58 4C B8 10 43 9B 5D C8 5E E0 A8 2F 09 6A

2. Некорректное отображение сдвига в развертывании ключа.