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

ОТЧЕТ

По лабораторной работе № 5
по дисциплине «Криптография и защита информации»
Тема: Исследование шифров AES, Кузнечик

Студент гр. 0303 _____ Болкунов В.О.

Преподаватель _____ Племянников А. К.

Санкт-Петербург
2023

Цель работы.

Цель работы: исследовать шифры AES и Кузнечик; получить практические навыки работы с ними, с использованием приложений Cryptool 1/2 и Литорея.

Порядок выполнения работы.

1. Изучить преобразования AES по шаблонной схеме AES Visualisation из CrypTool 2 с учетом рекомендаций Методического пособия
2. Провести исследование криптостойкости AES с учетом рекомендаций Методического пособия
3. Изучить действия нарушителя при атаке предсказанием дополнения на шифр в режиме CBC с учетом рекомендаций Методического пособия
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.
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

В качестве шифруемого сообщения была выбрана последовательность байт, соответствующая строке “*bolkunov_vlad*”:

M = 62 6F 6C 6B 75 6E 6F 76 5F 76 6C 61 64 00 00 00

В качестве же ключа шифрования была выбрана последовательность

K = 30 33 30 33 30 34 5F 6F 6C 65 67 6F 76 69 63 68, что соответствует строке “030304_olegovich”

1.1. Ручные вычисления

Для генерации ключа первого раунда и выполнения первого раунда шифрования была написана программа на языке Python 3 с использованием библиотеки NumPy, полная версия программы представлена в приложении А.

1.1.1. Раунд расширения ключа

В листинге 1 представлен фрагмент расширения ключа первого раунда.

Листинг 1. Формирование ключа первого раунда

```
# Берём последнюю 'колонку' (в нашем случае строка)
t = K[-1].copy()
# Сдвигаем циклически элементы (первый в конец)
t = np.roll(t, -1)
# Примеянем SubByte
t = np.array(list(
    map(
        lambda x: Sbox[x >> 4][x & 0x0f],
        t
    )
))
# Применяем xor с константой раунда
t = t ^ np.array([0x01, 0x00, 0x00, 0x00])
# Формируем раундовый ключ (t4 xor W0 xor W1 ...)
K1 = []
for col in K:
    t = col ^ t
    K1.append(t)

# Преобразуем к матрице numpy
K1 = np.array(K1)
```

В результате выполнения данного фрагмента получились следующие выходные данные (листинг 2):

Листинг 2. Результат генерации ключа

```
---Генерация ключа---

Последние 4 байта ключа (t4): [0x76 0x69 0x63 0x68]
t4 после RotWord: [0x69 0x63 0x68 0x76]
t4 после SubWord: [0xf9 0xfb 0x45 0x38]
t4 после Rcon(1): [0xf8 0xfb 0x45 0x38]
Итоговая матрица состояний ключа в первом раунде:
```

```
[[0xc8 0xf8 0x94 0xe2]
 [0xc8 0xfc 0x99 0xf0]
 [0x75 0x2a 0x4d 0x2e]
 [0xb 0x64 0xb 0x63]]
```

Итого ключ для первого раунда будет следующим:

K_1 = C8 C8 75 0B F8 FC 2A 64 94 99 4D 0B E2 F0 2E 63

1.1.2 Раунд шифрования

Проведём шифрование первого раунда с помощью полученного ключа, фрагмент программы в котором производится шифрование представлен в листинге 3.

Листинг 3. Шифрование на первом раунде

```
# Начальный раунд (xor сообщения с начальным ключом
E = M ^ K

# Замена S-box блоками (SubBytes)
E = np.array(list(
    map(
        lambda col: list(
            map(
                lambda x: Sbox[x >> 4][x & 0x0f],
                col
            )
        ),
        E
    )
))

# Осуществляем циклический сдвиг строк (т.к. у нас это столбцы
выполняем дополнительно транспонирование)
nE = []
for i in range(E.shape[0]):
    nE.append(np.roll(E.T[i], -i))

# Обновялем матрицу состоянии
E = np.array(nE).T

# Умножение байт в поле GF(256)
def g_mul(a, b): ... # См. приложение А

# Умножение на матрицу констант
nE = []
for i in range(E.shape[0]):
```

```
    col = []
    for j in range(C.shape[1]):
        p = 0
        for k in range(E.shape[1]):
            p ^= g_mul(E[i][k], C[k][j])
        col.append(p)
    nE.append(np.array(col))

E = np.array(nE).T

# Добавляем раундовый ключ
E = E.T ^ K1
```

В результате выполнения данной части программы были получены следующие выходные данные (листинг 4):

Листинг 4. Результаты шифрования на первом раунде

```
---Шифрование---

Матрица состояний сообщений после начального раунда (xor с
ключом):
[[0x52 0x45 0x33 0x12]
 [0x5c 0x5a 0x13 0x69]
 [0x5c 0x30 0xb 0x63]
 [0x58 0x19 0xe 0x68]]

Матрица состояний после SubBytes:
[[0x0 0x6e 0xc3 0xc9]
 [0x4a 0xbe 0x7d 0xf9]
 [0x4a 0x4 0x2b 0xfb]
 [0x6a 0xd4 0xab 0x45]]

Матрица состояний после ShiftRows:
[[0x0 0x6e 0xc3 0xc9]
 [0xbe 0x7d 0xf9 0x4a]
 [0x2b 0xfb 0x4a 0x4]
 [0x45 0x6a 0xd4 0xab]]

Матрица состояний после MixColumns:
[[0xb7 0x5f 0x27 0x1f]
 [0xca 0xe8 0x40 0xe0]
 [0x13 0x20 0xc9 0x5e]
 [0xf8 0xfa 0x6d 0x43]]

Матрица состояний после AddKey:
[[0x7f 0x32 0x87 0x1a]
 [0x97 0x14 0xb9 0xa]
 [0x52 0x6a 0x84 0x43]
 [0x14 0x84 0x55 0x20]]
```

Итого в результате выполнения первого раунда получаем следующую последовательность байт:

E_1 = 7F 97 52 14 32 14 6A 84 87 B9 84 55 1A 0A 43 20

1.2 Работа AES Visualizer в CrypTool 2

Проверим работу шифра AES в схеме AES Visualize в приложении CrypTool2.

1.2.2. Раунд расширения ключа

Схема шифрования AES изображена на рисунке 1.

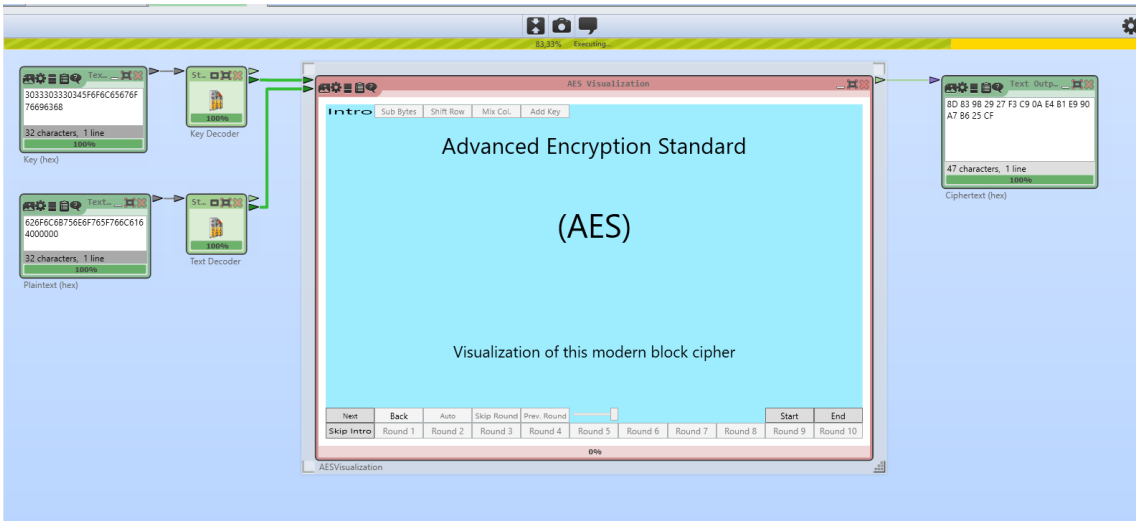

Рисунок 1: Схема AES Visualizer

Рассмотрим процесс расширения ключа первого раунда. На рисунке 2 изображена процедура RotWord. На рисунке 3 изображён результат применения процедуры SubWord – замена каждого байта процедурой SubByte по соответствующей S-Box таблице. На рисунке 4 – применение процедуры RCon(i). Далее на рисунке 5 – формируется ключ для первого раунда путём последовательного применения ***xor*** к полученному столбцу столбцов начального ключа.

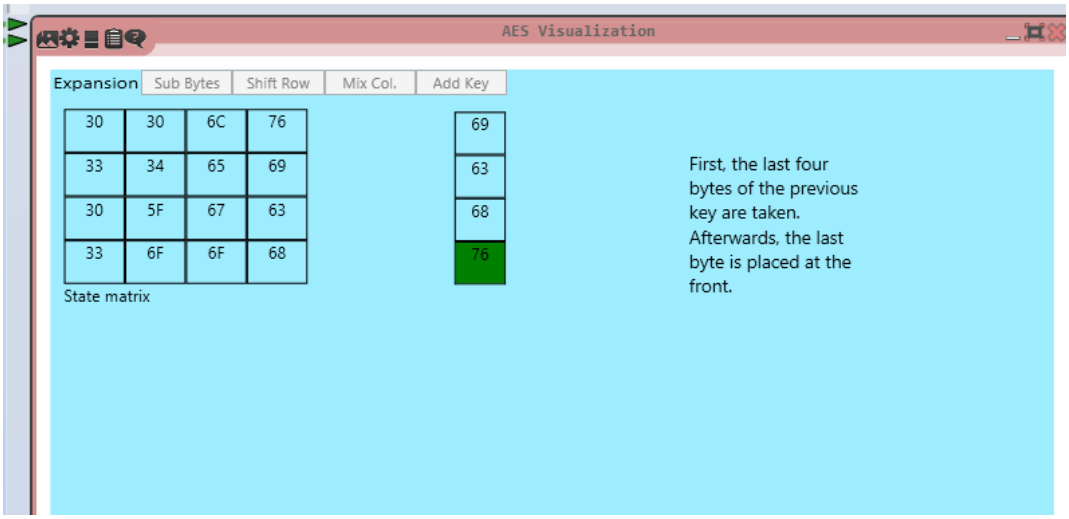

Рисунок 2: RotWord

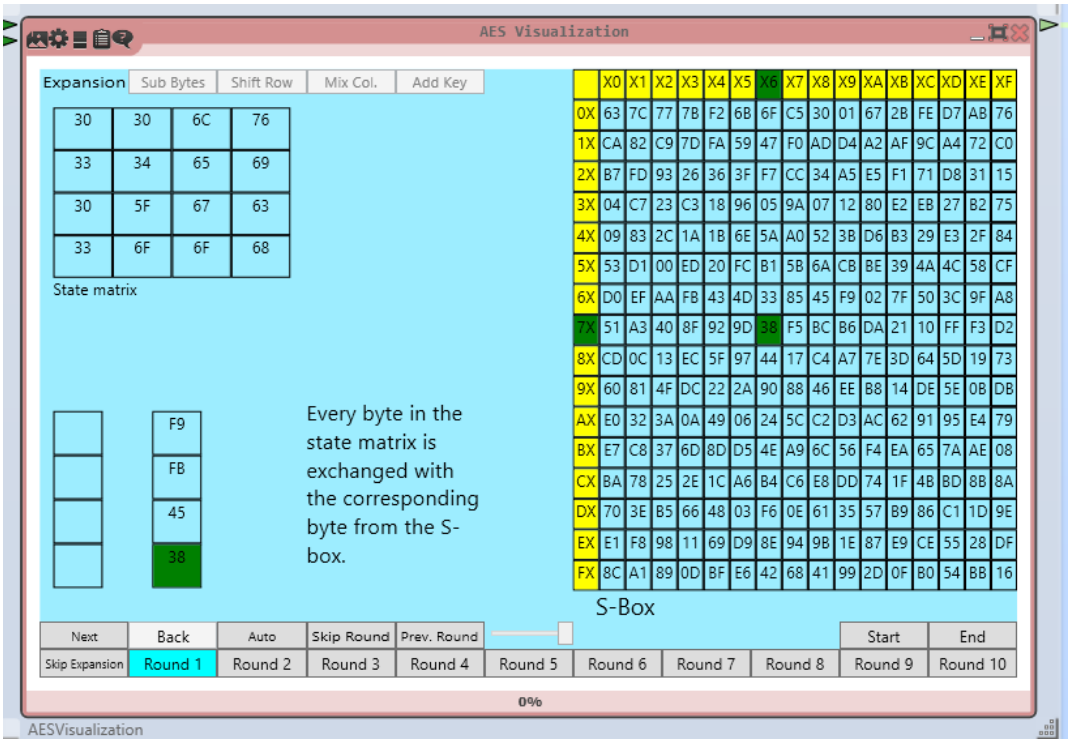

Рисунок 3: SubWord

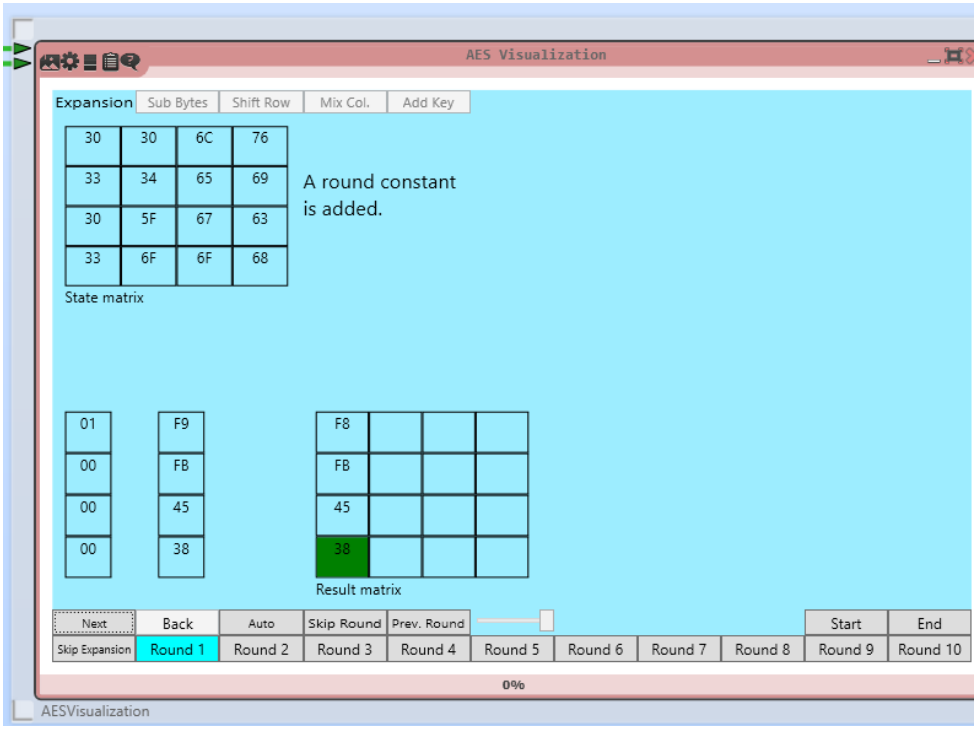

Рисунок 4: RCon(i)

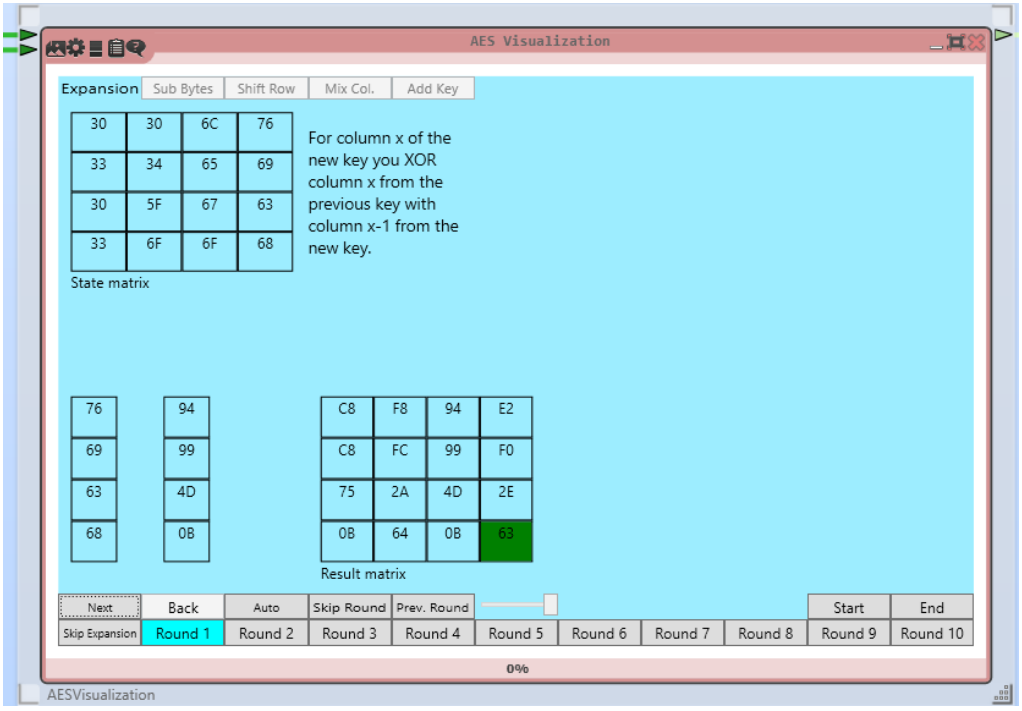

Рисунок 5: Ключ первого раунда

В результате получился следующий раундовый ключ:

K_1 = C8 C8 75 0B F8 FC 2A 64 94 99 4D 0B E2 F0 2E 63, что полностью совпадает с произведёнными вычислениями

1.2.2 Раунд шифрования

На рисунке 6 показан начальный раунд, в котором исходное сообщение суммируется операцией ***xor*** с исходным ключом.

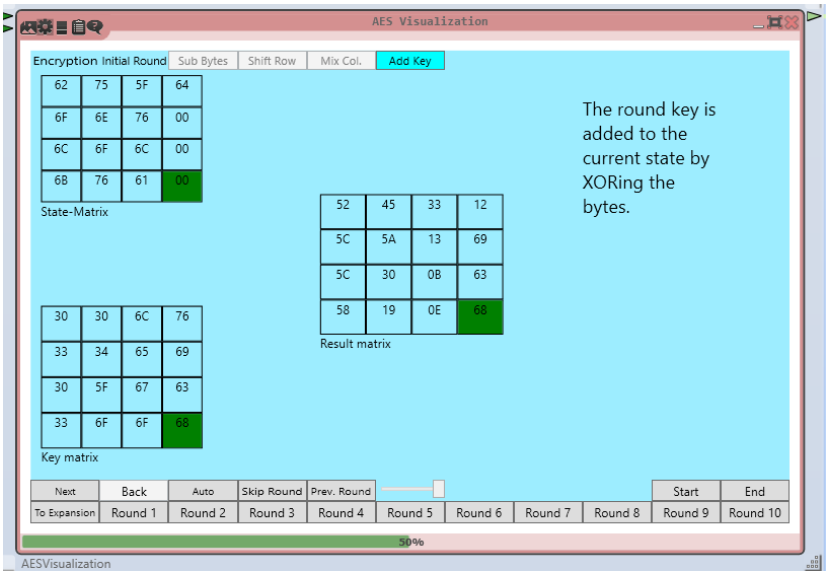

Рисунок 6: начальный раунд

На рисунке 7 изображено применение блока замены SubBytes.

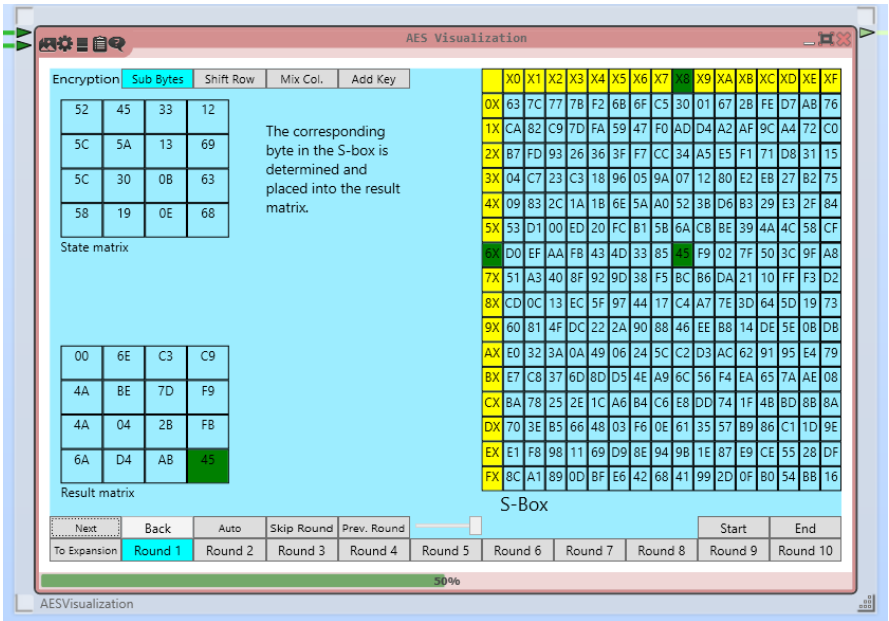

Рисунок 7: применение SubBytes

На рисунке 8 изображено применение процедуры сдвига рядов матрицы состояний (ShiftRow).

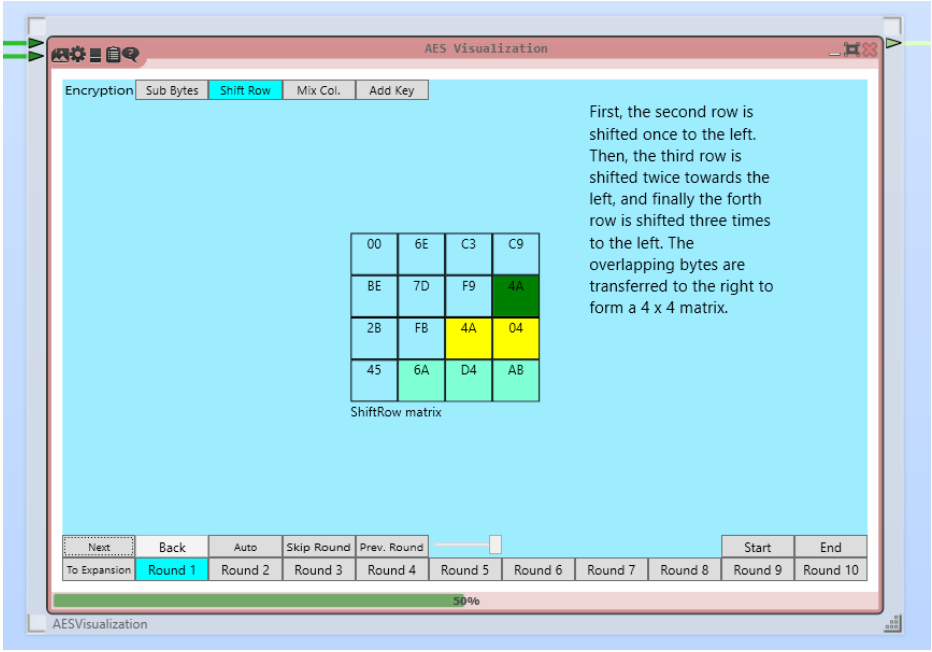

Рисунок 8: Применение ShiftRow

На рисунке 9 показана работа преобразования смешивания (Mix Columns)

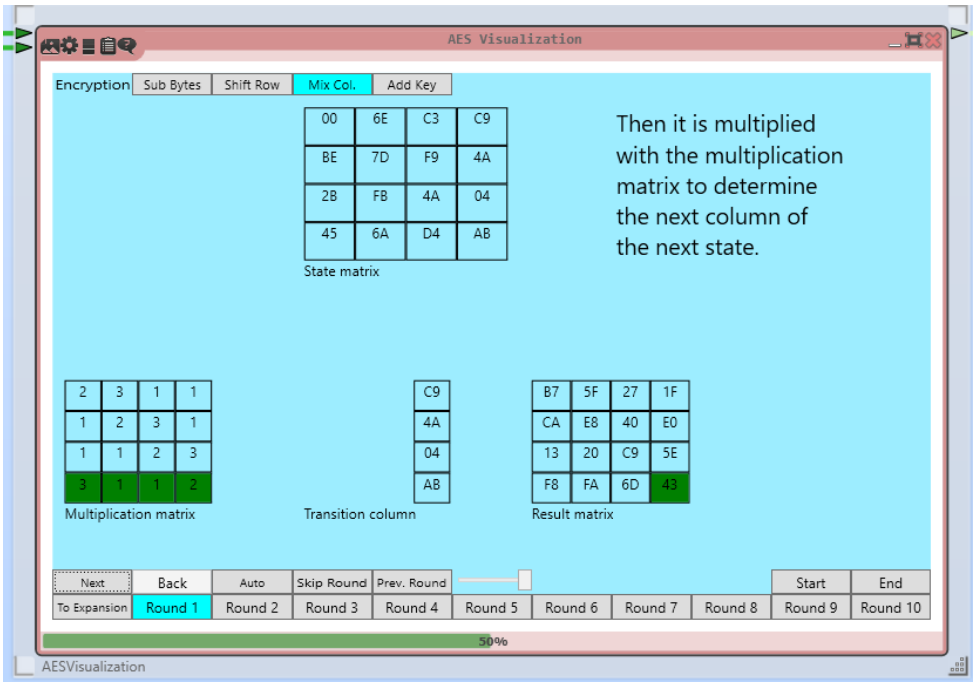

Рисунок 9: Применение MixColumns

На рисунке 10 изображено добавление раундового ключа операцией ***xor*** к матрице состояний.

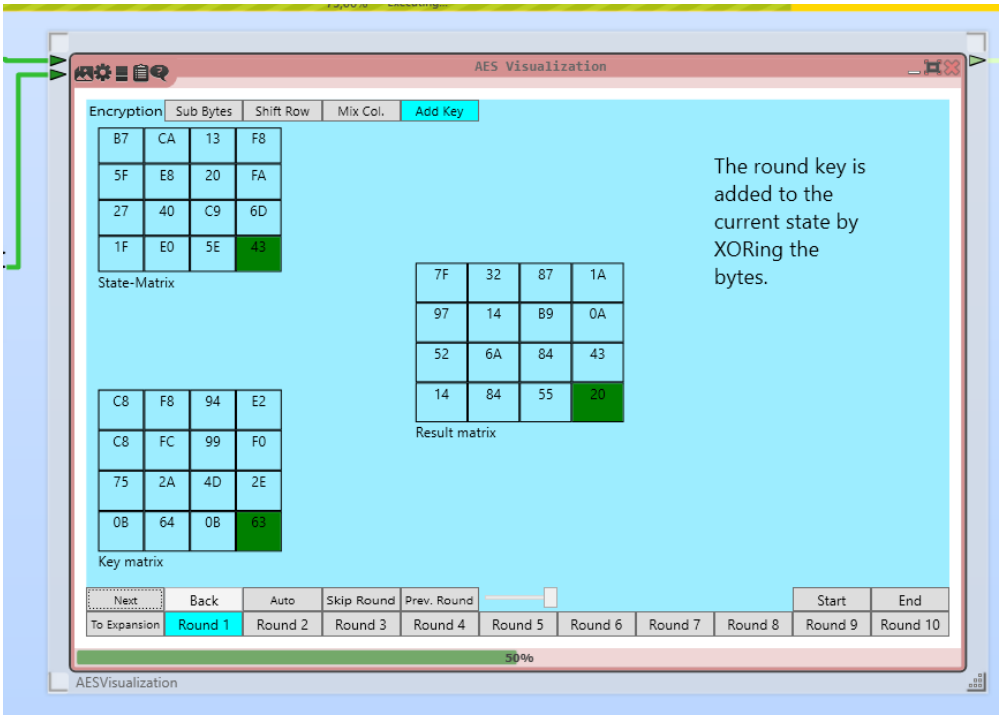

Рисунок 10: Применение AddKey

Итого в результате выполнения первого раунда CrypTool получил следующую последовательность байт:

E_1 = 7F 97 52 14 32 14 6A 84 87 B9 84 55 1A 0A 43 20 , что полностью соответствует вычисленному ранее значению.

2. Криптостойкость AES

С помощью схемы AES KeySearcher (рис. 11) была проведена оценка времени атаки грубой силы для произвольного сообщения для 1, 6 и 12 ядер и для разного количества известных байтов ключа. Результаты представлены в таблице 1.

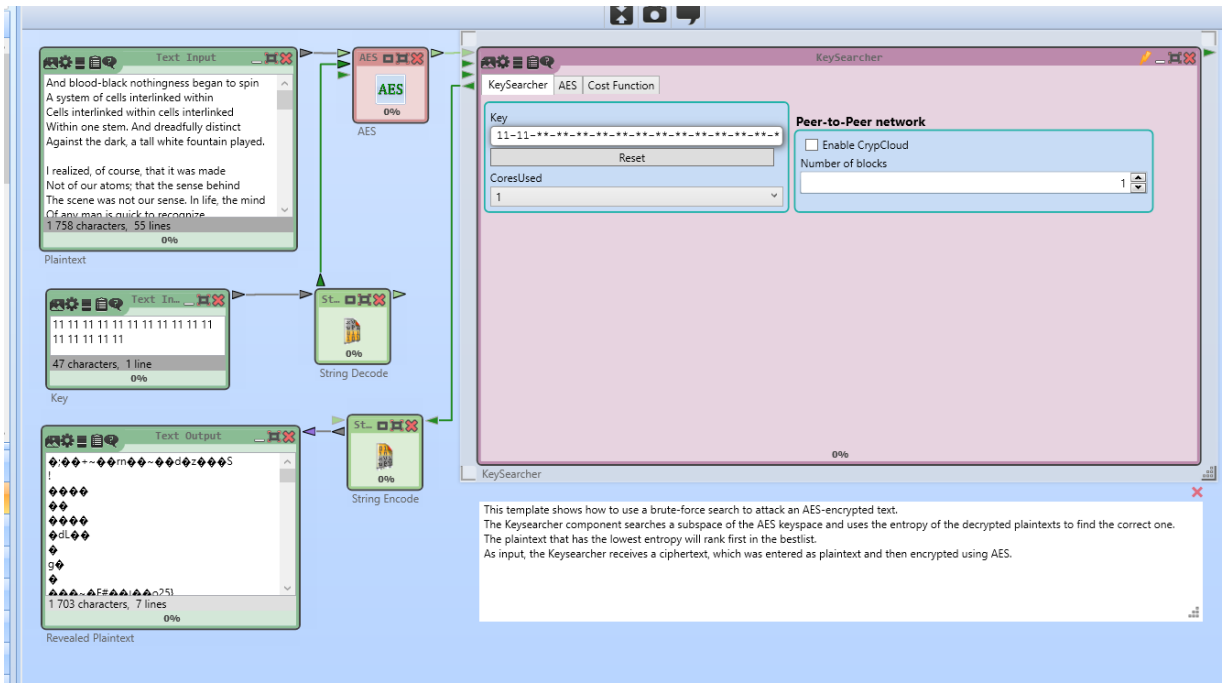

Рисунок 11: атака грубой силы на AES

Таблица 1: атака грубой силы на AES

N известных байт	Количество ядер		
	1	**6**	**12**
14	< 1 секунды	< 1 секунды	< 1 секунды
12	~ 2 часа	~ 20 минут	~ 12 минут
10	~ 5000 дней	~ 1000 дней	~ 600 дней

Аналогичная оценка проведена для сообщения с известной частью в формате “***DEAR SIRS.*THANKS!***”. Результаты атаки представлены в таблице 2.

Таблица 2: атака грубой силы на AES с известной частью сообщения

N известных байт	Количество ядер		
	1	**6**	**12**
14	< 1 секунды	< 1 секунды	< 1 секунды
12	~ 1 час	~ 13 минут	~ 9 минут
10	~ 3100 дней	~ 650 дней	~ 410 дней

3. Атака с предсказанием дополнения на AES

Для атаки с предсказанием дополнения было выбрано следующее сообщение (рис. 12):

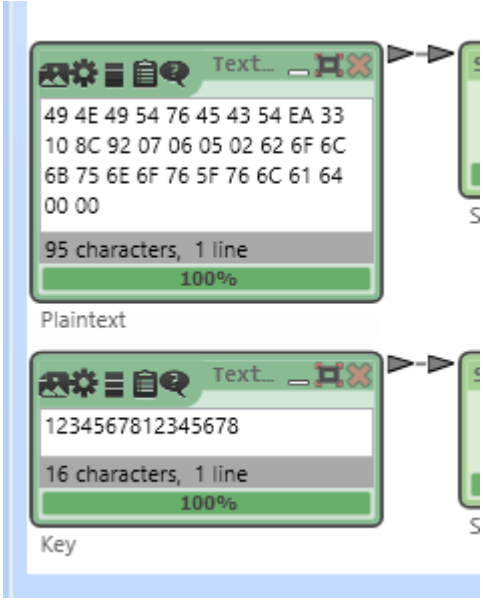

Рисунок 12: исходные данные

Во втором блоке (начиная с байтов 62 6F 6C 6B…) находится информация, которую требуется расшифровать.

На рисунках 13-16 представлены фазы работы атаки.

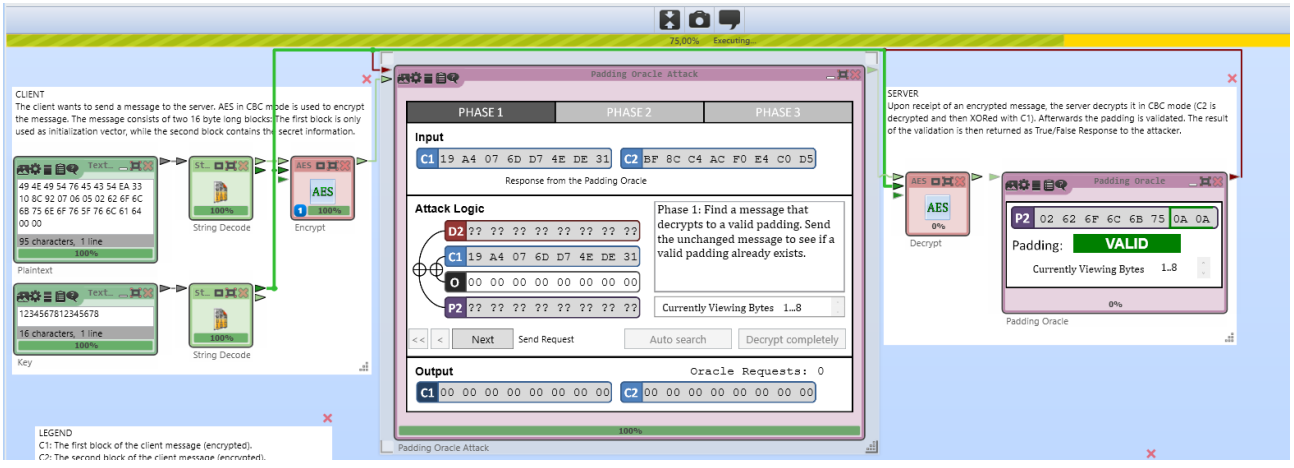

Рисунок 13: отправка исходного сообщения

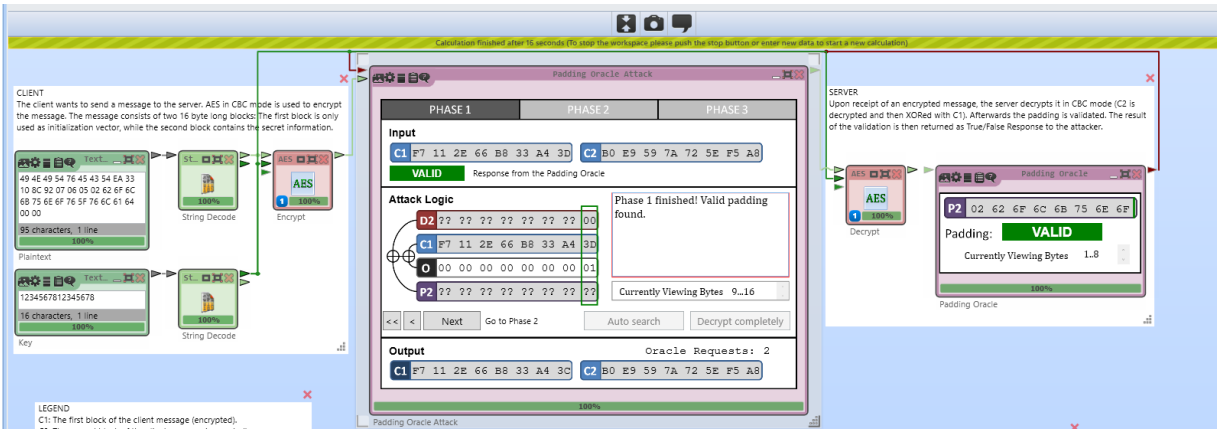

Рисунок 14: дополнение найдено

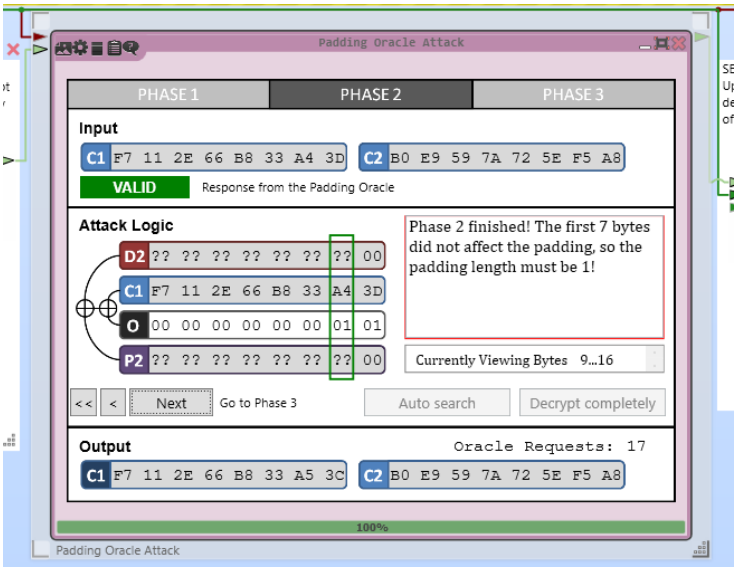

Рисунок 15: найдена длина дополнения

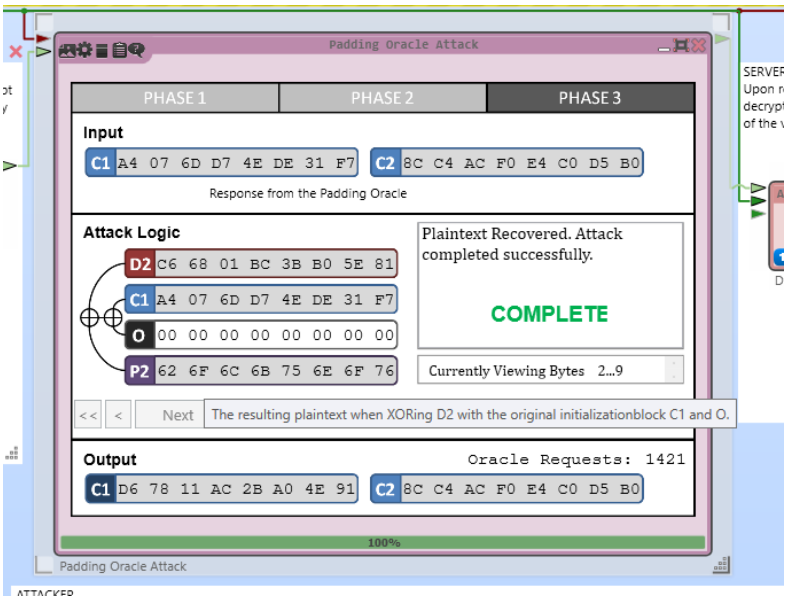

Рисунок 16: фрагмент сообщения расшифрован

Как можно заметить в P2 находится часть исходного текста, что говорит об успешной атаке.

4. Развёртывание ключа шифра Кузнечик

С помощью программы Литорея были проведены итерации развёртывания ключа в шифре Кузнечик.

Был выбран следующий ключ:

K = 0x30 0x33 0x30 0x33 0x30 0x34 0x5f 0x6f 0x6c 0x65 0x67 0x6f 0x76 0x69 0x63 0x68 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0

На рисунках 17 и 18 представлены 1 и 6 итерация развёртывания ключа.

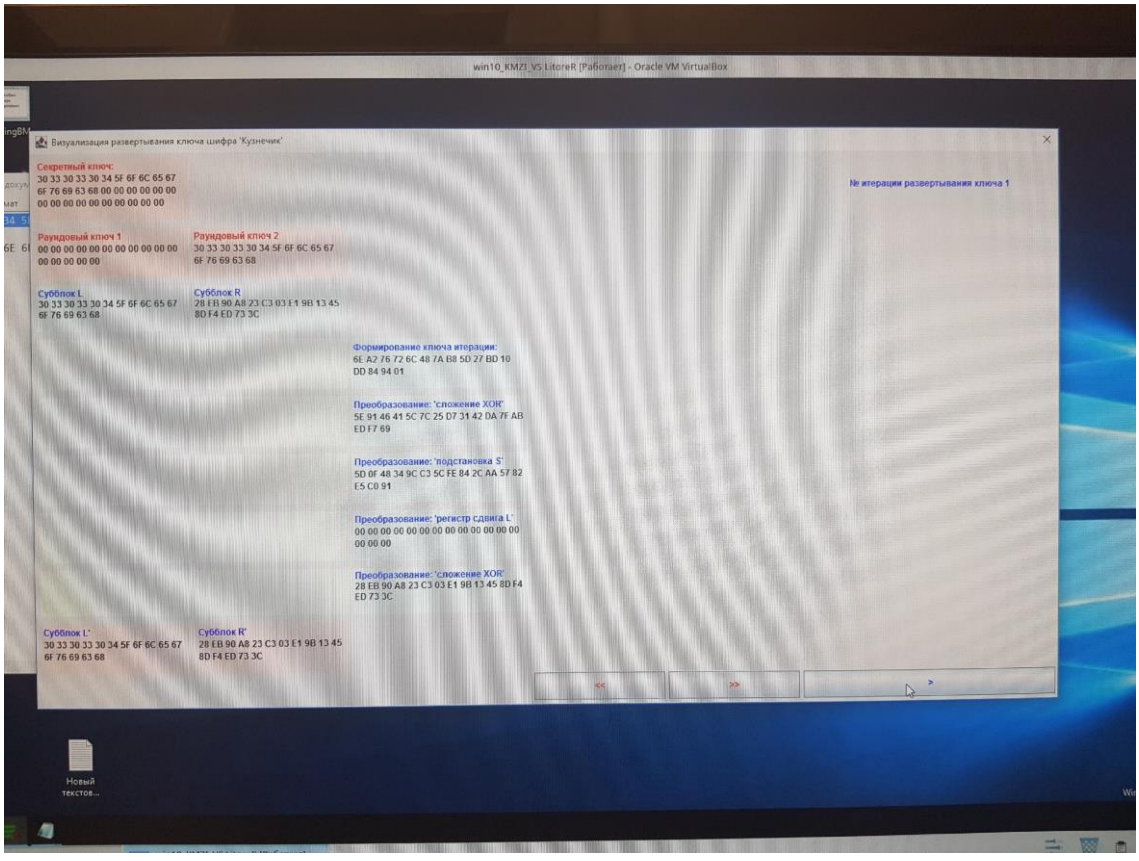

Рисунок 17: 1-ая итерация развёртывания ключа

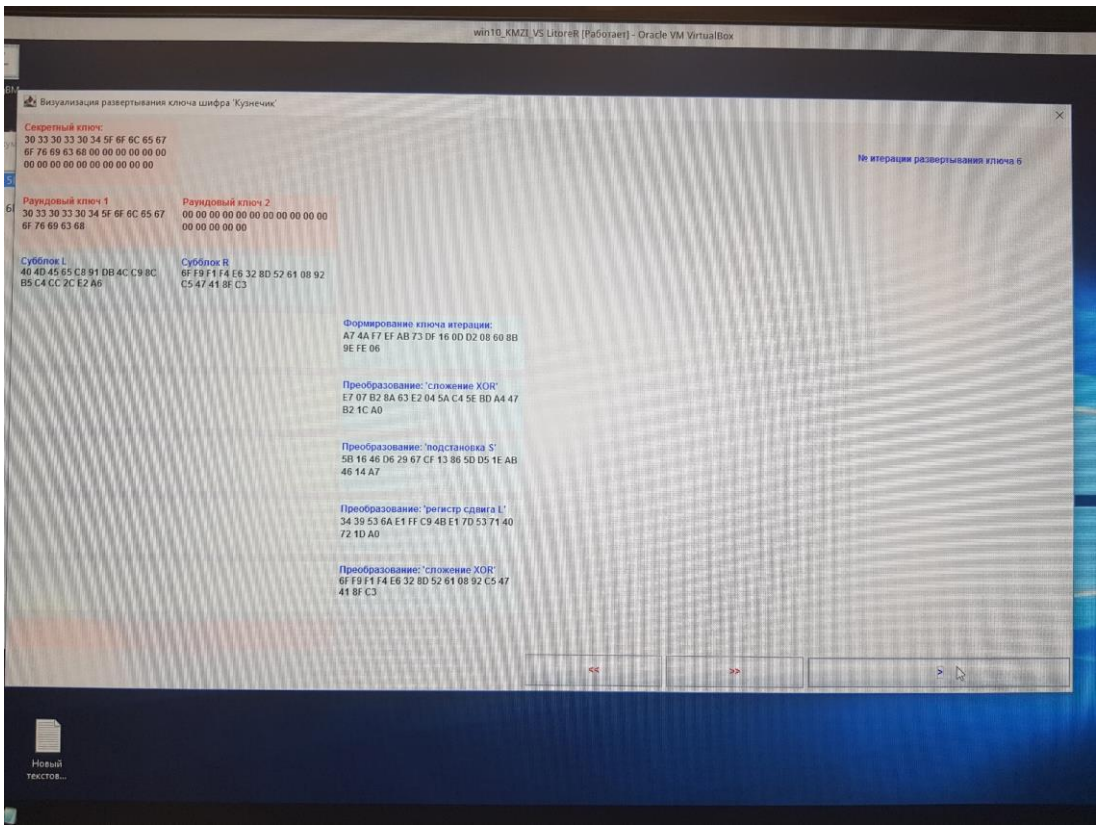

Рисунок 18: 6-ая итерация развёртывания ключа

Для проверки вычислений была написана программа, полная версия которой представлена в приложении Б. В листинге 5 представлен фрагмент вычисления раундовых ключей.

Листинг 5. Вычисление раундовых ключей

```
for i in range(4):
    # Берём два последних раундовых ключа
    k1, k2 = K[-2], K[-1]

    for j in range(8):
        # Сохраняем K1 для замены им K2
        _k1 = k1
        # Константа итерации
        c = C[i * 8 + j]
        # Xor с константой
        k1 = k1 ^ c
        # S блок (k1)
        k1 = np.array(list(map(lambda x: S[x >> 4][x & 0x0f],
k1)))
        # L блок (k1)
        k1 = L(k1)
        # Xor k1 и k2
        k1 = k1 ^ k2
        # Меняем k2 на k1
```

```
        k2 = _k1

    # Добавляем раундовые ключи
    K += [k1, k2]
```

Результаты выполнения программы вместе с шифрованием представлены в приложении В. В листинге 6 представлены результаты вычислений для 1ой и 6 итерации.

Листинг 6. Результаты итераций

```
---Итерация 1---
        C1 = [0x6e 0xa2 0x76 0x72 0x6c 0x48 0x7a 0xb8 0x5d 0x27 0xbd 0x10 0xdd 0x84 0x94
0x1]
        K3 xor c = [0x5e 0x91 0x46 0x41 0x5c 0x7c 0x25 0xd7 0x31 0x42 0xda 0x7f 0xab 0xed
0xf7 0x69]
        S(K3) = [0x5d 0xf 0x48 0x34 0x9c 0xc3 0x5c 0xfe 0x84 0x2c 0xaa 0x57 0x82 0xe5 0xc0
0x91]
        L(K3) = [0x28 0xeb 0x90 0xa8 0x23 0xc3 0x3 0xe1 0x9b 0x13 0x45 0x8d 0xf4 0xed 0x73
0x3c]
        K3 xor K4 = [0x28 0xeb 0x90 0xa8 0x23 0xc3 0x3 0xe1 0x9b 0x13 0x45 0x8d 0xf4 0xed
0x73 0x3c]
        K3 = [0x28 0xeb 0x90 0xa8 0x23 0xc3 0x3 0xe1 0x9b 0x13 0x45 0x8d 0xf4 0xed 0x73
0x3c]
        K4 = [0x30 0x33 0x30 0x33 0x30 0x34 0x5f 0x6f 0x6c 0x65 0x67 0x6f 0x76 0x69 0x63
0x68]
        ---Конец итерации---
…
---Итерация 6---
        C6 = [0xa7 0x4a 0xf7 0xef 0xab 0x73 0xdf 0x16 0xd 0xd2 0x8 0x60 0x8b 0x9e 0xfe 0x6]
        K3 xor c = [0xe7 0x7 0xb2 0x8a 0x63 0xe2 0x4 0x5a 0xc4 0x5e 0xbd 0xa4 0x47 0xb2 0x1c
0xa0]
        S(K3) = [0x5b 0x16 0x46 0xd6 0x29 0x67 0xcf 0x13 0x86 0x5d 0xd5 0x1e 0xab 0x46 0x14
0xa7]
        L(K3) = [0x5b 0xc0 0xa2 0x9e 0x7 0xcd 0x44 0x19 0x80 0x75 0xc1 0xb4 0x7 0x33 0x92
0x63]
        K3 xor K4 = [0x6f 0xf9 0xf1 0xf4 0xe6 0x32 0x8d 0x52 0x61 0x8 0x92 0xc5 0x47 0x41
0x8f 0xc3]
        K3 = [0x6f 0xf9 0xf1 0xf4 0xe6 0x32 0x8d 0x52 0x61 0x8 0x92 0xc5 0x47 0x41 0x8f 0xc3]
;
        K4 = [0x40 0x4d 0x45 0x65 0xc8 0x91 0xdb 0x4c 0xc9 0x8c 0xb5 0xc4 0xcc 0x2c 0xe2
0xa6]
        ---Конец итерации---
```

Можно заметить, что полученные значения в процессе вычисления совпадают* со значениями, полученными в программе Литорея.

5. Раундовые преобразования шифра Кузнечик

С помощью программы Литорея были проведены итерации развёртывания ключа в шифре Кузнечик.

Был выбран следующий ключ:

K = 0x30 0x33 0x30 0x33 0x30 0x34 0x5f 0x6f 0x6c 0x65 0x67 0x6f 0x76 0x69 0x63 0x68 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0

И блок:

M = 0x62 0x6f 0x6c 0x6b 0x75 0x6e 0x6f 0x76 0x5f 0x76 0x6c 0x61 0x64 0x0 0x0 0x0

На рисунках 19 и 20 представлены 1 и 6 раунды шифрования.

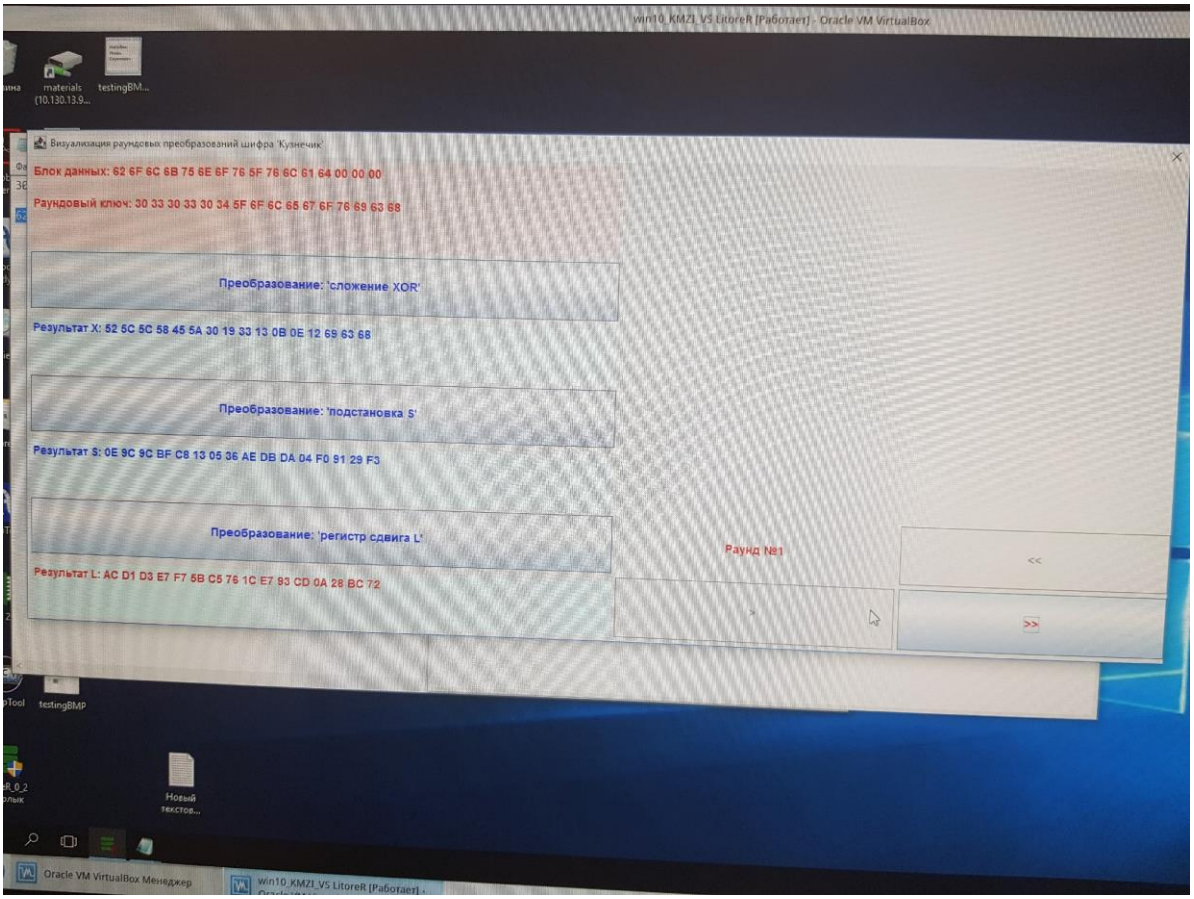

Рисунок 19: 1-ый раунд шифрования

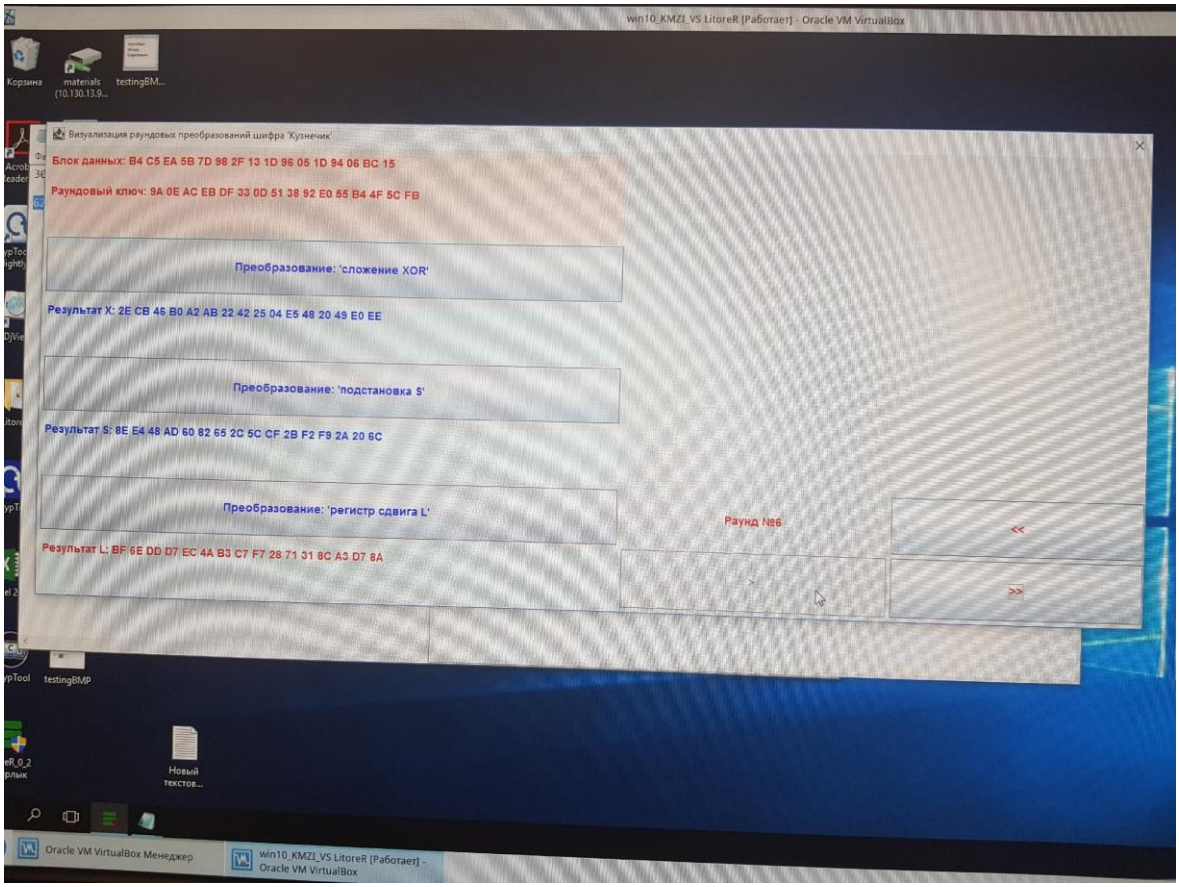

Рисунок 20: 6-ой раунд шифрования

Для проверки вычислений была написана программа, полная версия которой представлена в приложении Б. В листинге 7 представлен фрагмент вычисления шифрования блока сообщения.

Листинг 7. Вычисление раундовых ключей

```
for i in range(10):
    # Xor с раундовым ключом
    M = M ^ K[i]
    # S блок
    M = np.array(list(map(lambda x: S[x >> 4][x & 0x0f], M)))
    # L блок
    M = L(M)
```

Результаты выполнения программы вместе с шифрованием представлены в приложении В. В листинге 8 представлены результаты вычислений для 1ого и 6-го раунда.

Листинг 8. Результаты раундов

```
---Раунд 1---
M xor K1 = [0x52 0x5c 0x5c 0x58 0x45 0x5a 0x30 0x19 0x33 0x13 0xb 0xe 0x12 0x69 0x63
0x68]
S(M) = [0xe 0x9c 0x9c 0xbf 0xc8 0x13 0x5 0x36 0xae 0xdb 0xda 0x4 0xf0 0x91 0x29 0xf3]
L(M) = [0xac 0xd1 0xd3 0xe7 0xf7 0x5b 0xc5 0x76 0x1c 0xe7 0x93 0xcd 0xa 0x28 0xbc 0x72]
…
---Раунд 6---
M xor K6 = [0x2e 0xcb 0x46 0xb0 0xa2 0xab 0x22 0x42 0x25 0x4 0xe5 0x48 0x20 0x49 0xe0
0xee]
S(M) = [0x8e 0xe4 0x48 0xad 0x60 0x82 0x65 0x2c 0x5c 0xcf 0x2b 0xf2 0xf9 0x2a 0x20 0x6c]
L(M) = [0xbf 0x6e 0xdd 0xd7 0xec 0x4a 0xb3 0xc7 0xf7 0x28 0x71 0x31 0x8c 0xa3 0xd7 0x8a]
```

Выводы:

В ходе лабораторной работы были исследованы шифры AES, и Кузнечик.

- Для шифра AES были изучены преобразования в среде CrypTool 2.

Результаты работы шифра на первом раунде были успешно сопоставлены с результатами выполнения разработанной программы для раундового преобразования шифра AES (приложение А).

- Для шифра AES был проведён анализ криптостойкости для атаки грубой силы с известной частью ключа с разным количеством известных байт и с разным количеством ядер в среде CrypTool2. Аналогичная атака была проведена с известной частью исходного текста на основе регулярного выражения, что позволило уменьшить время атаки примерно в два раза.

- 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.

- Для шифра Кузнечик были изучены итерации развёртывания ключа в программе Литорея. Результаты развёртывания ключа были успешно сопоставлены с результатами (приложение В) выполнения разработанной программы для шифра кузнечик (приложение Б). Аналогичные действия были проведены для изучения раундов шифрования. Результаты раундов шифрования также были успешно сопоставлены с результатами выполнения разработанной программы.

ПРИЛОЖЕНИЕ А. Исходный код программы для шифра AES

```
import numpy as np

np.set_printoptions(formatter={'int': hex})

# Таблица S-Box подстановок
Sbox = np.array([
    0x63, 0x7c, 0x77, 0x7b, 0xf2, 0x6b, 0x6f, 0xc5, 0x30, 0x01,
0x67, 0x2b, 0xfe, 0xd7, 0xab, 0x76,
    0xca, 0x82, 0xc9, 0x7d, 0xfa, 0x59, 0x47, 0xf0, 0xad, 0xd4,
0xa2, 0xaf, 0x9c, 0xa4, 0x72, 0xc0,
    0xb7, 0xfd, 0x93, 0x26, 0x36, 0x3f, 0xf7, 0xcc, 0x34, 0xa5,
0xe5, 0xf1, 0x71, 0xd8, 0x31, 0x15,
    0x04, 0xc7, 0x23, 0xc3, 0x18, 0x96, 0x05, 0x9a, 0x07, 0x12,
0x80, 0xe2, 0xeb, 0x27, 0xb2, 0x75,
    0x09, 0x83, 0x2c, 0x1a, 0x1b, 0x6e, 0x5a, 0xa0, 0x52, 0x3b,
0xd6, 0xb3, 0x29, 0xe3, 0x2f, 0x84,
    0x53, 0xd1, 0x00, 0xed, 0x20, 0xfc, 0xb1, 0x5b, 0x6a, 0xcb,
0xbe, 0x39, 0x4a, 0x4c, 0x58, 0xcf,
    0xd0, 0xef, 0xaa, 0xfb, 0x43, 0x4d, 0x33, 0x85, 0x45, 0xf9,
0x02, 0x7f, 0x50, 0x3c, 0x9f, 0xa8,
    0x51, 0xa3, 0x40, 0x8f, 0x92, 0x9d, 0x38, 0xf5, 0xbc, 0xb6,
0xda, 0x21, 0x10, 0xff, 0xf3, 0xd2,
    0xcd, 0x0c, 0x13, 0xec, 0x5f, 0x97, 0x44, 0x17, 0xc4, 0xa7,
0x7e, 0x3d, 0x64, 0x5d, 0x19, 0x73,
    0x60, 0x81, 0x4f, 0xdc, 0x22, 0x2a, 0x90, 0x88, 0x46, 0xee,
0xb8, 0x14, 0xde, 0x5e, 0x0b, 0xdb,
    0xe0, 0x32, 0x3a, 0x0a, 0x49, 0x06, 0x24, 0x5c, 0xc2, 0xd3,
0xac, 0x62, 0x91, 0x95, 0xe4, 0x79,
    0xe7, 0xc8, 0x37, 0x6d, 0x8d, 0xd5, 0x4e, 0xa9, 0x6c, 0x56,
0xf4, 0xea, 0x65, 0x7a, 0xae, 0x08,
    0xba, 0x78, 0x25, 0x2e, 0x1c, 0xa6, 0xb4, 0xc6, 0xe8, 0xdd,
0x74, 0x1f, 0x4b, 0xbd, 0x8b, 0x8a,
    0x70, 0x3e, 0xb5, 0x66, 0x48, 0x03, 0xf6, 0x0e, 0x61, 0x35,
0x57, 0xb9, 0x86, 0xc1, 0x1d, 0x9e,
    0xe1, 0xf8, 0x98, 0x11, 0x69, 0xd9, 0x8e, 0x94, 0x9b, 0x1e,
0x87, 0xe9, 0xce, 0x55, 0x28, 0xdf,
    0x8c, 0xa1, 0x89, 0x0d, 0xbf, 0xe6, 0x42, 0x68, 0x41, 0x99,
0x2d, 0x0f, 0xb0, 0x54, 0xbb, 0x16
]).reshape((16, 16))

# Начальный ключ (для удобства транспонирован)
K = np.array([
    [0x30, 0x33, 0x30, 0x33],
    [0x30, 0x34, 0x5f, 0x6f],
    [0x6c, 0x65, 0x67, 0x6f],
    [0x76, 0x69, 0x63, 0x68]
])

# Блок сообщения (для удобства транспонирован)
M = np.array([
    [0x62, 0x6f, 0x6c, 0x6b],
```

```
    [0x75, 0x6e, 0x6f, 0x76],
    [0x5f, 0x76, 0x6c, 0x61],
    [0x64, 0x00, 0x00, 0x00],
])

print('---Генерация ключа---\n')

# Берём последнюю 'колонку' (в нашем случае строка)
t = K[-1].copy()
print(f'Последние 4 байта ключа (t4): {t}')

# Сдвигаем циклически элементы (первый в конец)
t = np.roll(t, -1)
print(f't4 после RotWord: {t}')

# Примеянем SubByte
t = np.array(list(
    map(
        lambda x: Sbox[x >> 4][x & 0x0f],
        t
    )
))
print(f't4 после SubWord: {t}')

# Применяем xor с константой раунда
t = t ^ np.array([0x01, 0x00, 0x00, 0x00])
print(f't4 после Rcon(1): {t}')

# Формируем раундовый ключ (t4 xor W0 xor W1 ...)
K1 = []
for col in K:
    t = col ^ t
    K1.append(t)

# Преобразуем к матрице numpy
K1 = np.array(K1)

# Выводим матрицу состояний. Здесь и далее вывод матриц
осуществляется в обратно транспонированном виде (как в CrypTool)
print(f'Итоговая матрица состояний ключа в первом
раунде:\n{K1.T}')

print('\n---Шифрование---\n')

# Начальный раунд (xor сообщения с начальным ключом
E = M ^ K

print(f'Матрица состояний сообщений после начального раунда (xor с
ключом):\n{E.T}\n')

# Замена S-box блоками (SubBytes)
E = np.array(list(
    map(
```

```
        lambda col: list(
            map(
                lambda x: Sbox[x >> 4][x & 0x0f],
                col
            )
        ),
        E
    )
))

print(f'Матрица состояний после SubBytes:\n{E.T}\n')

# Осуществляем циклический сдвиг строк (т.к. у нас это столбцы
выполняем дополнительно транспонирование)
nE = []
for i in range(E.shape[0]):
    nE.append(np.roll(E.T[i], -i))

# Обновялем матрицу состоянний
E = np.array(nE).T

print(f'Матрица состояний после ShiftRows:\n{E.T}\n')


# Умножение байт в поле GF(256)
https://en.wikipedia.org/wiki/Rijndael_MixColumns
def g_mul(a, b):
    p = 0
    for c in range(8):
        if (b & 1) != 0:
            p ^= a
        hi_bit_set = (a & 0x80) != 0
        a = (a << 1) & 0xFF
        if hi_bit_set:
            a ^= 0x1B
        b >>= 1

    return p


# Матрица констант
C = np.array([
    [2, 1, 1, 3],
    [3, 2, 1, 1],
    [1, 3, 2, 1],
    [1, 1, 3, 2],
])

# Умножение на матрицу констант
nE = []
for i in range(E.shape[0]):
    col = []
    for j in range(C.shape[1]):
```

```
            p = 0
            for k in range(E.shape[1]):
                p ^= g_mul(E[i][k], C[k][j])
            col.append(p)
        nE.append(np.array(col))

E = np.array(nE).T

print(f'Матрица состояний после MixColumns:\n{E.T}\n')

# Добавляем раундовый ключ
E = E.T ^ K1

print(f'Матрица состояний после AddKey:\n{E.T}')
```

ПРИЛОЖЕНИЕ Б. Исходный код программы для шифра Кузнечик

```
import numpy as np

np.set_printoptions(formatter={'int': hex}, edgeitems=30,
linewidth=100000)

# Блок замены
S = np.array([
    0xFC, 0xEE, 0xDD, 0x11, 0xCF, 0x6E, 0x31, 0x16, 0xFB, 0xC4,
0xFA, 0xDA, 0x23, 0xC5, 0x04, 0x4D,
    0xE9, 0x77, 0xF0, 0xDB, 0x93, 0x2E, 0x99, 0xBA, 0x17, 0x36,
0xF1, 0xBB, 0x14, 0xCD, 0x5F, 0xC1,
    0xF9, 0x18, 0x65, 0x5A, 0xE2, 0x5C, 0xEF, 0x21, 0x81, 0x1C,
0x3C, 0x42, 0x8B, 0x01, 0x8E, 0x4F,
    0x05, 0x84, 0x02, 0xAE, 0xE3, 0x6A, 0x8F, 0xA0, 0x06, 0x0B,
0xED, 0x98, 0x7F, 0xD4, 0xD3, 0x1F,
    0xEB, 0x34, 0x2C, 0x51, 0xEA, 0xC8, 0x48, 0xAB, 0xF2, 0x2A,
0x68, 0xA2, 0xFD, 0x3A, 0xCE, 0xCC,
    0xB5, 0x70, 0x0E, 0x56, 0x08, 0x0C, 0x76, 0x12, 0xBF, 0x72,
0x13, 0x47, 0x9C, 0xB7, 0x5D, 0x87,
    0x15, 0xA1, 0x96, 0x29, 0x10, 0x7B, 0x9A, 0xC7, 0xF3, 0x91,
0x78, 0x6F, 0x9D, 0x9E, 0xB2, 0xB1,
    0x32, 0x75, 0x19, 0x3D, 0xFF, 0x35, 0x8A, 0x7E, 0x6D, 0x54,
0xC6, 0x80, 0xC3, 0xBD, 0x0D, 0x57,
    0xDF, 0xF5, 0x24, 0xA9, 0x3E, 0xA8, 0x43, 0xC9, 0xD7, 0x79,
0xD6, 0xF6, 0x7C, 0x22, 0xB9, 0x03,
    0xE0, 0x0F, 0xEC, 0xDE, 0x7A, 0x94, 0xB0, 0xBC, 0xDC, 0xE8,
0x28, 0x50, 0x4E, 0x33, 0x0A, 0x4A,
    0xA7, 0x97, 0x60, 0x73, 0x1E, 0x00, 0x62, 0x44, 0x1A, 0xB8,
0x38, 0x82, 0x64, 0x9F, 0x26, 0x41,
    0xAD, 0x45, 0x46, 0x92, 0x27, 0x5E, 0x55, 0x2F, 0x8C, 0xA3,
0xA5, 0x7D, 0x69, 0xD5, 0x95, 0x3B,
    0x07, 0x58, 0xB3, 0x40, 0x86, 0xAC, 0x1D, 0xF7, 0x30, 0x37,
0x6B, 0xE4, 0x88, 0xD9, 0xE7, 0x89,
    0xE1, 0x1B, 0x83, 0x49, 0x4C, 0x3F, 0xF8, 0xFE, 0x8D, 0x53,
0xAA, 0x90, 0xCA, 0xD8, 0x85, 0x61,
    0x20, 0x71, 0x67, 0xA4, 0x2D, 0x2B, 0x09, 0x5B, 0xCB, 0x9B,
0x25, 0xD0, 0xBE, 0xE5, 0x6C, 0x52,
    0x59, 0xA6, 0x74, 0xD2, 0xE6, 0xF4, 0xB4, 0xC0, 0xD1, 0x66,
0xAF, 0xC2, 0x39, 0x4B, 0x63, 0xB6
]).reshape((16, 16))

# Вектор для L преобразования
l_vec = np.array([148, 32, 133, 16, 194, 192, 1, 251, 1, 192, 194,
16, 133, 32, 148, 1])


# Умножение по модулю многочлена x^8 + x^7 + x^6 + x + 1
def g_mul(a, b):
    r = 0
    while a:
        if a & 1:
```

```
            r ^= b
        if b & 0x80:
            b = (b << 1) ^ 0x1C3
        else:
            b <<= 1
        a >>= 1
    return r


# L преобразование
def L(_b: np.ndarray):
    b = _b.copy()

    for i in range(16):
        p = 0
        # Суммируем произведения байт на l_vec
        for (x, y) in zip(b, l_vec):
            p ^= g_mul(x, y)

        # Сдвигаем байты к младшему
        b = np.roll(b.copy(), 1)

        # Записываем в старший байт полученную сумму
        b[0] = p

    return b


# Генерируем константы
C = []
for i in range(32):
    C.append(L(np.array([0] * 15 + [i + 1])))

# Две части ключа
K1 = np.array([
    0x30, 0x33, 0x30, 0x33, 0x30, 0x34, 0x5f, 0x6f,
    0x6c, 0x65, 0x67, 0x6f, 0x76, 0x69, 0x63, 0x68
])
K2 = np.array([0x00] * 16)

# Массив раундовых ключей
K = [K1, K2]

for i in range(4):
    # Номера текущих ключей
    ki1 = 3 + i * 2
    ki2 = 4 + i * 2

    print(f'---Генерация ключей {ki1}, {ki2}---')
    # Берём два последних раундовых ключа
    k1, k2 = K[-2], K[-1]

    print(f'K{ki1 - 2} = {k1}')
```

```
        print(f'K{ki2 - 2} = {k2}\n')

        for j in range(8):
            # Сохраняем K1 для замены им K2
            _k1 = k1
            print(f'\t---Итерация {j + 1}---')

            # Константа итерации
            c = C[i * 8 + j]
            print(f'\tC{i * 8 + j + 1} = {c}')

            # Xor с константой
            k1 = k1 ^ c
            print(f'\tK{ki1} xor c = {k1}')

            # S блок (k1)
            k1 = np.array(list(map(lambda x: S[x >> 4][x & 0x0f],
k1)))
            print(f'\tS(K{ki1}) = {k1}')

            # L блок (k1)
            k1 = L(k1)
            print(f'\tL(K{ki1}) = {k1}')

            # Xor k1 и k2
            k1 = k1 ^ k2
            print(f'\tK{ki1} xor K{ki2} = {k1}')

            # Меняем k2 на k1
            k2 = _k1

            print(f'\tK{ki1} = {k1} ; K{ki2} = {k2}')
            print('\t---Конец итерации---\n')

        print(f'K{(i + 1) * 2} = {k1}')
        print(f'K{(i + 1) * 2 + 1} = {k2}')
        print('---Конец раунда---\n')

        # Добавляем раундовые ключи
        K += [k1, k2]

    print('\nРаундовые ключи:')
    for i in range(5):
        print(
            f'K{2 * i + 1} = {K[2 * i]} \n'
            f'K{2 * i + 2} = {K[2 * i + 1]} \n'
            f'---'
        )

    print('\n---Шифрование---')

    # Блок данных
    M = np.array([
```

```
    0x62, 0x6f, 0x6c, 0x6b, 0x75, 0x6e, 0x6f, 0x76,
    0x5f, 0x76, 0x6c, 0x61, 0x64, 0x00, 0x00, 0x00
])

print(f'M = {M}\n')

for i in range(10):
    print(f'---Раунд {i + 1}---')

    # Xor с раундовым ключом
    M = M ^ K[i]
    print(f'M xor K{i + 1} = {M}')

    # S блок
    M = np.array(list(map(lambda x: S[x >> 4][x & 0x0f], M)))
    print(f'S(M) = {M}')

    # L блок
    M = L(M)
    print(f'L(M) = {M}\n')

print(f'Зашифрованный блок: {M}')
```

ПРИЛОЖЕНИЕ В. Результат работы программы Б.

---Генерация ключей 3, 4---
K1 = [0x30 0x33 0x30 0x33 0x30 0x34 0x5f 0x6f 0x6c 0x65 0x67 0x6f 0x76 0x69 0x63 0x68]
K2 = [0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0]

---Итерация 1---
C1 = [0x6e 0xa2 0x76 0x72 0x6c 0x48 0x7a 0xb8 0x5d 0x27 0xbd 0x10 0xdd 0x84 0x94 0x1]
K3 xor c = [0x5e 0x91 0x46 0x41 0x5c 0x7c 0x25 0xd7 0x31 0x42 0xda 0x7f 0xab 0xed 0xf7 0x69]
S(K3) = [0x5d 0xf 0x48 0x34 0x9c 0xc3 0x5c 0xfe 0x84 0x2c 0xaa 0x57 0x82 0xe5 0xc0 0x91]
L(K3) = [0x28 0xeb 0x90 0xa8 0x23 0xc3 0x3 0xe1 0x9b 0x13 0x45 0x8d 0xf4 0xed 0x73 0x3c]
K3 xor K4 = [0x28 0xeb 0x90 0xa8 0x23 0xc3 0x3 0xe1 0x9b 0x13 0x45 0x8d 0xf4 0xed 0x73 0x3c]
K3 = [0x28 0xeb 0x90 0xa8 0x23 0xc3 0x3 0xe1 0x9b 0x13 0x45 0x8d 0xf4 0xed 0x73 0x3c]
K4 = [0x30 0x33 0x30 0x33 0x30 0x34 0x5f 0x6f 0x6c 0x65 0x67 0x6f 0x76 0x69 0x63 0x68]
---Конец итерации---

---Итерация 2---
C2 = [0xdc 0x87 0xec 0xe4 0xd8 0x90 0xf4 0xb3 0xba 0x4e 0xb9 0x20 0x79 0xcb 0xeb 0x2]
K3 xor c = [0xf4 0x6c 0x7c 0x4c 0xfb 0x53 0xf7 0x52 0x21 0x5d 0xfc 0xad 0x8d 0x26 0x98 0x3e]
S(K3) = [0xe6 0x9d 0xc3 0xfd 0xc2 0x56 0xc0 0xe 0x18 0xb7 0x39 0x9f 0x22 0xef 0xdc 0xd3]
L(K3) = [0x1b 0x63 0x1b 0xc3 0xa 0xc1 0x8 0x69 0x83 0xeb 0x83 0x0 0xb7 0x53 0x7f 0x4d]
K3 xor K4 = [0x2b 0x50 0x2b 0xf0 0x3a 0xf5 0x57 0x6 0xef 0x8e 0xe4 0x6f 0xc1 0x3a 0x1c 0x25]
K3 = [0x2b 0x50 0x2b 0xf0 0x3a 0xf5 0x57 0x6 0xef 0x8e 0xe4 0x6f 0xc1 0x3a 0x1c 0x25]
K4 = [0x28 0xeb 0x90 0xa8 0x23 0xc3 0x3 0xe1 0x9b 0x13 0x45 0x8d 0xf4 0xed 0x73 0x3c]
---Конец итерации---

---Итерация 3---

C3 = [0xb2 0x25 0x9a 0x96 0xb4 0xd8 0x8e 0xb 0xe7 0x69 0x4 0x30 0xa4 0x4f 0x7f 0x3]

K3 xor c = [0x99 0x75 0xb1 0x66 0x8e 0x2d 0xd9 0xd 0x8 0xe7 0xe0 0x5f 0x65 0x75 0x63 0x26]

S(K3) = [0xe8 0x35 0x45 0x9a 0xb9 0x1 0x53 0xc5 0xfb 0x5b 0x20 0x87 0x7b 0x35 0x29 0xef]

L(K3) = [0x1e 0xf9 0x95 0x5d 0xde 0x59 0x2c 0x39 0x99 0x2a 0x98 0x2e 0x2f 0x71 0xe2 0x8e]

K3 xor K4 = [0x36 0x12 0x5 0xf5 0xfd 0x9a 0x2f 0xd8 0x2 0x39 0xdd 0xa3 0xdb 0x9c 0x91 0xb2]

K3 = [0x36 0x12 0x5 0xf5 0xfd 0x9a 0x2f 0xd8 0x2 0x39 0xdd 0xa3 0xdb 0x9c 0x91 0xb2]
K4 = [0x2b 0x50 0x2b 0xf0 0x3a 0xf5 0x57 0x6 0xef 0x8e 0xe4 0x6f 0xc1 0x3a 0x1c 0x25]

---Конец итерации---

---Итерация 4---

C4 = [0x7b 0xcd 0x1b 0xb 0x73 0xe3 0x2b 0xa5 0xb7 0x9c 0xb1 0x40 0xf2 0x55 0x15 0x4]

K3 xor c = [0x4d 0xdf 0x1e 0xfe 0x8e 0x79 0x4 0x7d 0xb5 0xa5 0x6c 0xe3 0x29 0xc9 0x84 0xb6]

S(K3) = [0x3a 0x61 0x5f 0x63 0xb9 0x54 0xcf 0xbd 0x5e 0x0 0x9d 0xa4 0x1c 0x37 0x3e 0x55]

L(K3) = [0x1f 0x69 0x78 0x9a 0xdb 0xa 0x9e 0x4d 0xe 0xf3 0xb7 0x1e 0x81 0x48 0x1 0x85]

K3 xor K4 = [0x34 0x39 0x53 0x6a 0xe1 0xff 0xc9 0x4b 0xe1 0x7d 0x53 0x71 0x40 0x72 0x1d 0xa0]

K3 = [0x34 0x39 0x53 0x6a 0xe1 0xff 0xc9 0x4b 0xe1 0x7d 0x53 0x71 0x40 0x72 0x1d 0xa0]
K4 = [0x36 0x12 0x5 0xf5 0xfd 0x9a 0x2f 0xd8 0x2 0x39 0xdd 0xa3 0xdb 0x9c 0x91 0xb2]

---Конец итерации---

---Итерация 5---

C5 = [0x15 0x6f 0x6d 0x79 0x1f 0xab 0x51 0x1d 0xea 0xbb 0xc 0x50 0x2f 0xd1 0x81 0x5]

K3 xor c = [0x21 0x56 0x3e 0x13 0xfe 0x54 0x98 0x56 0xb 0xc6 0x5f 0x21 0x6f 0xa3 0x9c 0xa5]

S(K3) = [0x18 0x76 0xd3 0xdb 0x63 0x8 0xdc 0x76 0xda 0x1d 0x87 0x18 0xb1 0x73 0x4e 0x0]

L(K3) = [0x76 0x5f 0x40 0x90 0x35 0xb 0xf4 0x94 0xcb 0xb5 0x68 0x67 0x17 0xb0 0x73 0x14]

K3 xor K4 = [0x40 0x4d 0x45 0x65 0xc8 0x91 0xdb 0x4c 0xc9 0x8c 0xb5 0xc4 0xcc 0x2c 0xe2 0xa6]

K3 = [0x40 0x4d 0x45 0x65 0xc8 0x91 0xdb 0x4c 0xc9 0x8c 0xb5 0xc4 0xcc 0x2c 0xe2 0xa6]

K4 = [0x34 0x39 0x53 0x6a 0xe1 0xff 0xc9 0x4b 0xe1 0x7d 0x53 0x71 0x40 0x72 0x1d 0xa0]

---Конец итерации---

---Итерация 6---

C6 = [0xa7 0x4a 0xf7 0xef 0xab 0x73 0xdf 0x16 0xd 0xd2 0x8 0x60 0x8b 0x9e 0xfe 0x6]

K3 xor c = [0xe7 0x7 0xb2 0x8a 0x63 0xe2 0x4 0x5a 0xc4 0x5e 0xbd 0xa4 0x47 0xb2 0x1c 0xa0]

S(K3) = [0x5b 0x16 0x46 0xd6 0x29 0x67 0xcf 0x13 0x86 0x5d 0xd5 0x1e 0xab 0x46 0x14 0xa7]

L(K3) = [0x5b 0xc0 0xa2 0x9e 0x7 0xcd 0x44 0x19 0x80 0x75 0xc1 0xb4 0x7 0x33 0x92 0x63]

K3 xor K4 = [0x6f 0xf9 0xf1 0xf4 0xe6 0x32 0x8d 0x52 0x61 0x8 0x92 0xc5 0x47 0x41 0x8f 0xc3]

K3 = [0x6f 0xf9 0xf1 0xf4 0xe6 0x32 0x8d 0x52 0x61 0x8 0x92 0xc5 0x47 0x41 0x8f 0xc3]

K4 = [0x40 0x4d 0x45 0x65 0xc8 0x91 0xdb 0x4c 0xc9 0x8c 0xb5 0xc4 0xcc 0x2c 0xe2 0xa6]

---Конец итерации---

---Итерация 7---

C7 = [0xc9 0xe8 0x81 0x9d 0xc7 0x3b 0xa5 0xae 0x50 0xf5 0xb5 0x70 0x56 0x1a 0x6a 0x7]

K3 xor c = [0xa6 0x11 0x70 0x69 0x21 0x9 0x28 0xfc 0x31 0xfd 0x27 0xb5 0x11 0x5b 0xe5 0xc4]

S(K3) = [0x62 0x77 0x32 0x91 0x18 0xc4 0x81 0x39 0x84 0x4b 0x21 0x5e 0x77 0x47 0x2b 0x86]

L(K3) = [0xd5 0x53 0x39 0xb2 0x31 0x7b 0x9d 0x6d 0x48 0xe6 0x94 0x11 0x10 0x16 0x8f 0x2e]

K3 xor K4 = [0x95 0x1e 0x7c 0xd7 0xf9 0xea 0x46 0x21 0x81 0x6a 0x21 0xd5 0xdc 0x3a 0x6d 0x88]

K3 = [0x95 0x1e 0x7c 0xd7 0xf9 0xea 0x46 0x21 0x81 0x6a 0x21 0xd5 0xdc 0x3a 0x6d 0x88]

K4 = [0x6f 0xf9 0xf1 0xf4 0xe6 0x32 0x8d 0x52 0x61 0x8 0x92 0xc5 0x47 0x41 0x8f 0xc3]

---Конец итерации---

---Итерация 8---

C8 = [0xf6 0x59 0x36 0x16 0xe6 0x5 0x56 0x89 0xad 0xfb 0xa1 0x80 0x27 0xaa 0x2a 0x8]

K3 xor c = [0x63 0x47 0x4a 0xc1 0x1f 0xef 0x10 0xa8 0x2c 0x91 0x80 0x55 0xfb 0x90 0x47 0x80]

S(K3) = [0x29 0xab 0x68 0x58 0xc1 0x52 0xe9 0x1a 0x8b 0xf 0xdf 0xc 0xc2 0xe0 0xab 0xdf]

L(K3) = [0x9d 0x6a 0x2b 0xc5 0x42 0xa3 0xdf 0x65 0xd7 0x46 0xe5 0x52 0x34 0x58 0x32 0x58]

K3 xor K4 = [0xf2 0x93 0xda 0x31 0xa4 0x91 0x52 0x37 0xb6 0x4e 0x77 0x97 0x73 0x19 0xbd 0x9b]

K3 = [0xf2 0x93 0xda 0x31 0xa4 0x91 0x52 0x37 0xb6 0x4e 0x77 0x97 0x73 0x19 0xbd 0x9b]

K4 = [0x95 0x1e 0x7c 0xd7 0xf9 0xea 0x46 0x21 0x81 0x6a 0x21 0xd5 0xdc 0x3a 0x6d 0x88]

---Конец итерации---

K2 = [0xf2 0x93 0xda 0x31 0xa4 0x91 0x52 0x37 0xb6 0x4e 0x77 0x97 0x73 0x19 0xbd 0x9b]

K3 = [0x95 0x1e 0x7c 0xd7 0xf9 0xea 0x46 0x21 0x81 0x6a 0x21 0xd5 0xdc 0x3a 0x6d 0x88]

---Конец раунда---

---Генерация ключей 5, 6---

K3 = [0xf2 0x93 0xda 0x31 0xa4 0x91 0x52 0x37 0xb6 0x4e 0x77 0x97 0x73 0x19 0xbd 0x9b]

K4 = [0x95 0x1e 0x7c 0xd7 0xf9 0xea 0x46 0x21 0x81 0x6a 0x21 0xd5 0xdc 0x3a 0x6d 0x88]

---Итерация 1---

C9 = [0x98 0xfb 0x40 0x64 0x8a 0x4d 0x2c 0x31 0xf0 0xdc 0x1c 0x90 0xfa 0x2e 0xbe 0x9]

K5 xor c = [0x6a 0x68 0x9a 0x55 0x2e 0xdc 0x7e 0x6 0x46 0x92 0x6b 0x7 0x89 0x37 0x3 0x92]

S(K5) = [0x78 0xf3 0x28 0xc 0x8e 0xca 0xd 0x31 0x48 0xec 0x6f 0x16 0x79 0xa0 0x11 0xec]

L(K5) = [0x5a 0xc0 0xee 0x35 0x9 0xa 0x33 0x68 0xb6 0x36 0xe2 0x91 0x11 0xb6 0x7b 0xbe]

K5 xor K6 = [0xcf 0xde 0x92 0xe2 0xf0 0xe0 0x75 0x49 0x37 0x5c 0xc3 0x44 0xcd 0x8c 0x16 0x36]

K5 = [0xcf 0xde 0x92 0xe2 0xf0 0xe0 0x75 0x49 0x37 0x5c 0xc3 0x44 0xcd 0x8c 0x16 0x36]

K6 = [0xf2 0x93 0xda 0x31 0xa4 0x91 0x52 0x37 0xb6 0x4e 0x77 0x97 0x73 0x19 0xbd 0x9b]

---Конец итерации---

---Итерация 2---

C10 = [0x2a 0xde 0xda 0xf2 0x3e 0x95 0xa2 0x3a 0x17 0xb5 0x18 0xa0 0x5e 0x61 0xc1 0xa]

K5 xor c = [0xe5 0x0 0x48 0x10 0xce 0x75 0xd7 0x73 0x20 0xe9 0xdb 0xe4 0x93 0xed 0xd7 0x3c]

S(K5) = [0x2b 0xfc 0xf2 0xe9 0xe7 0x35 0xfe 0x3d 0xf9 0x9b 0x90 0x2d 0xde 0xe5 0xfe 0x7f]

L(K5) = [0xa6 0x25 0x57 0x40 0x7d 0x1f 0xb5 0x2d 0x45 0x76 0x9d 0x1c 0x89 0x91 0x5d 0x0]

K5 xor K6 = [0x54 0xb6 0x8d 0x71 0xd9 0x8e 0xe7 0x1a 0xf3 0x38 0xea 0x8b 0xfa 0x88 0xe0 0x9b]

K5 = [0x54 0xb6 0x8d 0x71 0xd9 0x8e 0xe7 0x1a 0xf3 0x38 0xea 0x8b 0xfa 0x88 0xe0 0x9b]

K6 = [0xcf 0xde 0x92 0xe2 0xf0 0xe0 0x75 0x49 0x37 0x5c 0xc3 0x44 0xcd 0x8c 0x16 0x36]

---Конец итерации---

---Итерация 3---

C11 = [0x44 0x7c 0xac 0x80 0x52 0xdd 0xd8 0x82 0x4a 0x92 0xa5 0xb0 0x83 0xe5 0x55 0xb]

K5 xor c = [0x10 0xca 0x21 0xf1 0x8b 0x53 0x3f 0x98 0xb9 0xaa 0x4f 0x3b 0x79 0x6d 0xb5 0x90]

S(K5) = [0xe9 0x6b 0x18 0xa6 0xf6 0x56 0x1f 0xdc 0xa3 0x38 0xcc 0x98 0x54 0x9e 0x5e 0xe0]

L(K5) = [0xe 0xa 0x34 0x65 0xf8 0x6b 0x12 0xea 0xb1 0x25 0xf2 0x74 0x55 0x7c 0xa3 0x4a]

K5 xor K6 = [0xc1 0xd4 0xa6 0x87 0x8 0x8b 0x67 0xa3 0x86 0x79 0x31 0x30 0x98 0xf0 0xb5 0x7c]

K5 = [0xc1 0xd4 0xa6 0x87 0x8 0x8b 0x67 0xa3 0x86 0x79 0x31 0x30 0x98 0xf0 0xb5 0x7c]

K6 = [0x54 0xb6 0x8d 0x71 0xd9 0x8e 0xe7 0x1a 0xf3 0x38 0xea 0x8b 0xfa 0x88 0xe0 0x9b]

---Конец итерации---

---Итерация 4---

C12 = [0x8d 0x94 0x2d 0x1d 0x95 0xe6 0x7d 0x2c 0x1a 0x67 0x10 0xc0 0xd5 0xff 0x3f 0xc]

K5 xor c = [0x4c 0x40 0x8b 0x9a 0x9d 0x6d 0x1a 0x8f 0x9c 0x1e 0x21 0xf0 0x4d 0xf 0x8a 0x70]

S(K5) = [0xfd 0xeb 0xf6 0x28 0x33 0x9e 0xf1 0x3 0x4e 0x5f 0x18 0x59 0x3a 0x4d 0xd6 0x32]

L(K5) = [0x17 0x11 0xb6 0x8d 0x46 0xde 0x2c 0x5e 0xf7 0xcc 0xd1 0x72 0x39 0xec 0xc1 0xe7]

K5 xor K6 = [0x43 0xa7 0x3b 0xfc 0x9f 0x50 0xcb 0x44 0x4 0xf4 0x3b 0xf9 0xc3 0x64 0x21 0x7c]

K5 = [0x43 0xa7 0x3b 0xfc 0x9f 0x50 0xcb 0x44 0x4 0xf4 0x3b 0xf9 0xc3 0x64 0x21 0x7c]

K6 = [0xc1 0xd4 0xa6 0x87 0x8 0x8b 0x67 0xa3 0x86 0x79 0x31 0x30 0x98 0xf0 0xb5 0x7c]

---Конец итерации---

---Итерация 5---

C13 = [0xe3 0x36 0x5b 0x6f 0xf9 0xae 0x7 0x94 0x47 0x40 0xad 0xd0 0x8 0x7b 0xab 0xd]

K5 xor c = [0xa0 0x91 0x60 0x93 0x66 0xfe 0xcc 0xd0 0x43 0xb4 0x96 0x29 0xcb 0x1f 0x8a 0x71]

S(K5) = [0xa7 0xf 0x15 0xde 0x9a 0x63 0x88 0xe1 0x51 0x27 0xb0 0x1c 0xe4 0xc1 0xd6 0x75]

L(K5) = [0x49 0x13 0xa6 0x85 0xf9 0xf2 0xdd 0x91 0xfa 0xe2 0x59 0x79 0x74 0xb0 0xd2 0x78]

K5 xor K6 = [0x88 0xc7 0x0 0x2 0xf1 0x79 0xba 0x32 0x7c 0x9b 0x68 0x49 0xec 0x40 0x67 0x4]

K5 = [0x88 0xc7 0x0 0x2 0xf1 0x79 0xba 0x32 0x7c 0x9b 0x68 0x49 0xec 0x40 0x67 0x4]
K6 = [0x43 0xa7 0x3b 0xfc 0x9f 0x50 0xcb 0x44 0x4 0xf4 0x3b 0xf9 0xc3 0x64 0x21 0x7c]

---Конец итерации---

---Итерация 6---

C14 = [0x51 0x13 0xc1 0xf9 0x4d 0x76 0x89 0x9f 0xa0 0x29 0xa9 0xe0 0xac 0x34 0xd4 0xe]

K5 xor c = [0xd9 0xd4 0xc1 0xfb 0xbc 0xf 0x33 0xad 0xdc 0xb2 0xc1 0xa9 0x40 0x74 0xb3 0xa]

S(K5) = [0x53 0x4c 0x58 0xc2 0x69 0x4d 0xae 0x9f 0xca 0x46 0x58 0xb8 0xeb 0xff 0x92 0xfa]

L(K5) = [0x94 0x70 0xf7 0x48 0xb6 0xf 0x65 0x4a 0x32 0x5f 0xab 0xec 0x3d 0xf5 0x16 0x6a]

K5 xor K6 = [0xd7 0xd7 0xcc 0xb4 0x29 0x5f 0xae 0xe 0x36 0xab 0x90 0x15 0xfe 0x91 0x37 0x16]

K5 = [0xd7 0xd7 0xcc 0xb4 0x29 0x5f 0xae 0xe 0x36 0xab 0x90 0x15 0xfe 0x91 0x37 0x16]
K6 = [0x88 0xc7 0x0 0x2 0xf1 0x79 0xba 0x32 0x7c 0x9b 0x68 0x49 0xec 0x40 0x67 0x4]

---Конец итерации---

---Итерация 7---

C15 = [0x3f 0xb1 0xb7 0x8b 0x21 0x3e 0xf3 0x27 0xfd 0xe 0x14 0xf0 0x71 0xb0 0x40 0xf]

K5 xor c = [0xe8 0x66 0x7b 0x3f 0x8 0x61 0x5d 0x29 0xcb 0xa5 0x84 0xe5 0x8f 0x21 0x77 0x19]

S(K5) = [0xcb 0x9a 0x80 0x1f 0xfb 0xa1 0xb7 0x1c 0xe4 0x0 0x3e 0x2b 0x3 0x18 0x7e 0x36]

L(K5) = [0x12 0xc9 0xac 0xe9 0x2e 0x4a 0xb7 0x63 0x44 0x9 0x88 0x1c 0x58 0xf 0x3b 0xff]

K5 xor K6 = [0x9a 0xe 0xac 0xeb 0xdf 0x33 0xd 0x51 0x38 0x92 0xe0 0x55 0xb4 0x4f 0x5c 0xfb]

K5 = [0x9a 0xe 0xac 0xeb 0xdf 0x33 0xd 0x51 0x38 0x92 0xe0 0x55 0xb4 0x4f 0x5c 0xfb]
K6 = [0xd7 0xd7 0xcc 0xb4 0x29 0x5f 0xae 0xe 0x36 0xab 0x90 0x15 0xfe 0x91 0x37 0x16]

---Конец итерации---

---Итерация 8---

C16 = [0x2f 0xb2 0x6c 0x2c 0xf 0xa 0xac 0xd1 0x99 0x35 0x81 0xc3 0x4e 0x97 0x54 0x10]

K5 xor c = [0xb5 0xbc 0xc0 0xc7 0xd0 0x39 0xa1 0x80 0xa1 0xa7 0x61 0x96 0xfa 0xd8 0x8 0xeb]

S(K5) = [0x5e 0x69 0x7 0xf7 0xe1 0xb 0x97 0xdf 0x97 0x44 0xa1 0xb0 0xaf 0x8d 0xfb 0xd0]

L(K5) = [0x38 0x49 0xaf 0x44 0x8a 0xf 0x4f 0x80 0xde 0xcb 0x99 0x8e 0xf7 0x8 0xb 0x6b]

K5 xor K6 = [0xef 0x9e 0x63 0xf0 0xa3 0x50 0xe1 0x8e 0xe8 0x60 0x9 0x9b 0x9 0x99 0x3c 0x7d]

K5 = [0xef 0x9e 0x63 0xf0 0xa3 0x50 0xe1 0x8e 0xe8 0x60 0x9 0x9b 0x9 0x99 0x3c 0x7d]
K6 = [0x9a 0xe 0xac 0xeb 0xdf 0x33 0xd 0x51 0x38 0x92 0xe0 0x55 0xb4 0x4f 0x5c 0xfb]

---Конец итерации---

K4 = [0xef 0x9e 0x63 0xf0 0xa3 0x50 0xe1 0x8e 0xe8 0x60 0x9 0x9b 0x9 0x99 0x3c 0x7d]
K5 = [0x9a 0xe 0xac 0xeb 0xdf 0x33 0xd 0x51 0x38 0x92 0xe0 0x55 0xb4 0x4f 0x5c 0xfb]
---Конец раунда---

---Генерация ключей 7, 8---
K5 = [0xef 0x9e 0x63 0xf0 0xa3 0x50 0xe1 0x8e 0xe8 0x60 0x9 0x9b 0x9 0x99 0x3c 0x7d]
K6 = [0x9a 0xe 0xac 0xeb 0xdf 0x33 0xd 0x51 0x38 0x92 0xe0 0x55 0xb4 0x4f 0x5c 0xfb]

---Итерация 1---

C17 = [0x41 0x10 0x1a 0x5e 0x63 0x42 0xd6 0x69 0xc4 0x12 0x3c 0xd3 0x93 0x13 0xc0 0x11]

K7 xor c = [0xae 0x8e 0x79 0xae 0xc0 0x12 0x37 0xe7 0x2c 0x72 0x35 0x48 0x9a 0x8a 0xfc 0x6c]

S(K7) = [0x26 0xb9 0x54 0x26 0x7 0xf0 0xa0 0x5b 0x8b 0x19 0x6a 0xf2 0x28 0xd6 0x39 0x9d]

L(K7) = [0xbf 0x59 0xf0 0xdf 0x50 0x38 0xc0 0xa 0xe2 0x39 0xcf 0xe4 0x45 0x77 0x88 0xd]

K7 xor K8 = [0x25 0x57 0x5c 0x34 0x8f 0xb 0xcd 0x5b 0xda 0xab 0x2f 0xb1 0xf1 0x38 0xd4 0xf6]

K7 = [0x25 0x57 0x5c 0x34 0x8f 0xb 0xcd 0x5b 0xda 0xab 0x2f 0xb1 0xf1 0x38 0xd4 0xf6]

K8 = [0xef 0x9e 0x63 0xf0 0xa3 0x50 0xe1 0x8e 0xe8 0x60 0x9 0x9b 0x9 0x99 0x3c 0x7d]

---Конец итерации---

---Итерация 2---

C18 = [0xf3 0x35 0x80 0xc8 0xd7 0x9a 0x58 0x62 0x23 0x7b 0x38 0xe3 0x37 0x5c 0xbf 0x12]

K7 xor c = [0xd6 0x62 0xdc 0xfc 0x58 0x91 0x95 0x39 0xf9 0xd0 0x17 0x52 0xc6 0x64 0x6b 0xe4]

S(K7) = [0xf8 0x96 0xca 0x39 0xbf 0xf 0x94 0xb 0x66 0xe1 0xba 0xe 0x1d 0x10 0x6f 0x2d]

L(K7) = [0x1b 0x69 0x19 0x67 0x21 0x55 0x3c 0x81 0xa3 0xfd 0x9e 0x82 0x1a 0xa0 0x91 0xd2]

K7 xor K8 = [0xf4 0xf7 0x7a 0x97 0x82 0x5 0xdd 0xf 0x4b 0x9d 0x97 0x19 0x13 0x39 0xad 0xaf]

K7 = [0xf4 0xf7 0x7a 0x97 0x82 0x5 0xdd 0xf 0x4b 0x9d 0x97 0x19 0x13 0x39 0xad 0xaf]

K8 = [0x25 0x57 0x5c 0x34 0x8f 0xb 0xcd 0x5b 0xda 0xab 0x2f 0xb1 0xf1 0x38 0xd4 0xf6]

---Конец итерации---

---Итерация 3---

C19 = [0x9d 0x97 0xf6 0xba 0xbb 0xd2 0x22 0xda 0x7e 0x5c 0x85 0xf3 0xea 0xd8 0x2b 0x13]

K7 xor c = [0x69 0x60 0x8c 0x2d 0x39 0xd7 0xff 0xd5 0x35 0xc1 0x12 0xea 0xf9 0xe1 0x86 0xbc]

S(K7) = [0x91 0x15 0x7c 0x1 0xb 0xfe 0xb6 0x3f 0x6a 0x58 0xf0 0x25 0x66 0x71 0x43 0x69]

L(K7) = [0xb 0x8d 0xd7 0x66 0x2b 0x33 0xa8 0x35 0xc2 0x2 0xf7 0x45 0x72 0x7b 0x4a 0xd3]

K7 xor K8 = [0x2e 0xda 0x8b 0x52 0xa4 0x38 0x65 0x6e 0x18 0xa9 0xd8 0xf4 0x83 0x43 0x9e 0x25]

K7 = [0x2e 0xda 0x8b 0x52 0xa4 0x38 0x65 0x6e 0x18 0xa9 0xd8 0xf4 0x83 0x43 0x9e 0x25]

K8 = [0xf4 0xf7 0x7a 0x97 0x82 0x5 0xdd 0xf 0x4b 0x9d 0x97 0x19 0x13 0x39 0xad 0xaf]

---Конец итерации---

---Итерация 4---

C20 = [0x54 0x7f 0x77 0x27 0x7c 0xe9 0x87 0x74 0x2e 0xa9 0x30 0x83 0xbc 0xc2 0x41 0x14]

K7 xor c = [0x7a 0xa5 0xfc 0x75 0xd8 0xd1 0xe2 0x1a 0x36 0x0 0xe8 0x77 0x3f 0x81 0xdf 0x31]

S(K7) = [0xc6 0x0 0x39 0x35 0x8d 0x1b 0x67 0xf1 0x8f 0xfc 0xcb 0x7e 0x1f 0xf5 0x61 0x84]

L(K7) = [0xda 0x7d 0x1c 0x35 0x4c 0x32 0xba 0x30 0xf4 0x6c 0x60 0xc2 0xc3 0x97 0x38 0x5d]

K7 xor K8 = [0x2e 0x8a 0x66 0xa2 0xce 0x37 0x67 0x3f 0xbf 0xf1 0xf7 0xdb 0xd0 0xae 0x95 0xf2]

K7 = [0x2e 0x8a 0x66 0xa2 0xce 0x37 0x67 0x3f 0xbf 0xf1 0xf7 0xdb 0xd0 0xae 0x95 0xf2]

K8 = [0x2e 0xda 0x8b 0x52 0xa4 0x38 0x65 0x6e 0x18 0xa9 0xd8 0xf4 0x83 0x43 0x9e 0x25]

---Конец итерации---

---Итерация 5---

C21 = [0x3a 0xdd 0x1 0x55 0x10 0xa1 0xfd 0xcc 0x73 0x8e 0x8d 0x93 0x61 0x46 0xd5 0x15]

K7 xor c = [0x14 0x57 0x67 0xf7 0xde 0x96 0x9a 0xf3 0xcc 0x7f 0x7a 0x48 0xb1 0xe8 0x40 0xe7]

S(K7) = [0x93 0x12 0xc7 0xc0 0x85 0xb0 0x28 0xd2 0x88 0x57 0xc6 0xf2 0x45 0xcb 0xeb 0x5b]

L(K7) = [0x2c 0x39 0xa9 0x3b 0x3b 0x3f 0x30 0x5c 0x82 0x86 0x2c 0x42 0xbb 0xdb 0xbf 0x87]

K7 xor K8 = [0x2 0xe3 0x22 0x69 0x9f 0x7 0x55 0x32 0x9a 0x2f 0xf4 0xb6 0x38 0x98 0x21 0xa2]

K7 = [0x2 0xe3 0x22 0x69 0x9f 0x7 0x55 0x32 0x9a 0x2f 0xf4 0xb6 0x38 0x98 0x21 0xa2]

K8 = [0x2e 0x8a 0x66 0xa2 0xce 0x37 0x67 0x3f 0xbf 0xf1 0xf7 0xdb 0xd0 0xae 0x95 0xf2]

---Конец итерации---

---Итерация 6---

C22 = [0x88 0xf8 0x9b 0xc3 0xa4 0x79 0x73 0xc7 0x94 0xe7 0x89 0xa3 0xc5 0x9 0xaa 0x16]

K7 xor c = [0x8a 0x1b 0xb9 0xaa 0x3b 0x7e 0x26 0xf5 0xe 0xc8 0x7d 0x15 0xfd 0x91 0x8b 0xb4]

S(K7) = [0xd6 0xbb 0xa3 0x38 0x98 0xd 0xef 0xf4 0x4 0x30 0xbd 0x2e 0x4b 0xf 0xf6 0x27]

L(K7) = [0xca 0x3c 0xd8 0x98 0x20 0x1b 0x4 0x40 0x77 0x22 0xc2 0x57 0xda 0xdc 0xd5 0xdf]

K7 xor K8 = [0xe4 0xb6 0xbe 0x3a 0xee 0x2c 0x63 0x7f 0xc8 0xd3 0x35 0x8c 0xa 0x72 0x40 0x2d]

K7 = [0xe4 0xb6 0xbe 0x3a 0xee 0x2c 0x63 0x7f 0xc8 0xd3 0x35 0x8c 0xa 0x72 0x40 0x2d]

K8 = [0x2 0xe3 0x22 0x69 0x9f 0x7 0x55 0x32 0x9a 0x2f 0xf4 0xb6 0x38 0x98 0x21 0xa2]

---Конец итерации---

---Итерация 7---

C23 = [0xe6 0x5a 0xed 0xb1 0xc8 0x31 0x9 0x7f 0xc9 0xc0 0x34 0xb3 0x18 0x8d 0x3e 0x17]

K7 xor c = [0x2 0xec 0x53 0x8b 0x26 0x1d 0x6a 0x0 0x1 0x13 0x1 0x3f 0x12 0xff 0x7e 0x3a]

S(K7) = [0xdd 0xbe 0x56 0xf6 0xef 0xcd 0x78 0xfc 0xee 0xdb 0xee 0x1f 0xf0 0xb6 0xd 0xed]

L(K7) = [0xe9 0xe6 0xba 0x98 0xb7 0x40 0x11 0x98 0xab 0x8b 0xb9 0x66 0xa 0x11 0x49 0x1d]

K7 xor K8 = [0xeb 0x5 0x98 0xf1 0x28 0x47 0x44 0xaa 0x31 0xa4 0x4d 0xd0 0x32 0x89 0x68 0xbf]

K7 = [0xeb 0x5 0x98 0xf1 0x28 0x47 0x44 0xaa 0x31 0xa4 0x4d 0xd0 0x32 0x89 0x68 0xbf]

K8 = [0xe4 0xb6 0xbe 0x3a 0xee 0x2c 0x63 0x7f 0xc8 0xd3 0x35 0x8c 0xa 0x72 0x40 0x2d]

---Конец итерации---

---Итерация 8---

C24 = [0xd9 0xeb 0x5a 0x3a 0xe9 0xf 0xfa 0x58 0x34 0xce 0x20 0x43 0x69 0x3d 0x7e 0x18]

K7 xor c = [0x32 0xee 0xc2 0xcb 0xc1 0x48 0xbe 0xf2 0x5 0x6a 0x6d 0x93 0x5b 0xb4 0x16 0xa7]

S(K7) = [0x2 0x6c 0xb3 0xe4 0x58 0xf2 0x95 0x74 0x6e 0x78 0x9e 0xde 0x47 0x27 0x99 0x44]

L(K7) = [0x39 0xb8 0xee 0xee 0xfd 0x42 0x63 0xb4 0x25 0x1 0x53 0xad 0x6c 0xd7 0xc0 0xf0]

K7 xor K8 = [0xdd 0xe 0x50 0xd4 0x13 0x6e 0x0 0xcb 0xed 0xd2 0x66 0x21 0x66 0xa5 0x80 0xdd]

K7 = [0xdd 0xe 0x50 0xd4 0x13 0x6e 0x0 0xcb 0xed 0xd2 0x66 0x21 0x66 0xa5 0x80 0xdd]

K8 = [0xeb 0x5 0x98 0xf1 0x28 0x47 0x44 0xaa 0x31 0xa4 0x4d 0xd0 0x32 0x89 0x68 0xbf]

---Конец итерации---

K6 = [0xdd 0xe 0x50 0xd4 0x13 0x6e 0x0 0xcb 0xed 0xd2 0x66 0x21 0x66 0xa5 0x80 0xdd]

K7 = [0xeb 0x5 0x98 0xf1 0x28 0x47 0x44 0xaa 0x31 0xa4 0x4d 0xd0 0x32 0x89 0x68 0xbf]

---Конец раунда---

---Генерация ключей 9, 10---

K7 = [0xdd 0xe 0x50 0xd4 0x13 0x6e 0x0 0xcb 0xed 0xd2 0x66 0x21 0x66 0xa5 0x80 0xdd]

K8 = [0xeb 0x5 0x98 0xf1 0x28 0x47 0x44 0xaa 0x31 0xa4 0x4d 0xd0 0x32 0x89 0x68 0xbf]

---Итерация 1---

C25 = [0xb7 0x49 0x2c 0x48 0x85 0x47 0x80 0xe0 0x69 0xe9 0x9d 0x53 0xb4 0xb9 0xea 0x19]

K9 xor c = [0x6a 0x47 0x7c 0x9c 0x96 0x29 0x80 0x2b 0x84 0x3b 0xfb 0x72 0xd2 0x1c 0x6a 0xc4]

S(K9) = [0x78 0xab 0xc3 0x4e 0xb0 0x1c 0xdf 0x42 0x3e 0x98 0xc2 0x19 0x83 0x14 0x78 0x86]

L(K9) = [0x37 0x18 0x96 0x7 0x7f 0x2f 0x5a 0x63 0xb5 0xdc 0x94 0x32 0x70 0xdc 0x70 0x0]

K9 xor K10 = [0xdc 0x1d 0xe 0xf6 0x57 0x68 0x1e 0xc9 0x84 0x78 0xd9 0xe2 0x42 0x55 0x18 0xbf]

K9 = [0xdc 0x1d 0xe 0xf6 0x57 0x68 0x1e 0xc9 0x84 0x78 0xd9 0xe2 0x42 0x55 0x18 0xbf]

K10 = [0xdd 0xe 0x50 0xd4 0x13 0x6e 0x0 0xcb 0xed 0xd2 0x66 0x21 0x66 0xa5 0x80 0xdd]

---Конец итерации---

---Итерация 2---

C26 = [0x5 0x6c 0xb6 0xde 0x31 0x9f 0xe 0xeb 0x8e 0x80 0x99 0x63 0x10 0xf6 0x95 0x1a]

K9 xor c = [0xd9 0x71 0xb8 0x28 0x66 0xf7 0x10 0x22 0xa 0xf8 0x40 0x81 0x52 0xa3 0x8d 0xa5]

S(K9) = [0x53 0x75 0x8c 0x81 0x9a 0xc0 0xe9 0x65 0xfa 0xd1 0xeb 0xf5 0xe 0x73 0x22 0x0]

L(K9) = [0x57 0x7c 0xf2 0x63 0x21 0x25 0x93 0x65 0xc1 0xc2 0x84 0xcc 0x9 0x5f 0x6c 0xd8]

K9 xor K10 = [0x8a 0x72 0xa2 0xb7 0x32 0x4b 0x93 0xae 0x2c 0x10 0xe2 0xed 0x6f 0xfa 0xec 0x5]

K9 = [0x8a 0x72 0xa2 0xb7 0x32 0x4b 0x93 0xae 0x2c 0x10 0xe2 0xed 0x6f 0xfa 0xec 0x5]

K10 = [0xdc 0x1d 0xe 0xf6 0x57 0x68 0x1e 0xc9 0x84 0x78 0xd9 0xe2 0x42 0x55 0x18 0xbf]

---Конец итерации---

---Итерация 3---

C27 = [0x6b 0xce 0xc0 0xac 0x5d 0xd7 0x74 0x53 0xd3 0xa7 0x24 0x73 0xcd 0x72 0x1 0x1b]

K9 xor c = [0xe1 0xbc 0x62 0x1b 0x6f 0x9c 0xe7 0xfd 0xff 0xb7 0xc6 0x9e 0xa2 0x88 0xed 0x1e]

S(K9) = [0x71 0x69 0x96 0xbb 0xb1 0x4e 0x5b 0x4b 0xb6 0x2f 0x1d 0xa 0x60 0xd7 0xe5 0x5f]

L(K9) = [0x9a 0x6b 0x21 0x62 0xb0 0xa0 0x3 0x9d 0x55 0xa2 0xcf 0xdd 0x8a 0xf7 0x6 0xb2]

K9 xor K10 = [0x46 0x76 0x2f 0x94 0xe7 0xc8 0x1d 0x54 0xd1 0xda 0x16 0x3f 0xc8 0xa2 0x1e 0xd]

K9 = [0x46 0x76 0x2f 0x94 0xe7 0xc8 0x1d 0x54 0xd1 0xda 0x16 0x3f 0xc8 0xa2 0x1e 0xd]

K10 = [0x8a 0x72 0xa2 0xb7 0x32 0x4b 0x93 0xae 0x2c 0x10 0xe2 0xed 0x6f 0xfa 0xec 0x5]

---Конец итерации---

---Итерация 4---

C28 = [0xa2 0x26 0x41 0x31 0x9a 0xec 0xd1 0xfd 0x83 0x52 0x91 0x3 0x9b 0x68 0x6b 0x1c]

K9 xor c = [0xe4 0x50 0x6e 0xa5 0x7d 0x24 0xcc 0xa9 0x52 0x88 0x87 0x3c 0x53 0xca 0x75 0x11]

S(K9) = [0x2d 0xb5 0xb2 0x0 0xbd 0xe2 0x88 0xb8 0xe 0xd7 0xc9 0x7f 0x56 0x6b 0x35 0x77]

L(K9) = [0xf2 0xc3 0x9 0xd3 0xe3 0x84 0x59 0xa8 0x89 0xc7 0x78 0x98 0x15 0xed 0x48 0xd0]

K9 xor K10 = [0x78 0xb1 0xab 0x64 0xd1 0xcf 0xca 0x6 0xa5 0xd7 0x9a 0x75 0x7a 0x17 0xa4 0xd5]

K9 = [0x78 0xb1 0xab 0x64 0xd1 0xcf 0xca 0x6 0xa5 0xd7 0x9a 0x75 0x7a 0x17 0xa4 0xd5]

K10 = [0x46 0x76 0x2f 0x94 0xe7 0xc8 0x1d 0x54 0xd1 0xda 0x16 0x3f 0xc8 0xa2 0x1e 0xd]

---Конец итерации---

---Итерация 5---

C29 = [0xcc 0x84 0x37 0x43 0xf6 0xa4 0xab 0x45 0xde 0x75 0x2c 0x13 0x46 0xec 0xff 0x1d]

K9 xor c = [0xb4 0x35 0x9c 0x27 0x27 0x6b 0x61 0x43 0x7b 0xa2 0xb6 0x66 0x3c 0xfb 0x5b 0xc8]

S(K9) = [0x27 0x6a 0x4e 0x21 0x21 0x6f 0xa1 0x51 0x80 0x60 0x55 0x9a 0x7f 0xc2 0x47 0x30]

L(K9) = [0xea 0x63 0xea 0xc5 0x90 0x3a 0xf7 0x7c 0x62 0x20 0x18 0x34 0xac 0x85 0x4b 0x2b]

K9 xor K10 = [0xac 0x15 0xc5 0x51 0x77 0xf2 0xea 0x28 0xb3 0xfa 0xe 0xb 0x64 0x27 0x55 0x26]

K9 = [0xac 0x15 0xc5 0x51 0x77 0xf2 0xea 0x28 0xb3 0xfa 0xe 0xb 0x64 0x27 0x55 0x26]

K10 = [0x78 0xb1 0xab 0x64 0xd1 0xcf 0xca 0x6 0xa5 0xd7 0x9a 0x75 0x7a 0x17 0xa4 0xd5]

---Конец итерации---

---Итерация 6---

C30 = [0x7e 0xa1 0xad 0xd5 0x42 0x7c 0x25 0x4e 0x39 0x1c 0x28 0x23 0xe2 0xa3 0x80 0x1e]

K9 xor c = [0xd2 0xb4 0x68 0x84 0x35 0x8e 0xcf 0x66 0x8a 0xe6 0x26 0x28 0x86 0x84 0xd5 0x38]

S(K9) = [0x83 0x27 0xf3 0x3e 0x6a 0xb9 0x89 0x9a 0xd6 0x9 0xef 0x81 0x43 0x3e 0x3f 0x6]

L(K9) = [0xdc 0x0 0xab 0x7a 0xd7 0x29 0x11 0x52 0x36 0xd6 0x98 0xf4 0x35 0x23 0x32 0xbc]

K9 xor K10 = [0xa4 0xb1 0x0 0x1e 0x6 0xe6 0xdb 0x54 0x93 0x1 0x2 0x81 0x4f 0x34 0x96 0x69]

K9 = [0xa4 0xb1 0x0 0x1e 0x6 0xe6 0xdb 0x54 0x93 0x1 0x2 0x81 0x4f 0x34 0x96 0x69]
K10 = [0xac 0x15 0xc5 0x51 0x77 0xf2 0xea 0x28 0xb3 0xfa 0xe 0xb 0x64 0x27 0x55 0x26]

---Конец итерации---

---Итерация 7---

C31 = [0x10 0x3 0xdb 0xa7 0x2e 0x34 0x5f 0xf6 0x64 0x3b 0x95 0x33 0x3f 0x27 0x14 0x1f]

K9 xor c = [0xb4 0xb2 0xdb 0xb9 0x28 0xd2 0x84 0xa2 0xf7 0x3a 0x97 0xb2 0x70 0x13 0x82 0x76]

S(K9) = [0x27 0x46 0x90 0xa3 0x81 0x83 0x3e 0x60 0xc0 0xed 0xbc 0x46 0x32 0xdb 0x24 0x8a]

L(K9) = [0x4d 0x4a 0x8f 0x67 0x65 0x95 0x45 0x5 0x45 0xd7 0x81 0xc4 0x4a 0x85 0xf1 0x14]

K9 xor K10 = [0xe1 0x5f 0x4a 0x36 0x12 0x67 0xaf 0x2d 0xf6 0x2d 0x8f 0xcf 0x2e 0xa2 0xa4 0x32]

K9 = [0xe1 0x5f 0x4a 0x36 0x12 0x67 0xaf 0x2d 0xf6 0x2d 0x8f 0xcf 0x2e 0xa2 0xa4 0x32]
K10 = [0xa4 0xb1 0x0 0x1e 0x6 0xe6 0xdb 0x54 0x93 0x1 0x2 0x81 0x4f 0x34 0x96 0x69]

---Конец итерации---

---Итерация 8---

C32 = [0x5e 0xa7 0xd8 0x58 0x1e 0x14 0x9b 0x61 0xf1 0x6a 0xc1 0x45 0x9c 0xed 0xa8 0x20]

K9 xor c = [0xbf 0xf8 0x92 0x6e 0xc 0x73 0x34 0x4c 0x7 0x47 0x4e 0x8a 0xb2 0x4f 0xc 0x12]

S(K9) = [0x3b 0xd1 0xec 0xb2 0x23 0x3d 0xe3 0xfd 0x16 0xab 0xce 0xd6 0x46 0xcc 0x23 0xf0]

L(K9) = [0xc1 0xa 0x9b 0xa6 0xaa 0x5a 0x7e 0x8d 0xc9 0x42 0x7b 0x31 0x93 0xf5 0xe5 0x8a]

K9 xor K10 = [0x65 0xbb 0x9b 0xb8 0xac 0xbc 0xa5 0xd9 0x5a 0x43 0x79 0xb0 0xdc 0xc1 0x73 0xe3]

K9 = [0x65 0xbb 0x9b 0xb8 0xac 0xbc 0xa5 0xd9 0x5a 0x43 0x79 0xb0 0xdc 0xc1 0x73 0xe3]

K10 = [0xe1 0x5f 0x4a 0x36 0x12 0x67 0xaf 0x2d 0xf6 0x2d 0x8f 0xcf 0x2e 0xa2 0xa4 0x32]

---Конец итерации---

K8 = [0x65 0xbb 0x9b 0xb8 0xac 0xbc 0xa5 0xd9 0x5a 0x43 0x79 0xb0 0xdc 0xc1 0x73 0xe3]

K9 = [0xe1 0x5f 0x4a 0x36 0x12 0x67 0xaf 0x2d 0xf6 0x2d 0x8f 0xcf 0x2e 0xa2 0xa4 0x32]

---Конец раунда---

Раундовые ключи:

K1 = [0x30 0x33 0x30 0x33 0x30 0x34 0x5f 0x6f 0x6c 0x65 0x67 0x6f 0x76 0x69 0x63 0x68]

K2 = [0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0]

K3 = [0xf2 0x93 0xda 0x31 0xa4 0x91 0x52 0x37 0xb6 0x4e 0x77 0x97 0x73 0x19 0xbd 0x9b]

K4 = [0x95 0x1e 0x7c 0xd7 0xf9 0xea 0x46 0x21 0x81 0x6a 0x21 0xd5 0xdc 0x3a 0x6d 0x88]

K5 = [0xef 0x9e 0x63 0xf0 0xa3 0x50 0xe1 0x8e 0xe8 0x60 0x9 0x9b 0x9 0x99 0x3c 0x7d]

K6 = [0x9a 0xe 0xac 0xeb 0xdf 0x33 0xd 0x51 0x38 0x92 0xe0 0x55 0xb4 0x4f 0x5c 0xfb]

K7 = [0xdd 0xe 0x50 0xd4 0x13 0x6e 0x0 0xcb 0xed 0xd2 0x66 0x21 0x66 0xa5 0x80 0xdd]

K8 = [0xeb 0x5 0x98 0xf1 0x28 0x47 0x44 0xaa 0x31 0xa4 0x4d 0xd0 0x32 0x89 0x68 0xbf]

K9 = [0x65 0xbb 0x9b 0xb8 0xac 0xbc 0xa5 0xd9 0x5a 0x43 0x79 0xb0 0xdc 0xc1 0x73 0xe3]

K10 = [0xe1 0x5f 0x4a 0x36 0x12 0x67 0xaf 0x2d 0xf6 0x2d 0x8f 0xcf 0x2e 0xa2 0xa4 0x32]

---Шифрование---

M = [0x62 0x6f 0x6c 0x6b 0x75 0x6e 0x6f 0x76 0x5f 0x76 0x6c 0x61 0x64 0x0 0x0 0x0]

---Раунд 1---

M xor K1 = [0x52 0x5c 0x5c 0x58 0x45 0x5a 0x30 0x19 0x33 0x13 0xb 0xe 0x12 0x69 0x63 0x68]

S(M) = [0xe 0x9c 0x9c 0xbf 0xc8 0x13 0x5 0x36 0xae 0xdb 0xda 0x4 0xf0 0x91 0x29 0xf3]

L(M) = [0xac 0xd1 0xd3 0xe7 0xf7 0x5b 0xc5 0x76 0x1c 0xe7 0x93 0xcd 0xa 0x28 0xbc 0x72]

---Раунд 2---
M xor K2 = [0xac 0xd1 0xd3 0xe7 0xf7 0x5b 0xc5 0x76 0x1c 0xe7 0x93 0xcd 0xa 0x28 0xbc 0x72]
S(M) = [0x64 0x1b 0x49 0x5b 0xc0 0x47 0xac 0x8a 0x14 0x5b 0xde 0xd9 0xfa 0x81 0x69 0x19]
L(M) = [0xb6 0x9b 0xe5 0x92 0x21 0x5 0xed 0x40 0x0 0x2e 0x8f 0x27 0x75 0x14 0x69 0xa2]

---Раунд 3---
M xor K3 = [0x44 0x8 0x3f 0xa3 0x85 0x94 0xbf 0x77 0xb6 0x60 0xf8 0xb0 0x6 0xd 0xd4 0x39]
S(M) = [0xea 0xfb 0x1f 0x73 0xa8 0x7a 0x3b 0x7e 0x55 0x15 0xd1 0xad 0x31 0xc5 0x4c 0xb]
L(M) = [0x3d 0x7e 0xc8 0x9f 0x3 0x23 0x9 0x70 0x12 0x1c 0x18 0x63 0xf6 0x1a 0x82 0xa0]

---Раунд 4---
M xor K4 = [0xa8 0x60 0xb4 0x48 0xfa 0xc9 0x4f 0x51 0x93 0x76 0x39 0xb6 0x2a 0x20 0xef 0x28]
S(M) = [0x1a 0x15 0x27 0xf2 0xaf 0x37 0xcc 0x70 0xde 0x8a 0xb 0x55 0x3c 0xf9 0x52 0x81]
L(M) = [0x8 0x91 0x9d 0xa8 0x8c 0x9b 0xb4 0x24 0xfa 0xbc 0x61 0x9 0x13 0xd2 0xdb 0xd9]

---Раунд 5---
M xor K5 = [0xe7 0xf 0xfe 0x58 0x2f 0xcb 0x55 0xaa 0x12 0xdc 0x68 0x92 0x1a 0x4b 0xe7 0xa4]
S(M) = [0x5b 0x4d 0x63 0xbf 0x4f 0xe4 0xc 0x38 0xf0 0xca 0xf3 0xec 0xf1 0xa2 0x5b 0x1e]
L(M) = [0xb4 0xc5 0xea 0x5b 0x7d 0x98 0x2f 0x13 0x1d 0x96 0x5 0x1d 0x94 0x6 0xbc 0x15]

---Раунд 6---
M xor K6 = [0x2e 0xcb 0x46 0xb0 0xa2 0xab 0x22 0x42 0x25 0x4 0xe5 0x48 0x20 0x49 0xe0 0xee]
S(M) = [0x8e 0xe4 0x48 0xad 0x60 0x82 0x65 0x2c 0x5c 0xcf 0x2b 0xf2 0xf9 0x2a 0x20 0x6c]
L(M) = [0xbf 0x6e 0xdd 0xd7 0xec 0x4a 0xb3 0xc7 0xf7 0x28 0x71 0x31 0x8c 0xa3 0xd7 0x8a]

---Раунд 7---
M xor K7 = [0x62 0x60 0x8d 0x3 0xff 0x24 0xb3 0xc 0x1a 0xfa 0x17 0x10 0xea 0x6 0x57 0x57]
S(M) = [0x96 0x15 0x22 0x11 0xb6 0xe2 0x92 0x23 0xf1 0xaf 0xba 0xe9 0x25 0x31 0x12 0x12]
L(M) = [0xd6 0x2a 0xae 0xe4 0x3e 0x9c 0xaf 0x95 0x6 0x81 0x7 0x2c 0xc4 0xda 0xaa 0xba]

---Раунд 8---

M xor K8 = [0x3d 0x2f 0x36 0x15 0x16 0xdb 0xeb 0x3f 0x37 0x25 0x4a 0xfc 0xf6 0x53 0xc2 0x5]
S(M) = [0xd4 0x4f 0x8f 0x2e 0x99 0x90 0xd0 0x1f 0xa0 0x5c 0x68 0x39 0xb4 0x56 0xb3 0x6e]
L(M) = [0x94 0x9f 0xb 0x1d 0x2 0x7 0xa7 0x65 0xfc 0x51 0xc 0x35 0xdd 0x7e 0xf2 0xaa]

---Раунд 9---
M xor K9 = [0xf1 0x24 0x90 0xa5 0xae 0xbb 0x2 0xbc 0xa6 0x12 0x75 0x85 0x1 0xbf 0x81 0x49]
S(M) = [0xa6 0xe2 0xe0 0x0 0x26 0x7d 0xdd 0x69 0x62 0xf0 0x35 0xa8 0xee 0x3b 0xf5 0x2a]
L(M) = [0x74 0xed 0x2f 0xea 0x6 0xc4 0x35 0x45 0xe3 0x49 0xef 0x53 0x5 0x2b 0x68 0x53]

---Раунд 10---
M xor K10 = [0x95 0xb2 0x65 0xdc 0x14 0xa3 0x9a 0x68 0x15 0x64 0x60 0x9c 0x2b 0x89 0xcc 0x61]
S(M) = [0x94 0x46 0x7b 0xca 0x93 0x73 0x28 0xf3 0x2e 0x10 0x15 0x4e 0x42 0x79 0x88 0xa1]
L(M) = [0x2a 0xbe 0x46 0x4d 0xb6 0x33 0x25 0x8a 0xe8 0xb0 0xcd 0x52 0x90 0xd6 0x7e 0x31]

Зашифрованный блок: [0x2a 0xbe 0x46 0x4d 0xb6 0x33 0x25 0x8a 0xe8 0xb0 0xcd 0x52 0x90 0xd6 0x7e 0x31]

ПРИМЕЧАНИЕ *

В программе литорея некорректно отображается результат работы L блока на всех итерациях при развёртывании ключа.