ФЕДЕРАЛЬНОЕ АГЕНСТВО СВЯЗИ
Федеральное государственное бюджетное образовательное учреждение высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. Проф. М. А. Бонч-Бруевича»

Кафедра Защищенных систем связи
Дисциплина «Основы криптографии»

Лабораторная работа № 6

Изучение и исследование блокового шифра AES

Вариант 4

Выполнил: ст. группы ИКТЗ-83

Громов А.А.

Проверил: Профессор кафедры ЗСС: д.т.н. проф. Яковлев В.А.

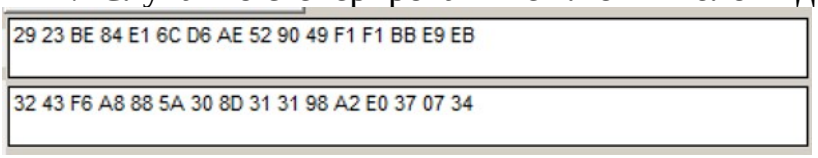
Цель работы

Изучить преобразования, выполняемые при шифровании и дешифровании сообщений в блоковом шифре AES, а также исследовать некоторые его свойства.

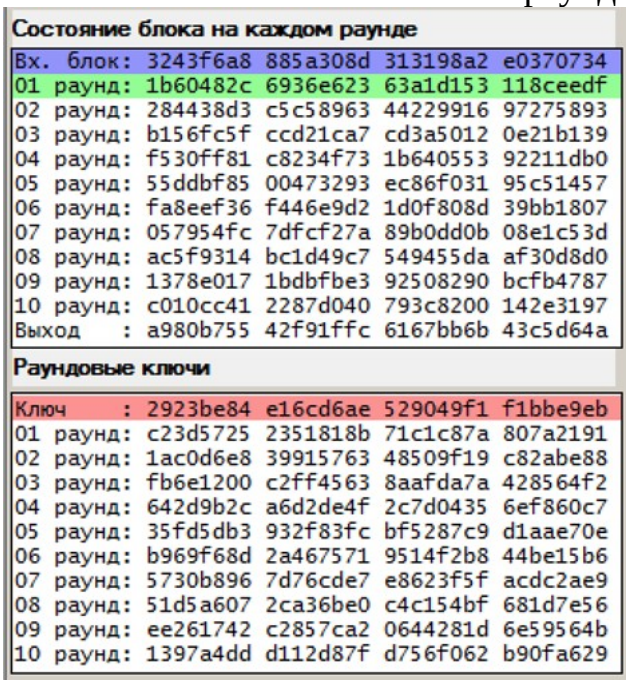
Используемое программное обеспечение

Для выполнения работы используется специальная программа “AES.exe”

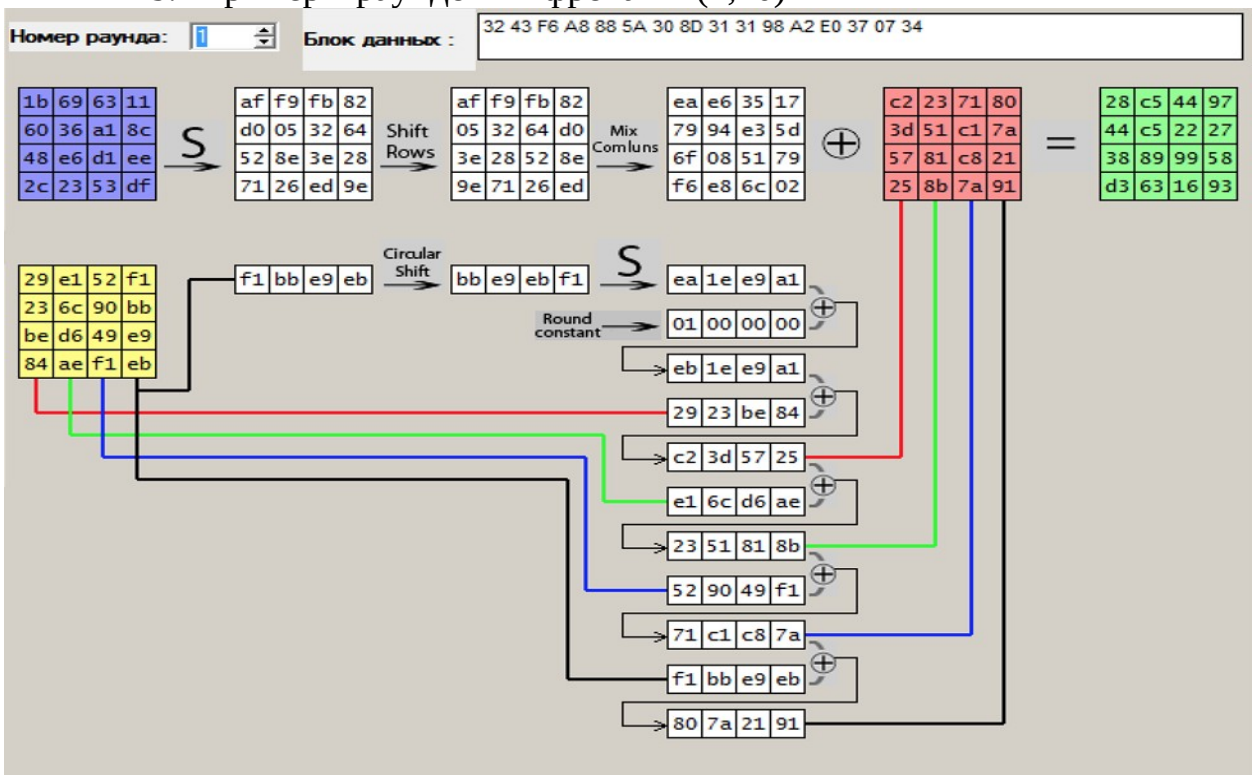
1. Случайно сгенерированные ключи и блоки данных.

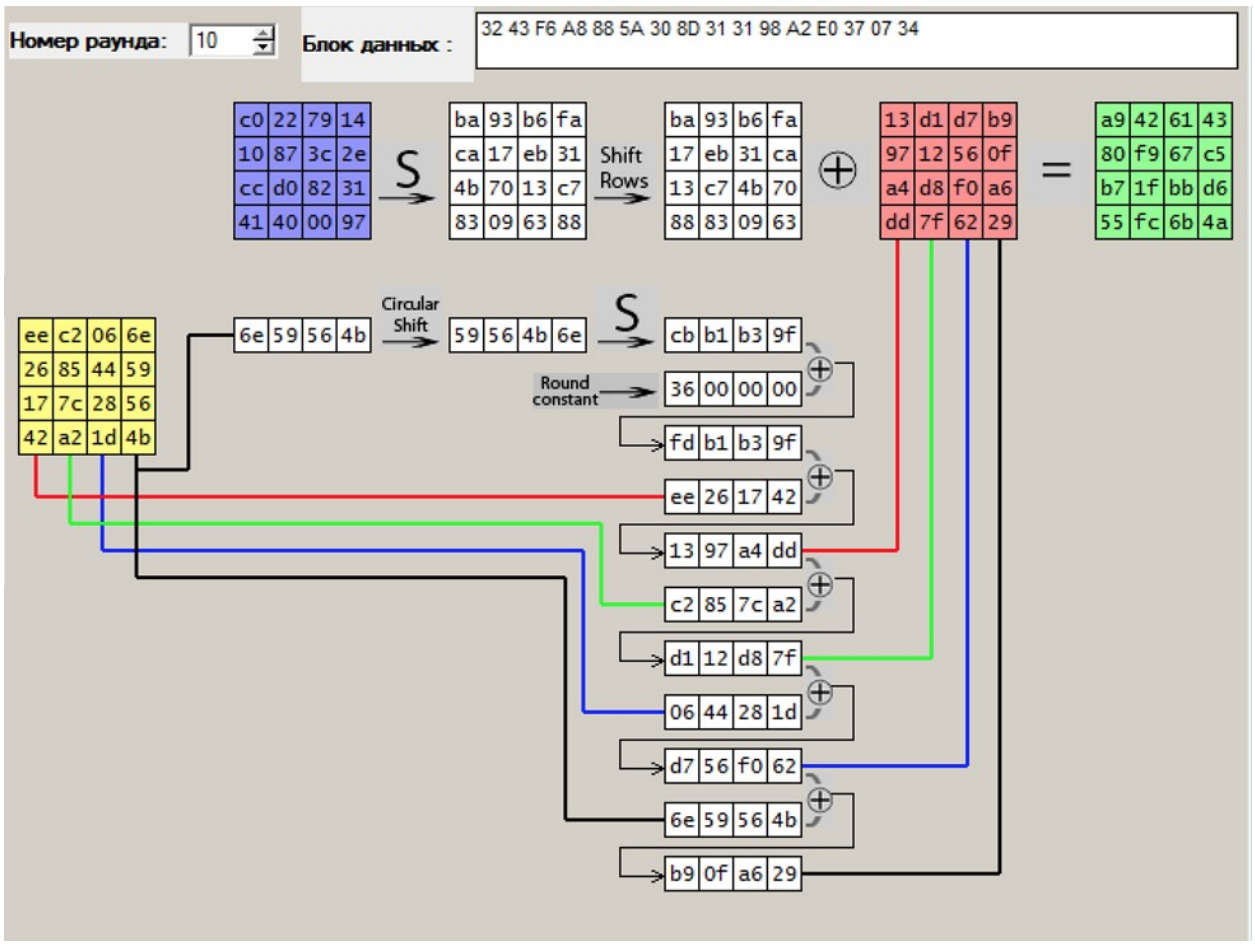


2. Шифрование данных
    a. Состояние блоков и раундовые ключи

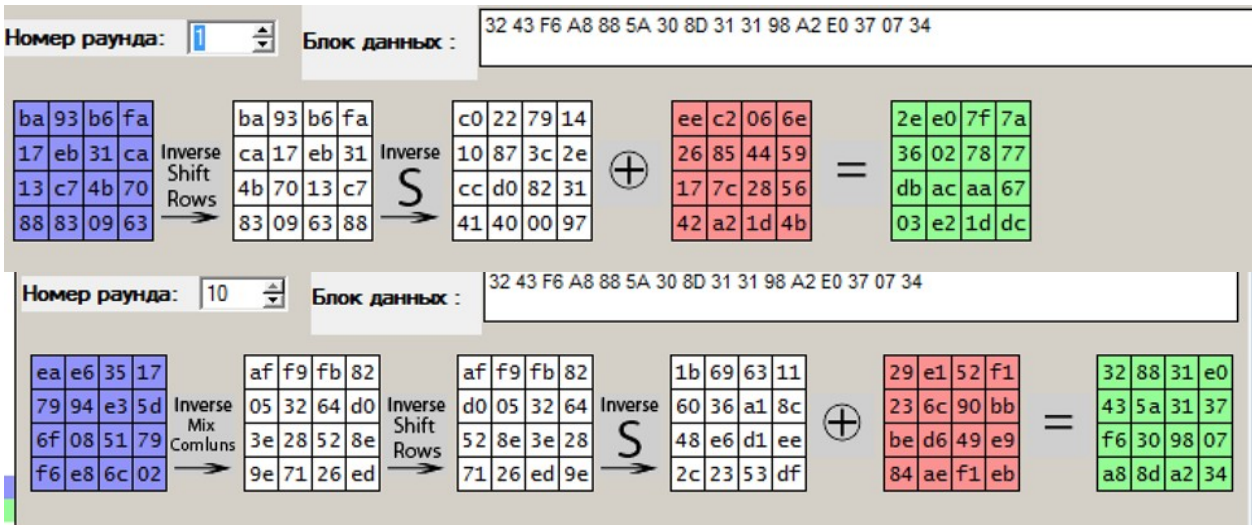


b. Примеры раундов шифрования(1,10)

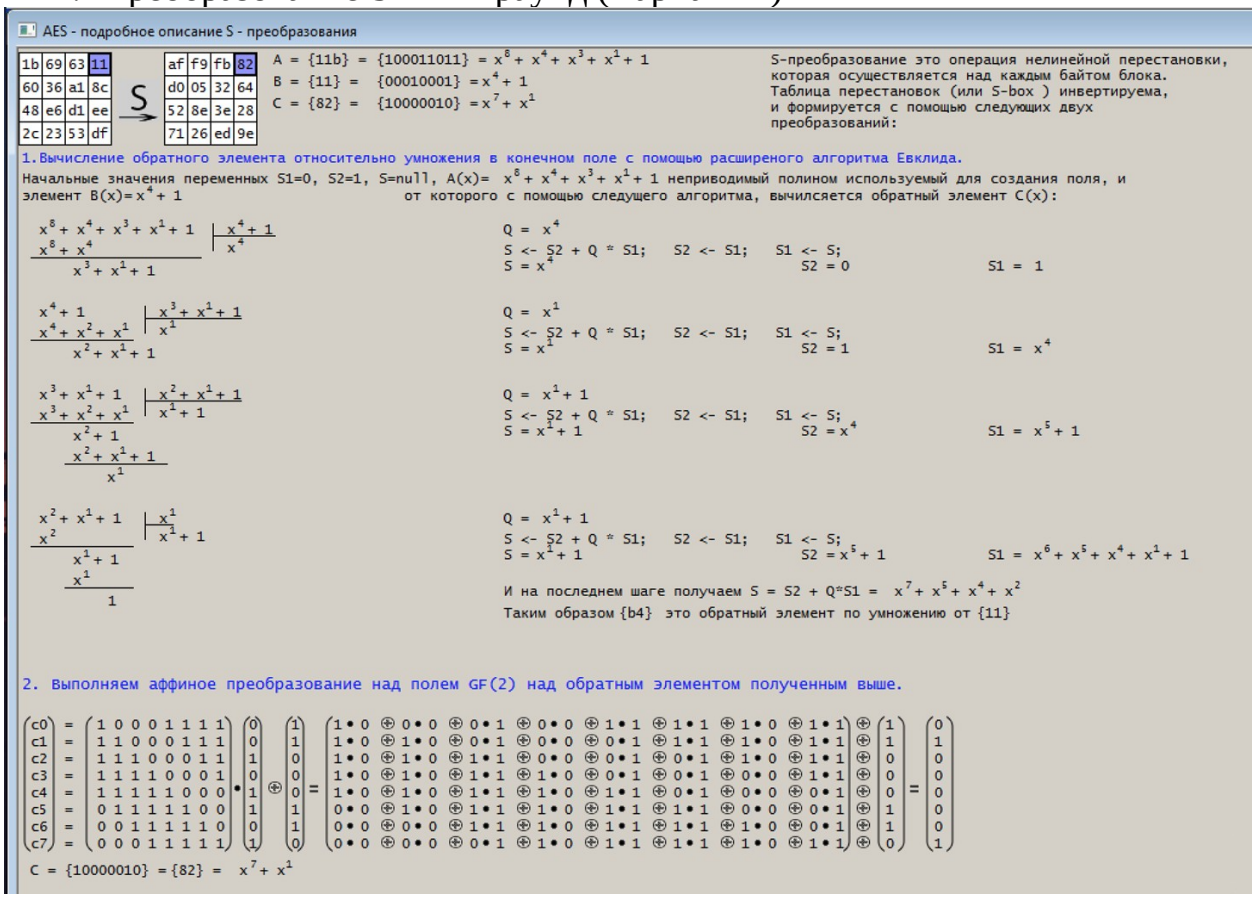




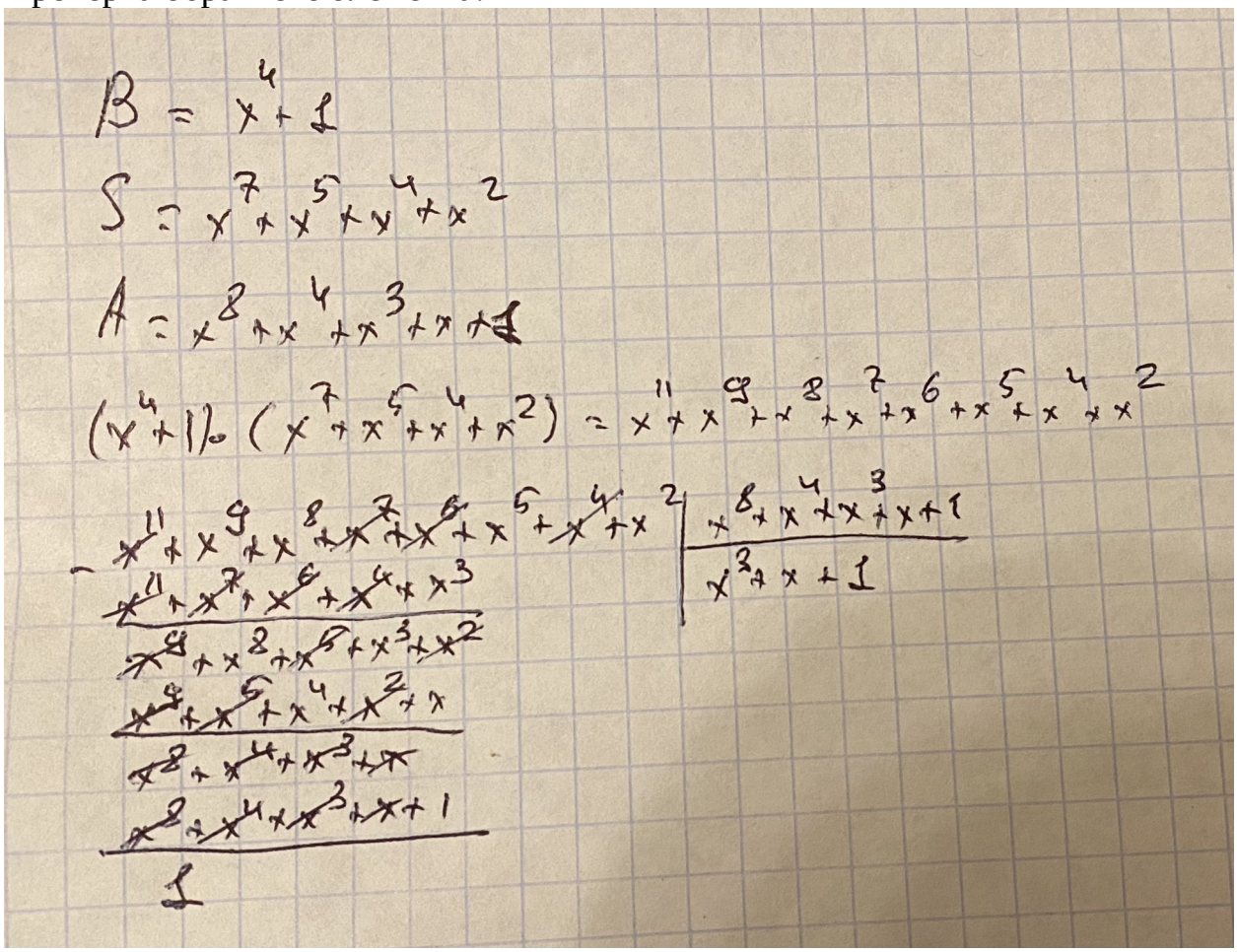
3. Расшифрование данных
    a. Примеры раундов расшифрования(1,10)



4. Преобразование S - 1ый раунд (Вариант 4)

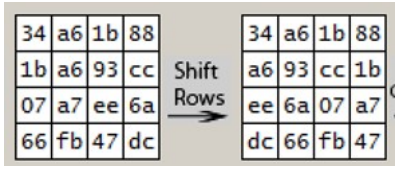


Проверка обратного элемента:

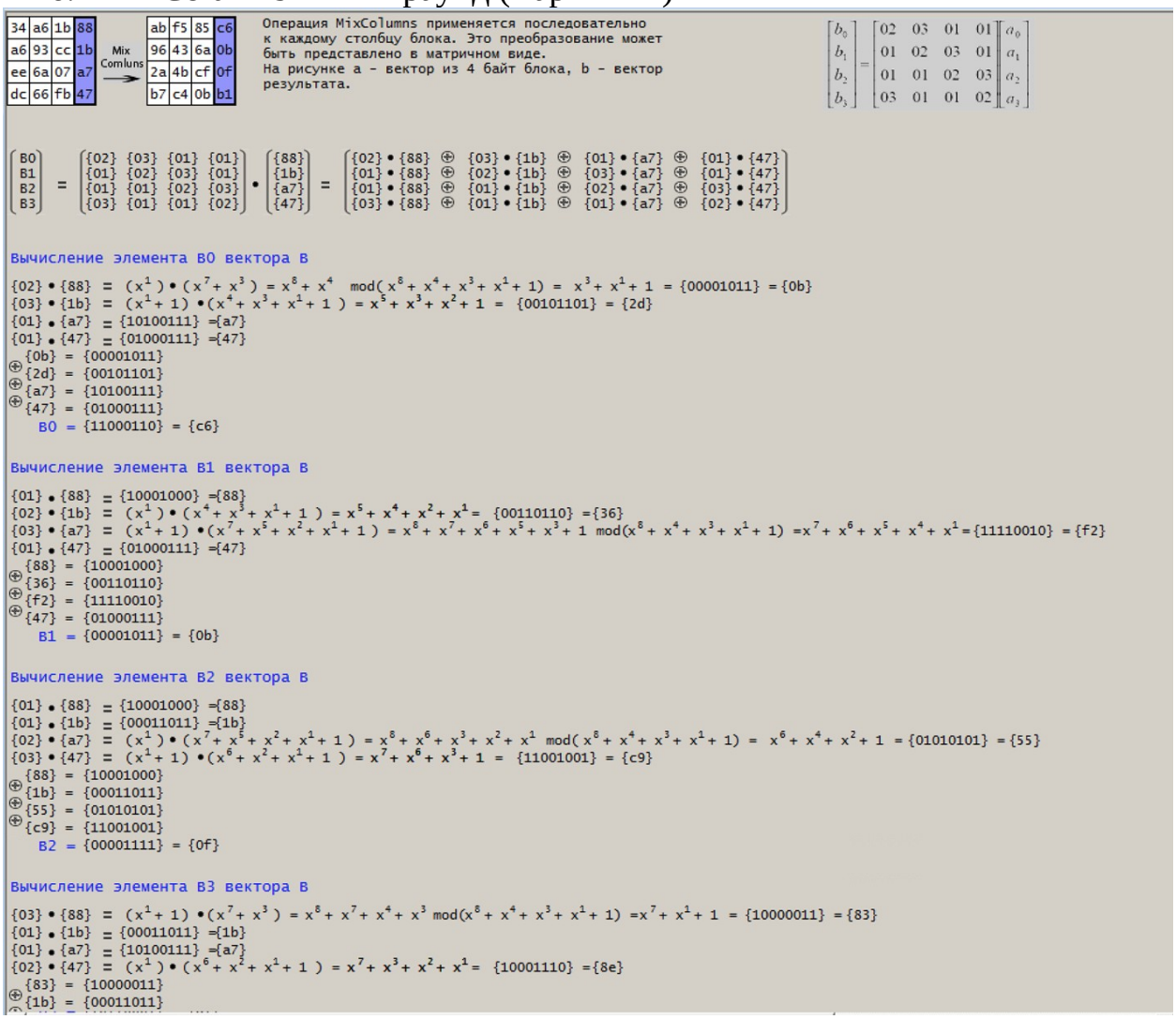


В остатке получилась 1, следовательно, обратный элемент вычислен правильно.

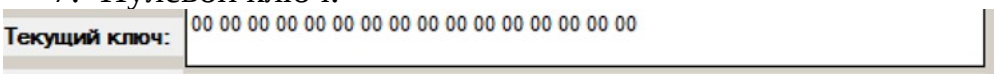
5. Shift Rows:



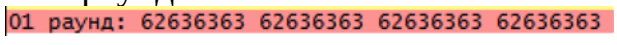
6. Mix Columns – 1-ый раунд (Варивнт 4)

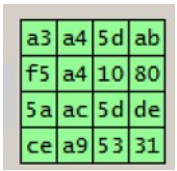


7. Нулевой ключ:



1-ый раунд:





2-ой раунд:

```
02 раунд: 9b9898c9 f9fbfbaa 9b9898c9 f9fbfbaa
```

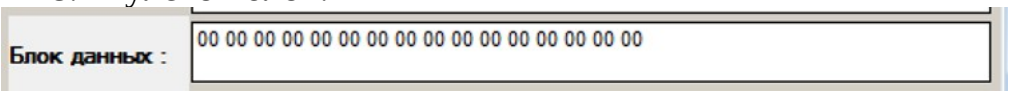
df	b8	22	70
13	91	5f	0b
11	c4	10	6a
47	ab	d3	ba

3-ий раунд:

```
03 раунд: 90973450 696ccffa f2f45733 0b0fac99
```

11	59	52	54
a1	23	ce	e6
a3	93	56	12
51	d8	f0	c7

8. Нулевой блок:



1-ый раунд:

12	11	63	22
f3	bd	15	95
c7	ca	2a	39
f7	c6	5b	0c

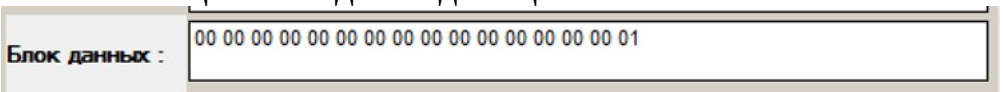
2-ой раунд:

14	1a	cd	f5
c6	55	25	a0
8d	49	7a	74
c5	31	68	4c

3-ий раунд:

6b	d6	10	2c
4f	e6	18	4f
3a	b5	a8	bf
d3	82	90	b9

9. Сообщение с одной единицей:



1-ый раунд:

91	11	63	22
70	bd	15	95
59	ca	2a	39
ea	c6	5b	0c

2-ой раунд:

84	f5	c0	11
8e	ba	32	18
c5	63	60	28
1d	f4	65	10

3-ий раунд:

cb	de	4a	c0
07	69	eb	39
bd	bc	87	f5
f8	f0	df	68

Вывод:

В ходе выполнения данной лабораторной работы мы изучили преобразования, выполняемые при шифровании и дешифровании сообщений в блоковом шифре AES, а также исследовали некоторые его свойства. По результатам из п. 7-9 можно сделать вывод, что число изменившихся бит после каждого преобразования (SubBytes; ShiftRows; MixColumns и AddRoundKey), с повышением номера раунда, увеличивается.