

**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 блочного 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 блочном 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.

|   |
|---|
| 29 23 BE 84 E1 6C D6 AE 52 90 49 F1 F1 BB E9 EB |
|---|

|   |
|---|
| 32 43 F6 A8 88 5A 30 8D 31 31 98 A2 E0 37 07 34 |
|---|

2. Шифрование данных

- а. Состояние блоков и раундовые ключи

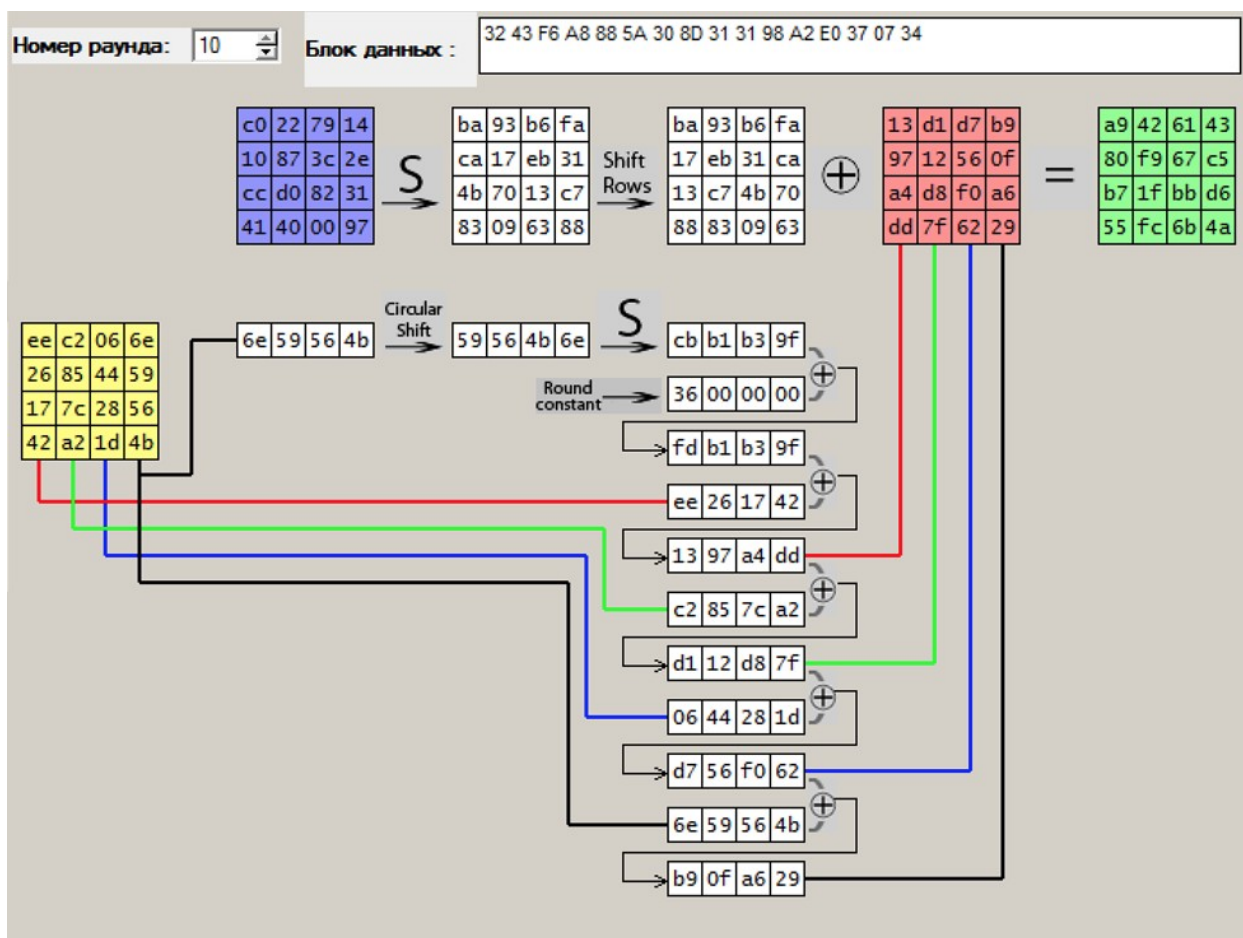
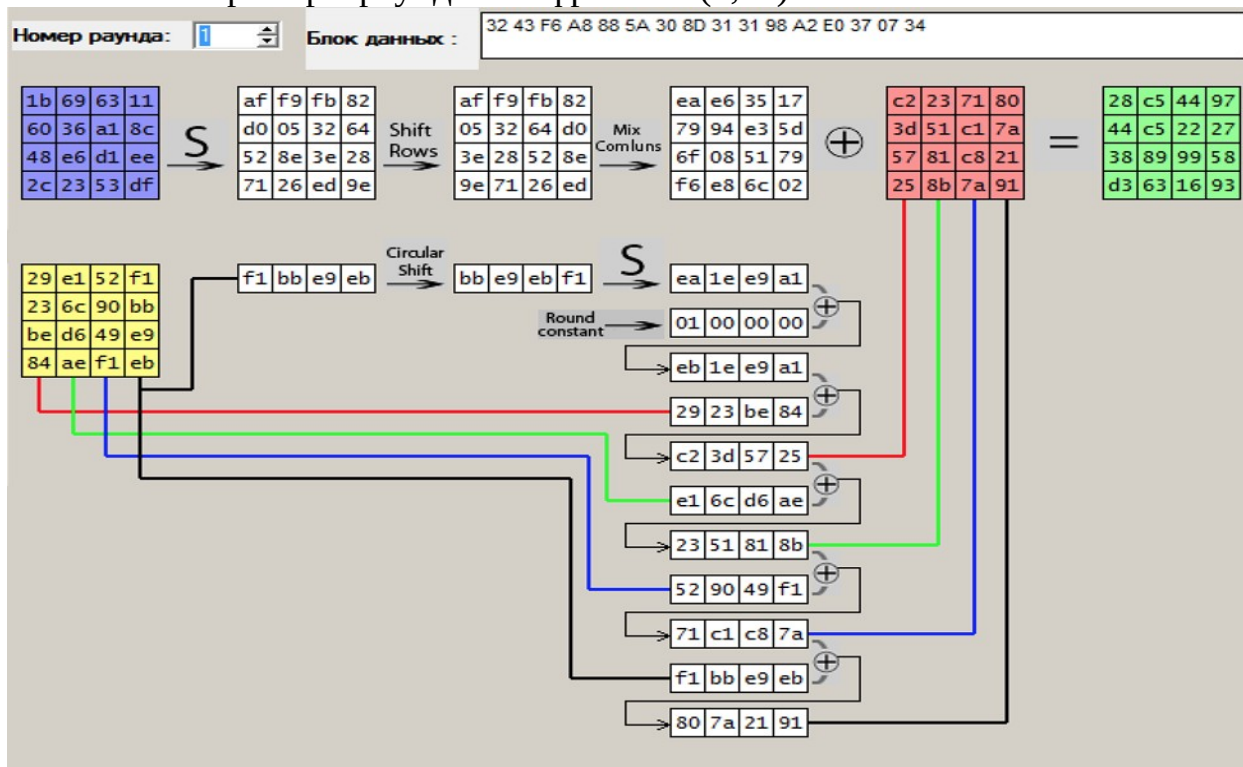
### Состояние блока на каждом раунде

|           |          |          |          |          |
|-----------|----------|----------|----------|----------|
| Вх. блок: | 3243f6a8 | 885a308d | 313198a2 | e0370734 |
| 01 раунд: | 1b60482c | 6936e623 | 63a1d153 | 118ceedf |
| 02 раунд: | 284438d3 | c5c58963 | 44229916 | 97275893 |
| 03 раунд: | b156fc5f | ccd21ca7 | cd3a5012 | 0e21b139 |
| 04 раунд: | f530ff81 | c8234f73 | 1b640553 | 92211db0 |
| 05 раунд: | 55ddb8f5 | 00473293 | ec86f031 | 95c51457 |
| 06 раунд: | fa8eef36 | f446e9d2 | 1d0f808d | 39bb1807 |
| 07 раунд: | 057954fc | 7dfcf27a | 89b0dd0b | 08e1c53d |
| 08 раунд: | ac5f9314 | bc1d49c7 | 549455da | af30d8d0 |
| 09 раунд: | 1378e017 | 1bdbf8e3 | 92508290 | bcbf4787 |
| 10 раунд: | c010cc41 | 2287d040 | 793c8200 | 142e3197 |
| Выход :   | a980b755 | 42f91ffc | 6167bb6b | 43c5d64a |

### Раундовые ключи

|           |          |          |          |          |
|-----------|----------|----------|----------|----------|
| Ключ :    | 2923be84 | e16cd6ae | 529049f1 | f1bbe9eb |
| 01 раунд: | c23d5725 | 2351818b | 71c1c87a | 807a2191 |
| 02 раунд: | 1ac0d6e8 | 39915763 | 48509f19 | c82abe88 |
| 03 раунд: | fb6e1200 | c2ff4563 | 8aafda7a | 428564f2 |
| 04 раунд: | 642d9b2c | a6d2de4f | 2c7d0435 | 6ef860c7 |
| 05 раунд: | 35fd5db3 | 932f83fc | bf5287c9 | d1aae70e |
| 06 раунд: | b969f68d | 2a467571 | 9514f2b8 | 44be15b6 |
| 07 раунд: | 5730b896 | 7d76cde7 | e8623f5f | acdc2ae9 |
| 08 раунд: | 51d5a607 | 2ca36be0 | c4c154bf | 681d7e56 |
| 09 раунд: | ee261742 | c2857ca2 | 0644281d | 6e59564b |
| 10 раунд: | 1397a4dd | d112d87f | d756f062 | b90fa629 |

## в. Примеры раундов шифрования(1,10)



**АЕС - подробное описание S - преобразования**

|    |    |    |    |
|----|----|----|----|
| 1b | 69 | 63 | 11 |
| 60 | 36 | a1 | 8c |
| 48 | e6 | d1 | ee |
| 2c | 23 | 53 | df |

$\rightarrow$

|    |    |    |    |
|----|----|----|----|
| af | f9 | fb | 82 |
| d0 | 05 | 32 | 64 |
| 52 | 8e | 3e | 28 |
| 71 | 26 | ed | 9e |

$A = \{11b\} = \{100011011\} = x^8 + x^4 + x^3 + x^1 + 1$   
 $B = \{11\} = \{00010001\} = x^4 + 1$   
 $C = \{82\} = \{10000010\} = x^7 + x^1$

S-преобразование это операция нелинейной перестановки, которая осуществляется над каждым байтом блока. Таблица перестановок (или S-box) инвертируема, и формируется с помощью следующих двух преобразований:

**1. Вычисление обратного элемента относительно умножения в конечном поле с помощью расширенного алгоритма Евклида.**

Начальные значения переменных S1=0, S2=1, S=null,  $A(x) = x^8 + x^4 + x^3 + x^1 + 1$  неприводимый полином используемый для создания поля, и элемент  $B(x) = x^4 + 1$  от которого с помощью следующего алгоритма, вычисляется обратный элемент C(x):

$$\begin{array}{r} x^8 + x^4 + x^3 + x^1 + 1 \quad | \quad x^4 + 1 \\ \underline{x^8 + x^4} \phantom{+ x^3 + x^1 + 1} \\ x^3 + x^1 + 1 \end{array}$$
  

$$\begin{array}{r} x^4 + 1 \quad | \quad x^3 + x^1 + 1 \\ \underline{x^4 + x^2 + x^1} \\ x^2 + x^1 + 1 \end{array}$$
  

$$\begin{array}{r} x^3 + x^1 + 1 \quad | \quad x^2 + x^1 + 1 \\ \underline{x^3 + x^2 + x^1} \\ x^2 + 1 \\ \underline{x^2 + x^1 + 1} \\ x^1 \end{array}$$
  

$$\begin{array}{r} x^2 + x^1 + 1 \quad | \quad x^1 \\ \underline{x^2 + x^1} \\ x^1 \\ \underline{x^1} \\ 1 \end{array}$$

$Q = x^4$   
 $S \leftarrow S2 + Q * S1; \quad S2 \leftarrow S1; \quad S1 \leftarrow S; \quad S2 = 0 \quad S1 = 1$

$Q = x^2$   
 $S \leftarrow S2 + Q * S1; \quad S2 \leftarrow S1; \quad S1 \leftarrow S; \quad S2 = 1 \quad S1 = x^4$

$Q = x^1 + 1$   
 $S \leftarrow S2 + Q * S1; \quad S2 \leftarrow S1; \quad S1 \leftarrow S; \quad S2 = x^4 \quad S1 = x^5 + 1$

$Q = x^2 + 1$   
 $S \leftarrow S2 + Q * S1; \quad S2 \leftarrow S1; \quad S1 \leftarrow S; \quad S2 = x^5 + 1 \quad S1 = x^6 + x^5 + x^4 + x^1 + 1$

И на последнем шаге получаем  $S = S2 + Q * S1 = x^7 + x^5 + x^4 + x^2$

Таким образом {b4} это обратный элемент по умножению от {11}

**2. Выполняем аффинное преобразование над полем GF(2) над обратным элементом полученным выше.**

|    |   |                   |
|----|---|-------------------|
| c0 | = | (1 0 0 0 1 1 1 1) |
| c1 | = | (1 1 0 0 0 1 1 1) |
| c2 | = | (1 1 1 0 0 0 1 1) |
| c3 | = | (1 1 1 1 0 0 0 1) |
| c4 | = | (1 1 1 1 1 0 0 0) |
| c5 | = | (0 1 1 1 1 1 0 0) |
| c6 | = | (0 0 1 1 1 1 1 0) |
| c7 | = | (0 0 0 1 1 1 1 1) |

$\cdot$

|   |   |   |   |   |   |   |   |
|---|---|---|---|---|---|---|---|
| 0 | 1 | 1 | 0 | 1 | 0 | 1 | 0 |
| 1 | 1 | 1 | 1 | 0 | 0 | 0 | 1 |
| 1 | 0 | 1 | 1 | 1 | 0 | 0 | 0 |
| 0 | 1 | 0 | 1 | 1 | 1 | 0 | 0 |
| 1 | 1 | 0 | 1 | 1 | 1 | 0 | 0 |
| 1 | 1 | 1 | 0 | 1 | 1 | 0 | 0 |
| 0 | 1 | 1 | 1 | 1 | 0 | 0 | 0 |
| 1 | 0 | 0 | 1 | 1 | 1 | 1 | 1 |

$\oplus$

$=$

|   |   |   |   |   |   |   |   |
|---|---|---|---|---|---|---|---|
| 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |
| 1 | 0 | 0 | 1 | 0 | 0 | 0 | 1 |
| 1 | 0 | 0 | 1 | 0 | 0 | 0 | 1 |
| 1 | 0 | 0 | 1 | 0 | 0 | 0 | 1 |
| 1 | 0 | 0 | 1 | 0 | 0 | 0 | 1 |
| 1 | 0 | 0 | 1 | 0 | 0 | 0 | 1 |
| 1 | 0 | 0 | 1 | 0 | 0 | 0 | 1 |
| 1 | 0 | 0 | 1 | 0 | 0 | 0 | 1 |

$\oplus$

|   |   |   |   |   |   |   |   |
|---|---|---|---|---|---|---|---|
| 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |
| 1 | 0 | 0 | 1 | 0 | 0 | 0 | 1 |
| 1 | 0 | 0 | 1 | 0 | 0 | 0 | 1 |
| 1 | 0 | 0 | 1 | 0 | 0 | 0 | 1 |
| 1 | 0 | 0 | 1 | 0 | 0 | 0 | 1 |
| 1 | 0 | 0 | 1 | 0 | 0 | 0 | 1 |
| 1 | 0 | 0 | 1 | 0 | 0 | 0 | 1 |
| 1 | 0 | 0 | 1 | 0 | 0 | 0 | 1 |

$\oplus$

|   |   |   |   |   |   |   |   |
|---|---|---|---|---|---|---|---|
| 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |
| 1 | 0 | 0 | 1 | 0 | 0 | 0 | 1 |
| 1 | 0 | 0 | 1 | 0 | 0 | 0 | 1 |
| 1 | 0 | 0 | 1 | 0 | 0 | 0 | 1 |
| 1 | 0 | 0 | 1 | 0 | 0 | 0 | 1 |
| 1 | 0 | 0 | 1 | 0 | 0 | 0 | 1 |
| 1 | 0 | 0 | 1 | 0 | 0 | 0 | 1 |
| 1 | 0 | 0 | 1 | 0 | 0 | 0 | 1 |

$\oplus$

|   |   |   |   |   |   |   |   |
|---|---|---|---|---|---|---|---|
| 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |
| 1 | 0 |   |   |   |   |   |   |



Проверка обратного элемента:

$$\begin{aligned}
 B &= x^4 + 1 \\
 S &= x^7 + x^5 + x^4 + x^2 \\
 A &= x^8 + x^4 + x^3 + x + 1 \\
 (x^4 + 1) \mid (x^7 + x^5 + x^4 + x^2) &= x^{11} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^2 \\
 &\quad - \underline{x^{11} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^2} \\
 &\quad \quad \quad \underline{x^8 + x^2 + x^5 + x^3 + x^2} \\
 &\quad \quad \quad \underline{x^8 + x^5 + x^4 + x^2 + x} \\
 &\quad \quad \quad \quad \quad \underline{x^2 + x^4 + x^3 + x} \\
 &\quad \quad \quad \quad \quad \underline{x^2 + x^4 + x^3 + x + 1} \\
 &\quad \quad \quad \quad \quad \quad \quad \quad 1
 \end{aligned}$$

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

##### 5. Shift Rows:

|    |    |    |    |                    |    |    |    |    |
|----|----|----|----|--------------------|----|----|----|----|
| 34 | a6 | 1b | 88 | Shift<br>Rows<br>→ | 34 | a6 | 1b | 88 |
| 1b | a6 | 93 | cc |                    | a6 | 93 | cc | 1b |
| 07 | a7 | ee | 6a |                    | ee | 6a | 07 | a7 |
| 66 | fb | 47 | dc |                    | dc | 66 | fb | 47 |

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

|             |             |                |  |  |
|-------------|-------------|----------------|--|--|
| 34 a6 1b 88 | ab f5 85 c6 | Mix<br>Columns | Операция MixColumns применяется последовательно к каждому столбцу блока. Это преобразование может быть представлено в матричном виде.<br>На рисунке a – вектор из 4 байт блока, b – вектор результата. | $\begin{bmatrix} b_3 \\ b_2 \\ b_1 \\ b_0 \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix}$ |
| a6 93 cc 1b | 96 43 6a 0b |                |  |  |
| ee 6a 07 a7 | 2a 4b cf 0f |                |  |  |
| dc 66 fb 47 | b7 c4 0b b1 |                |  |  |

$$\begin{bmatrix} B0 \\ B1 \\ B2 \\ B3 \end{bmatrix} = \begin{bmatrix} \{02\} & \{03\} & \{01\} & \{01\} \\ \{01\} & \{02\} & \{03\} & \{01\} \\ \{01\} & \{01\} & \{02\} & \{03\} \\ \{03\} & \{01\} & \{01\} & \{02\} \end{bmatrix} \cdot \begin{bmatrix} \{88\} \\ \{1b\} \\ \{a7\} \\ \{47\} \end{bmatrix} = \begin{bmatrix} \{02\} \cdot \{88\} \oplus \{03\} \cdot \{1b\} \oplus \{01\} \cdot \{a7\} \oplus \{01\} \cdot \{47\} \\ \{01\} \cdot \{88\} \oplus \{02\} \cdot \{1b\} \oplus \{03\} \cdot \{a7\} \oplus \{01\} \cdot \{47\} \\ \{01\} \cdot \{88\} \oplus \{01\} \cdot \{1b\} \oplus \{02\} \cdot \{a7\} \oplus \{03\} \cdot \{47\} \\ \{03\} \cdot \{88\} \oplus \{01\} \cdot \{1b\} \oplus \{01\} \cdot \{a7\} \oplus \{02\} \cdot \{47\} \end{bmatrix}$$

Вычисление элемента B0 вектора B

$\{02\} \cdot \{88\} = (x^1) \cdot (x^7 + x^3) = x^8 + x^4 \mod (x^8 + x^4 + x^3 + x^1 + 1) = x^3 + x^1 + 1 = \{00001011\} = \{0b\}$   
 $\{03\} \cdot \{1b\} = (x^1 + 1) \cdot (x^4 + x^3 + x^2 + x^1 + 1) = x^5 + x^3 + x^2 + 1 = \{00101101\} = \{2d\}$   
 $\{01\} \cdot \{a7\} = \{10100111\} = \{a7\}$   
 $\{01\} \cdot \{47\} = \{01000111\} = \{47\}$   
 $\{0b\} = \{00001011\}$   
 $\oplus \{2d\} = \{00101101\}$   
 $\oplus \{a7\} = \{10100111\}$   
 $\oplus \{47\} = \{01000111\}$   
 $B0 = \{11000110\} = \{c6\}$

Вычисление элемента B1 вектора B

$\{01\} \cdot \{88\} = \{10001000\} = \{88\}$   
 $\{02\} \cdot \{1b\} = (x^1) \cdot (x^4 + x^3 + x^2 + x^1 + 1) = x^5 + x^4 + x^2 + x^1 = \{00110110\} = \{36\}$   
 $\{03\} \cdot \{a7\} = (x^1 + 1) \cdot (x^7 + x^5 + x^2 + x^1 + 1) = x^8 + x^7 + x^6 + x^5 + x^3 + 1 \mod (x^8 + x^4 + x^3 + x^1 + 1) = x^7 + x^6 + x^5 + x^4 + x^1 = \{11110010\} = \{f2\}$   
 $\{01\} \cdot \{47\} = \{01000111\} = \{47\}$   
 $\{88\} = \{10001000\}$   
 $\oplus \{36\} = \{00110110\}$   
 $\oplus \{f2\} = \{11110010\}$   
 $\oplus \{47\} = \{01000111\}$   
 $B1 = \{00001011\} = \{0b\}$

Вычисление элемента B2 вектора B

$\{01\} \cdot \{88\} = \{10001000\} = \{88\}$   
 $\{01\} \cdot \{1b\} = \{00011011\} = \{1b\}$   
 $\{02\} \cdot \{a7\} = (x^1) \cdot (x^7 + x^5 + x^2 + x^1 + 1) = x^8 + x^6 + x^3 + x^2 + x^1 \mod (x^8 + x^4 + x^3 + x^1 + 1) = x^6 + x^4 + x^2 + 1 = \{01010101\} = \{55\}$   
 $\{03\} \cdot \{47\} = (x^1 + 1) \cdot (x^6 + x^2 + x^1 + 1) = x^7 + x^6 + x^3 + 1 = \{11001001\} = \{c9\}$   
 $\{88\} = \{10001000\}$   
 $\oplus \{1b\} = \{00011011\}$   
 $\oplus \{55\} = \{01010101\}$   
 $\oplus \{c9\} = \{11001001\}$   
 $B2 = \{00001111\} = \{0f\}$

Вычисление элемента B3 вектора B

$\{03\} \cdot \{88\} = (x^1 + 1) \cdot (x^7 + x^3) = x^8 + x^7 + x^4 + x^3 \mod (x^8 + x^4 + x^3 + x^1 + 1) = x^7 + x^1 + 1 = \{10000011\} = \{83\}$   
 $\{01\} \cdot \{1b\} = \{00011011\} = \{1b\}$   
 $\{01\} \cdot \{a7\} = \{10100111\} = \{a7\}$   
 $\{02\} \cdot \{47\} = (x^1) \cdot (x^6 + x^2 + x^1 + 1) = x^7 + x^3 + x^2 + x^1 = \{10001110\} = \{8e\}$   
 $\{83\} = \{10000011\}$   
 $\oplus \{1b\} = \{00011011\}$   
 $\oplus \{a7\} = \{10100111\}$   
 $\oplus \{8e\} = \{00001111\}$   
 $B3 = \{00001111\} = \{0f\}$

## 7. Нулевой ключ:

Текущий ключ: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

### 1-ый раунд:

01 раунд: 62636363 62636363 62636363 62636363

|    |    |    |    |
|----|----|----|----|
| a3 | a4 | 5d | ab |
| f5 | a4 | 10 | 80 |
| 5a | ac | 5d | de |
| ce | a9 | 53 | 31 |

2-ой раунд:

02 раунд: 9b9898c9 f9fbfbba 9b9898c9 f9fbfbba

|    |    |    |    |
|----|----|----|----|
| 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:

|               |   |
|---------------|---|
| Блок данных : | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |
|---------------|---|

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:

|               |  |
|---------------|--|
| Блок данных : | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 |
|---------------|--|

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 блочном 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.