ФЕДЕРАЛЬНОЕ АГЕНТСТВО 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 № 5

**Моделирование базового алгоритма шифрования ГОСТ Р34.12-2015**

**с длиной блока 64 бита**

**Вариант 14**

Выполнил: ст. гр. ИКТЗ-83

Мазеин Д.С.

Проверил: Яковлев В.А.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Цель лабораторной работы:

* Операции криптографических преобразования для двух раундов алгоритма шифрования согласно ГОСТ Р34-12-2015
* Представить результаты промежуточных вычислений и результат шифрования после второго раунда в двоичной и шестнадцатеричной формах

**Выполнение работы:**



Таблица 1. Раундовые подключи

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Ко** | 7 | 15 | 1 | 5 | 4 | 12 | 11 | 10 |
| **К1** | 3 | 14 | 5 | 0 | 9 | 7 | 5 | 4 |
| **К2** | 11 | 4 | 6 | 10 | 7 | 1 | 12 | 3 |
| **К3** | 2 | 1 | 8 | 4 | 12 | 9 | 7 | 5 |
| **К4** | 5 | 3 | 13 | 10 | 9 | 6 | 4 | 1 |
| **К5** | 1 | 0 | 4 | 8 | 5 | 9 | 3 | 14 |
| **К6** | 13 | 11 | 5 | 2 | 1 | 6 | 9 | 8 |
| **К7** | 8 | 12 | 9 | 7 | 6 | 3 | 2 | 1 |

Таблица 2. Подстановки

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Адрес** | **S1** | **S2** | **S3** | **S4** | **S5** | **S6** | **S7** | **S8** |
| **0** | 7 | 1 | 11 | 9 | 15 | 8 | 10 | 7 |
| **1** | 12 | 6 | 5 | 14 | 4 | 2 | 5 | 0 |
| **2** | 0 | 10 | 7 | 0 | 12 | 4 | 0 | 9 |
| **3** | 5 | 5 | 14 | 13 | 11 | 11 | 12 | 5 |
| **4** | 14 | 7 | 4 | 15 | 5 | 7 | 13 | 12 |
| **5** | 3 | 9 | 3 | 3 | 8 | 12 | 2 | 6 |
| **6** | 9 | 12 | 13 | 5 | 2 | 13 | 7 | 10 |
| **7** | 10 | 3 | 0 | 8 | 1 | 1 | 9 | 3 |
| **8** | 1 | 13 | 8 | 6 | 10 | 5 | 4 | 8 |
| **9** | 11 | 8 | 6 | 11 | 9 | 15 | 3 | 11 |
| **10** | 15 | 0 | 2 | 10 | 6 | 3 | 11 | 15 |
| **11** | 6 | 15 | 9 | 7 | 0 | 6 | 6 | 2 |
| **12** | 4 | 14 | 15 | 1 | 3 | 14 | 14 | 1 |
| **13** | 8 | 2 | 10 | 4 | 14 | 9 | 8 | 13 |
| **14** | 2 | 11 | 1 | 12 | 13 | 0 | 1 | 4 |
| **15** | 13 | 4 | 12 | 2 | 7 | 10 | 15 | 14 |

**Исходное сообщение**

8.3.0.4.8.3.0.4. 8.3.0.4.8.3.0.4.

0100 0000 0011 1000 0100 0000 0011 1000 N2

**4 0 3 8 4 0 3 8**

0100 0000 0011 1000 0100 0000 0011 1000 N1

**4 0 3 8 4 0 3 8**

[ + ] mod 232

0111 1111 0001 0101 0100 1100 1011 1010 Ко

**7 15(F) 1 5 4 12(C) 11(B) 10(A)**

**---------------------------------------------------------**

0011 1111 0100 1101 1000 1100 1111 0010 на вых. СМ mod232

**3 15(F) 4 13(D) 8 12(C) 15(F) 2**

0101 0100 0100 0001 1010 1110 1111 1001 из узла замены

**5 4 4 1 10 14(E) 15(F) 9**

0000 1101 0111 0111 1100 1010 1010 0010 на вых.рег. сдвига

на 11 разрядов

( + ) mod2

0100 0000 0011 1000 0100 0000 0011 1000 N2

0100 1101 0100 1111 1000 1010 1001 1010 на вых. СМ mod2 и в N1

**4 13(D) 4 15(F) 8 10(A) 9 10(A)**

0100 0000 0011 1000 0100 0000 0011 1000 N2

**2-й раунд аналогично**

0100 0000 0011 1000 0100 0000 0011 1000 N2

**4 0 3 8 4 0 3 8**

0100 1101 0100 1111 1000 1010 1001 1010 N1

**4 13(D) 4 15(F) 8 10(A) 9 10(A)**

[ + ] mod 232

0011 1110 0101 0000 1001 0111 0101 0100 К1

**3 14(E) 5 0 9 7 5 4**

**---------------------------------------------------------**

0000 1011 1010 0000 0010 0001 1110 1110 на вых. СМ mod232

**0 11(B) 10(A) 0 2 1 14(E)14(E)**

0111 1111 0010 1001 1100 0010 0001 0100 из узла замены

**7 15(F) 2 9 12(C) 2 1 4**

0100 1110 0001 0000 1010 0011 1111 1001 на вых.рег. сдвига

на 11 разрядов

( + ) mod2

0100 0000 0011 1000 0100 0000 0011 1000 N2

0000 1110 0010 1000 1110 0011 1100 0001 на вых. СМ mod2 и в N1

**0 14(E) 2 8 14(E) 3 12(C) 1**

0100 1101 0100 1111 1000 1010 1001 1010  **N2**