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

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **К1** | 7 | 15 | 1 | 5 | 4 | 12 | 11 | 10 |
| **К2** | 3 | 14 | 5 | 0 | 9 | 7 | 5 | 4 |

Таблица 2. Подстановки

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Вход** | **π0** | **π1** | **π2** | **π3** | **π4** | **π5** | **π6** | **π7** |
| **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 |

1-й раунд:

Исходное сообщение: 8.3.1.4.8.3.1.4. 8.3.1.4.8.3.1.4.

0100 0001 0011 1000 0100 0001 0011 1000 N2

4 1 3 8 4 1 3 8

0100 0001 0011 1000 0100 0001 0011 1000 N1

4 1 3 8 4 1 3 8

[+]

0111 1111 0001 0101 0100 1100 1011 1010 K1

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

------------------------------------------------------

1100 0000 0100 1101 1000 1101 1111 0010 на вых. СМ

12(C) 0 4 13(D) 8 13(D) 15(F) 2

0100 0001 0100 0100 1010 1001 1111 1001 из узла подстановок

4 1 4 4 10(A) 9 15(F) 9

0010 0101 0100 1010 0000 0010 0000 1010 на вых. рег. сдвига

[+]

0100 0001 0011 1000 0100 0001 0011 1000 N2

0110 0100 0111 0010 0100 0011 0011 0010 на вых. СМ и в N1  
 6 4 7 2 4 3 3 2

0100 0001 0011 1000 0100 0001 0011 1000 N2

2-й раунд:

0100 0001 0011 1000 0100 0001 0011 1000 N2

4 1 3 8 4 1 3 8

0110 0100 0111 0010 0100 0011 0011 0010 N1

6 4 7 2 4 3 3 2

[+]

0011 1110 0101 0000 1001 0111 0101 0100 K2

3 14(E) 5 0 9 7 5 4

-----------------------------------------------------

1010 0010 1100 0010 1101 1010 1000 0110 на вых. СМ

10(А) 2 12(C) 2 13(D) 10(А) 8 6

1111 1010 1111 0000 1110 0011 0100 1010 из узла подстановок

15(F) 10(A) 15(F) 0 14(E) 3 4 10(A)

1000 0111 0001 1010 0101 0111 1101 0111 на вых. рег. Сдвига

[+]

0100 0001 0011 1000 0100 0001 0011 1000 N2

1100 0110 0010 0010 0001 0110 1110 1111‬ на вых. СМ и в N1

12(C) 6 2 2 1 6 14(E) 15(F)

0100 0001 0011 1000 0100 0001 0011 1000 N2