**МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ**

**Федеральное государственное бюджетное образовательное**

**учреждение высшего образования**

**«Санкт-Петербургский государственный университет телекоммуникаций**

**им. проф. М. А. Бонч-Бруевича»**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

Кафедра «Защищенные системы связи»

Дисциплина «Основы криптографии с открытыми ключами»

# Лабораторная работа № 6

**«Криптосистема Рабина»**

**4 вариант**

Выполнил: Громов А. А.

ИКТЗ-83

Проверил: Яковлев В. А.

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

Санкт-Петербург

2021

**Цель работы**

Закрепить знания, полученные на лекциях по теме “Криптосистема Рабина”.

**Задание**

1.Выполнить упражнения по расшифрованию криптограммы, полученной в криптосистеме Рабина.

2.Зашифровать сообщение в криптосистеме Рабина.

**Порядок**

1. Выбрать вариант задания в табл 1.
2. Зашифровать сообщение табл. 1
3. Расшифровать криптограмму табл.2

Таблица1

|  |  |  |  |
| --- | --- | --- | --- |
| № | p | q | M |
| 4 | 31 | 11 | 480 |

n = p\*q = 31\*11 = 341

480 = 256+128+64+32 = 111100000

480=256+224

*Для проверки расшифруем получившуюся криптограмму:*

*p* = 4\*7+3 => используем формулу:

*q* = 4\*2+3 => используем формулу:

НОД(31, 11):

31 = 11\*2+ 9

11 = 9\*1+ 2

9 = 2\*4 + 1

Расширенный алгоритм Евклида:

1 = 9 – 4\*2

2 = 11 – 9\*1

9 = 31 – 11\*2

1 = 9 – (11 – 9\*1)\*4 = 9\*5 – 4\*11 = 5\*(31 – 11\*2) – 4\*11 = 5\*31 – 14\*11

Можно видеть, что:

1. **Расшифровать криптограмму**

Исходные данные: *p* = 23, *q* = 7, *M* = 144, *С* = 128

*p* = 4\*5+3 => используем формулу:

*p* = 4\*1+3 => используем формулу:



НОД(23, 7):

23 = 7\*3+ 2

7 = 2\*3+ 1

2 = **1**\*2 + 0

Расширенный алгоритм Евклида:

1 = 7 – 2\*3

2 = 23 – 7\*3

1 = 7 – (23 – 7\*3)\*3 = –3\*23 + 10\*7

Можно видеть, что:

Примечание 1. Если сообщение меньше модуля, то сообщение необходимо разбить на две части путем представления сообщения в двоичном виде.

Таблица2

|  |  |  |
| --- | --- | --- |
| № | М | С |
| 4 | 21 | 119 |

Примечание 2.

1. При расшифровании использовать ключи р=23, q=7 для вариантов с 1-26.
2. Перед расшифрованием проверить есть ли решение у задачи.
3. После расшифрования сверить расшифрованное сообщение с исходным по табл.