**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 |

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.