|  |  |
| --- | --- |
|  | |
| МИНОБРНАУКИ РОССИИ | |
| Федеральное государственное бюджетное образовательное учреждениевысшего профессионального образования"Российский технологический университет"МИРЭА | |
| Институт информационных технологий (ИТ) |  |
| Кафедра ВТ |  |

|  |  |
| --- | --- |
| **ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №4** | |
| **по дисциплине** | |
| **«Защита информации»** | |
|  | |
| Выполнил студент группы ИВБО-01-15 | Пушкарев Е.В. |
| Принял | Воронков С. О. |

|  |  |  |
| --- | --- | --- |
| Лабораторные работы выполнены | «\_\_»\_\_\_\_\_\_\_201\_\_ г. |  |
|  |  |  |
| «Зачтено» | «\_\_»\_\_\_\_\_\_\_201\_\_ г. |  |

Москва 2018

**Задание:**

Разработать программу, осуществляющую передачу сообщений по протоколу RSA на примере общения двух собеседников.

**Решение:**

При работе алгоритма:.

1. Выбираются простые большие P и Q
2. Вычисляется N = P \* Q
3. Вычисляется вспомогательное число f = (P – 1) \* (Q – 1)
4. Выбирается случайное d, такое что d < f, d и f взаимно простые (не имеют общих делителей кроме 1).
5. Вычисляется e, такое что e \* d mod f = 1.
6. Для каждого блока сообщения (M = M1M2…Mn) находится Ci = Mi^d mod N.
7. Собеседник передает массив зашифрованных блоков Ci
8. Переданное сообщение расшифровывается Mi = Ci ^ e mod N.

**Вывод:**

После выполнения описанного алгоритма было передано и расшифровано одно и то же сообщение по протоколу RSA.

**Ссылка на git-репозиторий:**

https://github.com/Kefir103/CryptLabRSA