|  |  |  |  |
| --- | --- | --- | --- |
|  | |  |  |
| МИНОБРНАУКИ РОССИИ | | | |
| Федеральное государственное бюджетное образовательное учреждениевысшего образования«МИРЭА – Российский технологический университет»РТУ МИРЭА | | | |
| **ИНСТИТУТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ**  **КАФЕДРА ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ** | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ОТЧЁТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №4** | | | |
| **по дисциплине** | | | |
| **«Защита информации»** | | | |
| Выполнил студент группы ИВБО-01-15 | | Шлыков А.В. | |
| Принял | | Воронков С.О. | |
| Работа представлена к защите | «\_\_»\_\_\_\_\_\_\_201\_ г. | | *(подпись студента)* |
| «Допущен к защите» | «\_\_»\_\_\_\_\_\_\_201\_г. | | *(подпись руководителя)* |

Москва 2018

**Задание:**

Разработать программу, реализующую алгоритм RSA

**Решение:**

Генерируется простое число P: 211

Генерируется второе простое число Q: 977

Вычисляется N= 210367

Вычисляется f= 209160

Вычисляется d= 128297

Вычисляется e= 53033

Вводится сообщение: 12345 и отправляется на сервер

Сервер получает закодированное сообщение ['1', '25377', '183329', '58742', '115319'] e=53033и N=210367. И расшифровывает его

Клиент получает ['1', '2', '3', '4', '5']

**Вывод:**

Клиент и сервер успешно сгенерировали одинаковые ключи и проверили их, не обмениваясь ими.