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

|  |  |
| --- | --- |
| **ОТЧЁТ ПО ЛАБОРАТОРНЫМ РАБОТАМ** | |
| **по дисциплине** | |
| **«Защита информации»** | |
|  | |
| Выполнил студент группы ИВБО-01-15 | Поляков И.С. |
| 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: 11

Генерируется второе простое число Q: 13

Вычисляется N= 143

Вычисляется f= 120

Вычисляется d= 97

Вычисляется e= 433

Вводится сообщение: 567 и отправляется на сервер

Сервер получает закодированное сообщение =['135', '19', '72'], e=433 и N=143. И расшифровывает его

Клиент получает ['5', '6', '7']

**Вывод:**

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