|  |
| --- |
| Описание: https://lh6.googleusercontent.com/QcftzNtI05T0Y6fjdSh1Rr2rt8oqZ1IvnLvbn1jLJ7CCyteVir3k-xBLv4SL1wAgWJsRhmmJSR0UW-RP63_GQenE4vVWv05BRoZTsmIcBccVTnfxwmsnNMvjg599x9SqZd8E3dkd |
| МИНОБРНАУКИ РОССИИ |
| Федеральное государственное бюджетное образовательное учреждениевысшего образования"МИРЭА - Российский технологический университет"РТУ МИРЭА |

Институт информационных технологий

Кафедра вычислительной техники

**ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №4**

**по дисциплине**

**«Защита информации»**

Студент группы ИВБО-07-15 Боязитов И. Э.

Принял Воронков С. О.

Москва 2018

Постановка задачи:

Разработать программу, реализующую алгоритм RSA.

Ход выполнения работы:

1. Создаются два объекта класса Клиент (Алиса и Боб).
2. Боб получает сгенерированный Алисой ее публичный ключ, который он использует для шифрования своего сообщения, причем сообщение шифруется блоками, где в качестве блока используется код символа из Unicode. Зашифрованное сообщение отсылается Алисе.
3. Алиса расшифровывает полученное сообщение своим закрытым ключом.

Вывод:

Алгоритм работает корректно, сообщение успешно зашифровывается и расшифровывается.