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

|  |  |
| --- | --- |
| **ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №4** | |
| **по дисциплине** | |
| «Защита информации» | |
|  | |
| Выполнил студент группы ИВБО-04-15  Принял | Камаев А. А.  Воронков С. О. |
|  |  |

|  |  |  |
| --- | --- | --- |
| Лабораторная работа выполнена | «\_\_»\_\_\_\_\_\_\_201\_\_ г. | *\_\_\_\_\_\_\_\_\_\_\_\_\_\_* |
|  |  |  |
| «Зачтено» | «\_\_»\_\_\_\_\_\_\_201\_\_ г. | *\_\_\_\_\_\_\_\_\_\_\_\_\_\_* |

Москва 2018

Постановка задачи

Разработать клиент-серверное приложение, реализующую алгоритм шифрования RSA.

Ход выполнения работы

1) Разработана пара программ (клиент-сервер). Сервер получает от клиента слова, которые объединяются в одну строку. При получении от клиента сообщения “SEND” сервер отправляет клиенту строку. При получении “CLEAR” – очищает её.

2) Разработаны методы, реализующие шифровку/дешифровку сообщений при помощи алгоритма RSA. При подключении клиента, сервер вычисляет отправляет ему пару открытых ключей. Клиент отправляет зашифрованное этими ключами сообщение, и, заодно, отправляет пару своих открытых ключей (для ответа сервера). Сервер расшифровывает сообщение закрытым ключом и использует открытые ключи клиента для отправки следующего сообщения. После каждого сообщения генерируются две новых пары ключей.

Вывод

Разработано клиент-серверное приложение, реализующее алгоритм RSA. Программа работает корректно, все данные передаются без потерь.