|  |  |  |
| --- | --- | --- |
|  | |  |
| 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 №2** | |
| **по дисциплине** | |
| «Защита информации» | |
|  | |
| Выполнил студент группы ИВБО-04-15  Принял | Афатов Д. В.  Воронков С. О. |
|  |  |

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

Москва 2018

Постановка задачи:

Разработать программу, реализующую алгоритм Диффи-Хелмана. Результат выполнения алгоритма записать в текстовый файл.

Ход выполнения:

Было написано клиент-серверное приложение, использующее интерфейс, базирующийся на Swing. Для наглядности данных, которые передаются через внешнюю среду и доступны не только пользователям, участвующие в передаче данных, была реализована «внешняя среда» отображающая в логе интерфейса всю информацию, что проходит передачу. В результате вся передача данных между клиентом и другим клиентом происходит через «внешнюю среду». Клиент может передавать сообщения другому клиенту после установки соединения, при котором вычисляется общий ключ шифрования именно алгоритмом Диффи-Хелмана. Сообщение кодируется обычным шифром Цезаря. «Внешняя среда» и каждый из клиентов ведет лог.

Вывод:

Разработанная программа работает корректно. Закрытые ключи сходятся.