|  |  |  |
| --- | --- | --- |
|  | |  |
| 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 | Бахирко В. А.  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 работы

1) Написание класса Test4

Инициализируем переменные.

2) Создание основных формул.

Y1 = (int) Math.pow(A, x1) % P;

Y2 = (int) Math.pow(A, x2) % P;

Z1 = (int) Math.pow(Y2, x1) % P;

Z2 = (int) Math.pow(Y1, x2) % P;

3) Вывод в лог.   
 log.txt

Вывод

Разработана программа, реализующая алгоритм Диффи-Хеллмана. Программа работает корректно, закрытые ключи сходятся. Cделана программа в IntelliJ IDEA 2018.