|  |  |  |
| --- | --- | --- |
|  | |  |
| 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 | Камаев А. 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 User

В данном классе описаны методы для вычислений и передачи информации.

2) Создание текстового файла, содержащего множество значений числа P:

В текстовый файл “Число P” заносятся возможные значения, каждое находится на новой строке.

3) Написание метода main

3.1 В этом методе определены:

- значение числа P (выбирается случайно из файла “Число P.txt”);

- значение числа A (выбирается случайным образом, 1 < A < P – 1);

- значения X1 и X2 (выбираются случайным образом).

3.2 Описан процесс записи в текстовый файл:

Результаты вычислений и передачи информации между пользователями записываются в файл “log.txt”.

Вывод

Разработана программа, реализующая алгоритм Диффи-Хеллмана. Программа работает корректно, закрытые ключи сходятся.