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

|  |  |
| --- | --- |
| **ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №2** | |
| **по дисциплине** | |
| **«Защита информации»** | |
|  | |
| Выполнил студент группы ИВБО-01-15 | Пушкарев Е.В. |
| Принял | Воронков С. О. |

|  |  |  |
| --- | --- | --- |
| Лабораторные работы выполнены | «\_\_»\_\_\_\_\_\_\_201\_\_ г. |  |
|  |  |  |
| «Зачтено» | «\_\_»\_\_\_\_\_\_\_201\_\_ г. |  |

Москва 2018

**Задание:**

Разработать программу, реализующую алгоритм согласования ключей Диффи-Хеллмана на примере общения двух абонентов.

**Решение:**

При работе алгоритма:

1. Вместе с собеседником устанавливает одинаковые значения P, которое является простым числом и A (1 < A < P-1)
2. Собеседники генерируют закрытые ключи X
3. Собеседники вычисляют значения Y = Ax mod P
4. Происходит обмен между собеседниками значениями Y
5. Собеседники вычисляют значения K=Yx mod P (где Y – значение, принятое собеседником)
6. Если К совпадают, то значения, установленные собеседником - верны

**Вывод:**

После выполнения описанного алгоритма абоненты получили один и тот же ключ.

**Ссылка на git-репозиторий:**

https://github.com/Kefir103/CryptLab2