|  |  |  |  |
| --- | --- | --- | --- |
|  | |  |  |
| МИНОБРНАУКИ РОССИИ | | | |
| Федеральное государственное бюджетное образовательное учреждениевысшего образования«МИРЭА – Российский технологический университет»РТУ МИРЭА | | | |
| **ИНСТИТУТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ**  **КАФЕДРА ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ** | | | |

|  |  |
| --- | --- |
| **ОТЧЁТ ПО ЛАБОРАТОРНЫМ РАБОТАМ** | |
| **по дисциплине** | |
| **«Защита информации»** | |
|  | |
| Выполнил студент группы ИВБО-01-15 | Поляков И.С. |
| Принял | Воронков С.О. |
|  |  |
|  |  |

|  |  |  |
| --- | --- | --- |
| Работа представлена к защите | «\_\_»\_\_\_\_\_\_\_201\_ г. | *(подпись студента)* |
|  |  |  |
| «Допущен к защите» | «\_\_»\_\_\_\_\_\_\_201\_г. | *(подпись руководителя)* |

Москва 2018

**Задание:**

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

**Решение:**

|  |
| --- |
| 1. Генерируется число для расчёта P = 11 |
| 1. Генерируется А, такое что 1<A<10 А = 5 |
| 1. Пользователь 1 генерирует секретное число 9 |
| 1. Пользователь 1 вычисляет y1 = 9 |
| 1. Пользователь 2 генерирует секретное число 8 |
| 1. Пользователь 2 вычисляет y2 = 4 |
| 1. Пользователи обмениваются y |
| 1. Пользователь 1 считает ключ 3 |
| 1. Пользователь 2 считает ключ 3 |
| 1. Ключи равны |

**Вывод:**

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