|  |  |  |  |
| --- | --- | --- | --- |
|  | |  |  |
| 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 srp-6

**Решение:**

Вводим простое число: 11

Вводим имя пользователя: user

Вводим пароль: password

Генерируется генератор g = 11

Генерируется x= 9

Генерируется v= 2

I,s,v,N отправляются на сервер

Сервер сохраняет данные

Генерируется a= 21

Вычисляется A=g^a mod N= 21

Отправляется на сервер I,A

Сервер вычисляет b=219 и B=27.000000 и отправляет их клиенту

Обе стороны вычисляют U=h(A,B)= 4

Обе стороны вычисляют K=h(((B-k\*(g^x mod N))^a+u\*x) mod N = 1

Обе стороны вычисляют M= 8 и обмениваются информацией. Данные совпадают, значит ключи сгенерированы корректно

**Вывод:**

Клиент и сервер успешно сгенерировали одинаковые ключи и проверили их, не обмениваясь ими.