Лабораторная работа №17

Реализация протокола Диффи-Хеллмана

Цель: Приобрести практические навыки в реализации криптографических протоколов распределения ключей

Введение

Первым протоколом открытого распределения ключей был протокол Диффи-Хеллмана.

Пусть - простое число; - примитивный элемент группы GF(p); - сеансовый ключ. Тогда протокол имеет следующий вид:

1.

2.

3.

Однако стоит помнить, что данный протокол обладает уязвимостью перед атакой "человек по середине". Поэтому необходимо производить аутентификацию сторон.

1. Рабочее задание

1.1 Реализовать протокол Диффи-Хеллмана

2. Требования к реализации

2.1 Для реализации пользователей используются виртуальные машины между которыми установлено сетевое соединение.

2.2 Должна быть предусмотрена процедура генерации параметров.

2.3 Ключ и промежуточные значения параметров должны записываться в файлы абонентов.

Подписать исходный код своей электронной подписью, выслать на адрес ladg91@mail.ru с темой lab17, после получения подписанного преподавателем исходного кода, прийти и защитить его.