Лабораторная работа №16

Реализация протокола передачи ключа

Цель: Приобрести практические навыки в реализации криптографических протоколов распределения ключей

Введение

Для передачи сеансовых ключей симметричных шифров могут использоваться асимметричные шифры. Рассмотрим протокол аутентифицированной передачи секретного ключа

Пусть - сеансовый ключ; - открытый ключ ассиметричного шифра пользователя B; - цифровая подпись пользователя A. Тогда протокол имеет следующий вид:

1. Рабочее задание

1.1 Реализовать протокол передачи ключа на основе ассиметричного шифра.

2. Требования к реализации

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

2.2 Используется шифр RSA из лабораторной работы №3.

2.3 Используется подпись RSA из лабораторной работы №7.

2.4 Для цифровой подписи используется хеш-функция SHA-512 из лабораторной работы №5.

2.5 Доверенным центром для цифровой подписи выступает сам подписывающий абонент.

2.6 Сеансовый ключ представляет собой 256 битовую случайную последовательность. Реализовать генерацию последовательности (можно использовать встроенный генератор случайных чисел). Ключ должен записываться в файл у отправителя при его генерации и должен записываться в файл у получателя при его получении.

2.7 Нельзя использовать готовые реализации шифра, цифровой подписи RSA и хеш-функции SHA.

Подписать исходный код своей электронной подписью, выслать на адрес ladg91@mail.ru с темой lab16, после получения подписанного преподавателем исходного кода, прийти и защитить его.