Лабораторная работа №13

Протокол аутентификации на основе ассиметричного шифра

Цель: Приобрести практические навыки в реализации протоколов идентификации.

Введение

Еще один способ реализовать протокол идентификации основан на использовании ассиметричных шифров. Рассмотрим подобный протокол:

1.

2.

где – асимметричный алгоритм шифрования на открытом ключе пользователя ; – случайное число; – идентификатор пользователя .

1. Рабочее задание

1.1 Реализовать трехпроходный протокол идентификации.

2. Требования к реализации

2.1 Реализовать протокол на базе 2-х виртуальных машин – каждая машина представляет собой отдельного пользователя.

2.2 Использовать требования лабораторной работы №3.

2.3 Результат идентификации выводится на экран.

Подписать исходный код своей электронной подписью, выслать на адрес ladg91@mail.ru с темой lab13, после получения подписанного преподавателем исходного кода, прийти и защитить его.