Лабораторная работа №12

Трехпроходный протокол идентификации

Цель: Приобрести практические навыки в реализации протоколов идентификации.

Введение

Рассмотрим трехпроходный протокол идентификации, предложенный международной организацией по стандартизации:

1.

2.

3.

где – симметричный алгоритм шифрования на общем для пользователей ключе; – случайные числа; – идентификаторы пользователей ; – некоторые сообщения.

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 шифр AES для зашифрования данных. Разрешено использовать сторонние реализации данного шифра.

2.3 Ключ предварительно генерируется и пересылается между пользователями.

2.4 Предусмотреть возможность ввода сообщений .

2.5 Результат идентификации выводится на экран.

Подписать исходный код своей электронной подписью, выслать на адрес ladg91@mail.ru с темой lab12, после получения подписанного преподавателем исходного кода, прийти и защитить его.