Лабораторная работа №11

Двухпроходный протокол идентификации

Цель: Приобрести практические навыки в реализации протоколов идентификации.

Введение

Аутентификация в широком смысле обозначает установление подлинности. Протоколы идентификации – протоколы, позволяющие установить подлинность взаимодействующих сторон. Одним из решений для построения подобных протоколов является использование симметричных шифров. Рассмотрим двухпроходный протокол идентификации, предложенный международной организацией по стандартизации:

1.

2. ,

где – симметричный алгоритм шифрования на общем для пользователей ключе; – выбор между временной меткой , либо случайным числом ; – идентификаторы пользователей ; – некоторые сообщения.

1. Рабочее задание

1.1 Реализовать двухпроходный протокол идентификации.

2. Требования к реализации

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

2.2 Предусмотреть возможность выбора для идентификации временной метки или случайного числа.

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

2.4 Ключ предварительно генерируется и пересылается между пользователями.

2.5 Предусмотреть возможность ввода сообщений .

2.6 Временная метка представляется в формате аналогичном в CAdES.

2.7 Результат идентификации выводится на экран.

Подписать исходный код своей электронной подписью, выслать на адрес ladg91@mail.ru с темой lab11, после получения подписанного преподавателем исходного кода, прийти и защитить его.