Лабораторная работа №18

Реализация простого протокола экспоненциального распределения ключей

Цель: Приобрести практические навыки в реализации криптографических протоколов распределения ключей

Введение

Простой протокол экспоненциального распределения ключей (Simple Password Exponential Key Exchange, SPEKE) является модификацией протокола Диффи-Хеллмана, в котором используется процедура аутентификации на этапе формирования параметров.

Пусть - хеш-функция; - общий пароль пользователей. Тогда .

Стоит отметить, что в этом случае может не являться примитивным элементом.

1. Рабочее задание

1.1 Реализовать простой протокол экспоненциального распределения ключей

2. Требования к реализации

2.1 Дополнить реализацию лабораторной работы №17 возможностью использования парольной схемы из лабораторной работы №14.

2.2 Используется хеш-функция SHA-512 из лабораторной работы №5.

2.3 Нельзя использовать готовые реализации хеш-функции SHA.

Подписать исходный код своей электронной подписью, выслать на адрес ladg91@mail.ru с темой lab18, после получения подписанного преподавателем исходного кода, прийти и защитить его.