Лабораторная работа №15

Реализация протокола идентификации Фиата-Шамира

Цель: Приобрести практические навыки в реализации криптографических протоколов доказательства знания с нулевым разглашением

Введение

Доказательство знания (протокол доказательства знания) (proof of knowledge) – интерактивное доказательство, в котором доказывающий убеждает проверяющего в том, что он владеет секретной информацией. Протокол интерактивного доказательства должен учитывать возможность обмана со стороны обоих участников. Если участник А (доказывающий) на самом деле не знает доказываемого утверждения (либо от имени участника А выступает кто-либо другой), то участник В должен обнаружить факт обмана. Одним из таких протоколов является протокол Фиата-Шамира. Опишем данный протокол.

Пусть - доверенный центр, - доказывающий и проверяющий соответственно.

1.

, где и - достаточно большие простые числа.

2.

Итеративная процедура протокола:

3.1

3.2

3.3

3.4 . Если условие выполнено, то итерация завершена.

1. Рабочее задание

1.1 Реализовать протокол Фиата-Шамира.

2. Требования к реализации

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

2.2 Все входящие и исходящие данные на виртуальные машины должны фиксироваться.

2.3 Значения и генерируются случайно с помощью алгоритма генерации простых чисел. Размер и - 512 бит. Значения и должны выбираться случайно.

2.4 Протокол должен сделать 10 итерационных проходов.

2.5 После прохождения итерационных проходов должен выдаваться на виртуальных машинах доказывающего и проверяющего, что идентификация успешно завершена.

Подписать исходный код своей электронной подписью, выслать на адрес ladg91@mail.ru с темой lab15, после получения подписанного преподавателем исходного кода, прийти и защитить его.