Лабораторная работа №19

Схема Блома

Цель: Приобрести практические навыки в реализации криптографических протоколов распределения ключей

Введение

Опишем схему Блома распределения ключей.

Выберем поле , имеющее конечное, но достаточно большое число элементов, и зафиксируем различных элементов . Каждый элемент , припишем -му абоненту сети, Эти элементы не являются секретными и могут храниться на общедоступном сервере сети. Выберем теперь многочлен над полем степени вида

*,*

где . Его коэффициенты являются секретными и должны храниться только в центре распределения ключей. Каждый абонент получает в качестве ключевых материалов набор состоящий из коэффициентов многочлена , т.е. каждый пользователь обладает собственным многочленом.

Для связи между абонентами и теперь можно использовать общий ключ , который могут вычислить оба абонента.

*.*

1. Рабочее задание

1.1 Реализовать протокол распределения ключей Блома

2. Требования к реализации

2.1 Реализовать схему Блома для двух пользователей. Также должен быть реализован доверенный центр, который распределяет начальные параметры для пользователей.

2.2 Параметры схемы должны генрироваться автоматически.

2.3 Общий сеансовый ключ должен выводиться у пользователей.

Подписать исходный код своей электронной подписью, выслать на адрес ladg91@mail.ru с темой lab19, после получения подписанного преподавателем исходного кода, прийти и защитить его.