Лабораторная работа №20

(n,t)-пороговая схема Шамира

Цель: Приобрести практические навыки в реализации криптографических протоколов разделения секрета

Введение

Рассмотрим схему разделения секрета Шамира.

Пусть Схема разделения секрета между пользователями называется -пороговой, если любая группа из пользователей может восстановить секрет, в то время как никакая группа из меньшего числа пользователей не может получить никакой информации о секрете.

Выберем поле и зафиксируем различных несекретных элементов . Каждый элемент , припишем -му абоненту сети, Выберем также случайных элементов и составим из них многочлен над полем степени .

Положим . Вычислим теперь значения и распределим в качестве долей между участниками наборы .

Для восстановления секрета можно воспользоваться интерполяционной формулой Лагранжа. Путь имеются пар , где . Тогда формула Лагранжа имеет вид:

Так как , то из формулы Лагранжа получаем равенства:

1. Рабочее задание

1.1 Реализовать протокол разделения секрета

2. Требования к реализации

2.1 Реализовать (n,t)-пороговую схему Шамира для произвольного задаваемого множества пользователей.

2.2 Параметры схемы должны генрироваться автоматически.

2.3 Программа должна содержать возможность восстановления секрета.

Подписать исходный код своей электронной подписью, выслать на адрес ladg91@mail.ru с темой lab20, после получения подписанного преподавателем исходного кода, прийти и защитить его.