Лабораторная работа №10

Групповая цифровая подпись

Цель: Приобрести практические навыки в реализации групповой цифровой подписи по стандарту CAdES.

Введение

Схема групповой подписи позволяет некоторой группе подписать документ совместно. Групповая электронная цифровая подпись обладает следующими свойствами, которые отличают ее от обычной:

* автором подписи могут быть только члены группы;
* в любое время можно убедиться, что ее автор является членом группы;
* нет возможности определить, кто именно из членов группы является автором подписи.

Схема групповой подписи выглядит следующим образом:

1. Автор генерирует большое количество пар ключей (открытый и закрытый (секретный)). Каждый член группы получает от него свой набор ключей. При этом все наборы ключей у всех пользователей группы различны.
2. Автор помещает все открытые ключи в некоторый справочник в случайном порядке, сохраняя в секрете информацию, кому какой из ключей принадлежит.
3. Чтобы подписать документ, член группы выбирает ключ из предоставленных ему.
4. Чтобы проверить подлинность подписи, необходимо выбрать соответствующий открытый ключ из справочника.

Рассмотрим конкретную реализацию схемы групповой цифровой подписи.

Пусть - большое простое число (длиной не менее 1024 бит), такое, что число , где - простое число (в реальных системах достаточно большое простое число. В рамках лабораторной работы будем считать, что ). Выбирается элемент . Каждый -й представитель группы генерирует секретный ключ , по которому вычисляется открытый ключ , где - количество членов группы () (без лидера).

Пусть у лидера () группы открытый ключ , где - секретный ключ лидера. Проверка подписи осуществляется с помощью открытого ключа лидера.Лидер также имеет внутригрупповой открытый ключ , где ; , - простые числа; ; - дополнительный секретный параметр лидера; - функция Эйлера.

Пусть задана хеш-функция . Группа решила подписать сообщение .

1. .

.

2.

.

3.

.

4. .

.

5. .

Цифровая подпись .

Проверка цифровой подписи осуществляется следующим образом:

1. .

2. .

3.

4. .

Если выполняется последнее равенство, то цифровая подпись считается верной.

1. Рабочее задание

1.1 Реализовать схему групповой подписи в формате CAdES.

2. Требования к реализации

2.1 Реализовать групповую подпись на базе 3-х виртуальных машин: 1 лидера и 2-х членов группы.

2.2 Требования по реализации аналогичные лабораторной работе №7.

Подписать исходный код своей электронной подписью, выслать на адрес ladg91@mail.ru с темой lab10, после получения подписанного преподавателем исходного кода, прийти и защитить его.