Лабораторная работа №8

Цифровая подпись Эль-Гамаля

Цель: Приобрести практические навыки в реализации цифровой подписи Эль-Гамаля по стандарту CAdES.

Введение

Цифровая подпись Эль-Гамаля является еще одним распространенным видом цифровой подписи.

Пусть p - простое число; α - образующий элемент группы ; ;

Открытым ключом цифровой подписи (ключом проверки подписи) является набор (α,β,p). Закрытым ключом (ключом формирования подписи, ключом подписи) является (a). Обозначим через - значение хеш-функции от сообщения.

Формирование цифровой подписи производится следующим образом.

1. Выбирается случайное число , ;

2. Вычисляется значение ;

3. Вычислить значение

4. Подпись .

Проверка цифровой подписи производится по следующей формуле.

.

Если выполняется равенство, то цифровая подпись считается верной.

SubjectPublicKeyInfo в стандарте PKCS8 имеет следующую структуру: {alpha, beta, p},

где alpha- образующий элемент группы α;

beta - открытый элемент β;

p - число p.

Данные представляются в виде натуральных чисел.

Стандарт PKCS 12 (RFC 5958) устанавливает правила для формата файла закрытого ключа.

Закрытый ключ имеет следующий вид: {privateExponent},

где privateExponent - секретная экспонента a.

Данные представляются в виде натурального числа.

1. Рабочее задание

1.1 Реализовать схему цифровой подписи Эль-Гамаля в формате CAdES.

2. Требования к реализации

2.1 Требования по реализации аналогичные предыдущей лабораторной работе.

Подписать исходный код своей электронной подписью, выслать на адрес ladg91@mail.ru с темой lab8, после получения подписанного преподавателем исходного кода, прийти и защитить его.