Лабораторная работа №9

Цифровая подпись Фиата-Шамира

Цель: Приобрести практические навыки в реализации цифровой подписи Фиата-Шамира по стандарту CAdES.

Введение

Цифровая подпись Фиата-Шамира является еще одним примером цифровых подписей.

Пусть , где p,q - простые числа. Пусть задана хеш-функция - переводящая некоторое сообщение в строку длины m.

Пользователь генерирует m различных случайных чисел . В соответствии этим числам вычисляются числа .

Открытым ключом цифровой подписи (ключом проверки подписи) является набор чисел (, n). Закрытым ключом (ключом формирования подписи, ключом подписи) является (). Пусть - сообщение.

Формирование цифровой подписи производится следующим образом.

1. Выбирается случайное число ;

2. Вычисляется значение ;

3. Вычислить значение ;

4. Вычислит ;

5. Подпись .

Проверка цифровой подписи производится следующим образом:

1. Вычислить ;

2. Вычислить ;

3. Проверить равенство .

Если выполняется последнее равенство, то цифровая подпись считается верной.

1. Рабочее задание

1.1 Реализовать схему цифровой подписи Фиата-Шамира в формате CAdES.

2. Требования к реализации

2.1 Требования по реализации аналогичные лабораторной работе №7.

Подписать исходный код своей электронной подписью, выслать на адрес ladg91@mail.ru с темой lab9, после получения подписанного преподавателем исходного кода, прийти и защитить его.