Лабораторная работа № 9

Российский государственный стандарт на электронную (цифровую) подпись

1. Цель работы

Изучение принципов формирования электронной цифровой подписи с использованием алгоритмов, реализованных в Российском государственном стандарте на электронную (цифровую) подпись.

2. Основы теории

Российский стандарт ГОСТ Р34.10-94 был принят в 1994 году. В основе стандарта лежит алгоритм, называемый DSA (Digital Signature Algorithm) и являющийся вариацией подписи Эль-Гамаля.

Вначале для некоторого сообщества пользователей выбираются общие несекретные параметры. Прежде всего необходимо найти два простых числа, q длиной 256 бит и p длиной 1024 бита, между которыми выполняется соотношение

$$p=bq+1 \quad (1)$$

для некоторого целого b. Старшие биты в p и q должны быть равны единице. Затем выбирается число $a>1$, такое, что

$$a^q \bmod p=1 \quad . \quad (2)$$

В результате получаем три общих параметра — p, q и a.

Далее, каждый пользователь выбирает случайно число x, удовлетворяющее неравенству $0<x<q$, и вычисляет

$$y=a^x \bmod p \quad . \quad (3)$$

Число x будет секретным ключом пользователя, а число y — открытым ключом.

На этом этап выбора параметров заканчивается, и мы готовы к тому, чтобы формировать и проверять подписи.

Пусть имеется сообщение m, которое необходимо подписать. Генерация подписи выполняется следующим образом:

1. Вычисляем значение хеш-функции $h=h(\overline{m})$ для сообщения m, значение хеш-функции должно лежать в пределах $0<h<q$ (в российском варианте хеш-функция определяется ГОСТом Р34.11-94).

2. Формируем случайное число k, $0<k<q$.

3. Вычисляем $r=(ak \bmod p) \bmod q$. Если оказывается так, что $r=0$, то возвращаемся к шагу 2.

4. Вычисляем $s=(kh+xr) \bmod q$. Если $s=0$, то возвращаемся к шагу 2.

5. Получаем подписанное сообщение $(\overline{m};r,s)$.

Для проверки подписи делаем следующее.

1. Вычисляем хеш-функцию для сообщения $h=h(\overline{m})$.

2. Проверяем выполнение неравенств $0<r<q$, $0<s<q$.

3. Вычисляем $u_1=s\,h^{-1} \bmod q$, $u_2=-r\,h^{-1} \bmod q$.

4. Вычисляем $v=(a^{u_1} y^{u_2} \bmod p) \bmod q$.

5. Проверяем выполнение равенства $v=r$.

Если хотя бы одна из проверок на шагах 2 и 5 не дает нужного результата, то подпись считается недействительной. Если же все проверки удачны, то подпись считается подлинной.

Чтобы найти параметр a , удовлетворяющий (2), рекомендуется использовать следующий метод. Берем случайное число $g>1$ и вычисляем

$$a=g^{(p-1)/q} \bmod p \qquad (4)$$

Если $a>1$, то это то, что нам нужно. Если при вычислении по (14) мы получаем $a=1$, то нужно просто взять другое число g .

3. Объекты и средства исследования

Объектами исследования являются алгоритмы формирования электронной цифровой подписи с использованием, реализованные в Российском государственном стандарте на электронную (цифровую) подпись.

4. Подготовка к работе

4.1 Изучить теоретическую часть

4.2 Получить задание у преподавателя

5. Программа работы

5.1 Составить алгоритм, реализующий заданный метод формирования электронной цифровой подписи .

5.2 Разработать и отладить программу

5.3 Оформить отчет

6. Контрольные вопросы

6.1. Для чего нужна цифровая подпись?

6.2. Назовите основные свойства цифровой подписи.

6.3. Какие схемы цифровой подписи существуют? Какая схема самая распространенная?

6.4. Как осуществляется подпись в Российском стандарте ГОСТ Р34.10-94?

6.6. Как осуществляется проверка на подлинность подписи в Российском стандарте ГОСТ Р34.10-94?

Содержание отчета

1. Титульный лист
2. Задание
3. Схема алгоритма формирования электронной цифровой подписи
4. Текст программы
5. Скриншоты
6. Выводы

Литература

1. Баричев С.Г, Серов Р.Е. Основы современной криптографии: Учебное пособие. - М.: Горячая линия - Телеком, 2002.

2. Иванов М. А. Криптографические методы защиты информации в компьютерных системах и сетях. М.:КУДИЦ-ОБРАЗ, 2001 - 368 с.

Задания к работе

1 вариант. Разработать программу для генерации ЭЦП по ГОСТ Р34.10-94. Рекомендуемое значение p=31481 (для вычисления хэша воспользоваться киптографической библиотекой).

2 вариант. Разработать программу для проверки ЭЦП по ГОСТ Р34.10-94. Рекомендуемое значение p=31481 (для вычисления хэша воспользоваться киптографической библиотекой).