**МИНОБРНАУКИ РОССИИ**

**Санкт-Петербургский государственный**

**электротехнический университет**

**«ЛЭТИ» им. В.И. Ульянова (Ленина)**

**Кафедра информационной безопасности**

отчет

**по лабораторной работе №8**

**по дисциплине «Криптография и защита информации»**

Тема: **Изучение цифровой подписи**

|  |  |  |
| --- | --- | --- |
| Студент гр. 8383 |  | Киреев К.А. |
| Преподаватель |  | Племянников А.К. |

Санкт-Петербург

2021

**Выводы**

* Изучены механизмы генерации ключевых пар для различных алгоритмов.
  + Алгоритм RSA генерирует пары – открытый ключ и – закрытый ключ на основе двух больших простых чисел и , которые впоследствии должны быть уничтожены.
  + Алгоритм DSA генерирует пары – открытый ключ и – закрытый ключ на основе простого числа (длина от 512 до 1024 бит), (такого, что ) и .
  + Алгоритм генерирует пары – открытый ключ и – закрытый ключ на основе произвольно выбранной эллиптической кривой , где – простое число, произвольно выбранной точки на данной кривой, , простое число (порядок одной из циклических подгрупп группы точек эллиптической кривой). Наименьшая скорость генерация была у алгоритма EC-239 и составила 0.01 секунд.
* Изучен механизм создания цифровой подписи с различными ключами.

Лучше всего использовать ECDSA для создания и подтверждения подписи. Операция создания занимает 0 секунд, а процесс проверки 0.002 секунд. Вычисление DSA подписи быстрее, чем вычисление подписей RSА, однако DSA требуется больше времени на проверку целостности.

* Изучен алгоритм формирования и проверки подписи ECDSA, основанный на эллиптических кривых.

Открытый ключ представляет собой пару , где – параметры, задающие определённую эллиптическую кривую, – произвольная точка на кривой, – порядок циклической подгруппы группы точек эллиптической кривой, такой, что для некоторой точки , лежащей на кривой, верно: , где – закрытый ключ.

* Изучено создание сертификатов в среде PKI.

PKI решает криптозадачи такие как обеспечение конфиденциальности и целостности информации; обеспечение аутентификации пользователей и ресурсов, к которым обращаются пользователи; обеспечение возможности подтверждения совершенных пользователями действий. Сертификат — это электронный документ, который содержит: открытый ключ пользователя, информацию о пользователе, которому принадлежит сертификат, информацию о сроке действия сертификата, информацию об издателе сертификата и другие атрибуты, цифровую подпись удостоверяющего центра, выдавшего сертификат. Сертификат подтверждает электронную цифровую подпись и открытый ключ отправителя.

* Изучено создание подписи и проверка документа на целостность после внесения изменений средствами Adobe Acrobat Reader.