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 (e, n) – открытый ключ и d – закрытый ключ на основе двух больших простых чисел p и q, которые впоследствии должны быть уничтожены.
  - Алгоритм DSA генерирует пары (e_1, e_2, p, q) – открытый ключ и d – закрытый ключ на основе простого числа p (длина от 512 до 1024 бит), q (такого, что $(p-1) = 0 \; mod \; q$) и d.
  - Алгоритм $ECDSA$ генерирует пары (a, b, e_1, e_2, p, q) – открытый ключ и d – закрытый ключ на основе произвольно выбранной эллиптической кривой $E_p(a, b)$, где p – простое число, произвольно выбранной точки на данной кривой, d, простое число q (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 RSA, однако DSA требуется больше времени на проверку целостности.

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

Открытый ключ представляет собой пару (a, b, q, p, e_1, e_2), где a, b, p – параметры, задающие определённую эллиптическую кривую, e_1 – произвольная точка на кривой, q – порядок циклической подгруппы группы точек

эллиптической кривой, такой, что для некоторой точки $e_1 = (x_1, y_1)$, лежащей на кривой, верно: $q \times (x_1, y_1) = 0$; $e_2 = d \times e_1$, где d – 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.