МИНОБРНАУКИ РОССИИ
САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ
ЭЛЕКТРОТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
«ЛЭТИ» ИМ. В.И. УЛЬЯНОВА (ЛЕНИНА)
Кафедра МО ЭВМ

ОТЧЕТ

по лабораторной работе №8

«Изучение цифровой подписи»

Студент гр. 8382 _____ Мирончик П.Д.

Преподаватель _____ Племянников А.К.

Санкт-Петербург

2021

ВЫВОДЫ

1. Рассмотрены генераторы ключевых пар для алгоритмов RSA, DSA и ECDSA. Определено, что RSA и DSA выполняют генерацию за примерно одинаковое время (3-4 секунды), в то время как ECDSA значительно быстрее – за 16мс.

2. Рассмотрен общий алгоритм создания цифровой подписи документа: по сообщению генерируется хеш, затем он шифруется закрытым ключем, а для проверки подписи необходимо расшифровать хеш открытым ключем и сравнить его с хешем сообщения, по которому выполняется проверка. Экспериментально выяснено, что время создания подписи для документа достаточно невелико – подпись документа длиной 5000 символов заняла от 0мс (DSA) до 12мс (RSA).

3. Рассмотрен алгоритм цифровой подписи на эллиптических кривых. Проведено подписание документа и проверка соответствия документа его подписи, а также проверка того, что измененный документ подписи не соответствует. Повторены лекционные шаги по зашифрованию и расшифрованию сообщения с использованием средств визуализации CrypTool и подтверждена корректность вычислений.

4. Выполнено пошаговое создание подписи документа с использованием подпрограммы CrypTool - пошаговой визуализации подписи документа. В результате был сгенерирован сертификат. После сравнения его структуры с представленной в лекции оказалось, порядок пунктов отличается.

5. Проведена попытка подписания документа с использованием экспортированного из CrypTool сертификата. Подписать документ не удалось в связи с “неподдерживаемым алгоритмом открытых ключей”. После этого был сгенерирован сертификат средствами Adobe Reader, которым был успешно подписан документ. Затем в подписанный документ были внесены изменения, что подтвердилось при проверке подписи.