МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования «Полоцкий государственный университет»

Факультет информационных технологий

Кафедра вычислительных систем и сетей

**ЛАБОРАТОРНАЯ РАБОТА №2**

по дисциплине: **«Теория Информации»**

на тему: «ЭЛЕКТРОННАЯ ЦИФРОВАЯ ПОДПИСЬ»

ВЫПОЛНИЛ студент группы 16-ИТ-3

Яблонский А.С

ПРОВЕРИЛА преподаватель

Захарова И.Ю

Полоцк 2018 г.

**КРАТКИЕ ТЕОРЕТЕЧЕСКИЕ СВЕДЕНИЯ**

**Secure Hash Algorithm 1** — алгоритм криптографического хеширования. Для входного сообщения произвольной длины (максимум 2^64 - 1 {\displaystyle 2^{64}-1}2^2бит, что примерно равно 2 эксабайта) алгоритм генерирует 160-битное (20 байт) хеш-значение, называемое также дайджестом сообщения, которое обычно отображается как шестнадцатиричное число, длиной в 40 цифр. Используется во многих криптографических приложениях и протоколах. Также рекомендован в качестве основного для государственных учреждений в США.

**Электронная подпись** (ЭП), **Электронная цифровая подпись** (ЭЦП), **Цифровая подпись** (ЦП) — реквизит электронного документа, полученный в результате криптографического преобразования информации с использованием закрытого ключа подписи и позволяющий проверить отсутствие искажения информации в электронном документе с момента формирования подписи (целостность), принадлежность подписи владельцу сертификата ключа подписи (авторство), а в случае успешной проверки подтвердить факт подписания электронного документа (неотказуемость).

**АНАЛИЗ ЗАДАНИЯ**

1. Реализовать алгоритм вычисления хеш-функции SHA-1 для файла с произвольным размером и содержимым.

2. Реализовать программное средство, выполняющее генерацию и проверку ЭЦП файла с произвольным содержимым на базе алгоритма RSA с использованием для вычисления хеш-функции ранее реализованного алгоритма SHA-1.

**Основные и промежуточные результаты по каждому пункту хода выполнения работы**

В данной таблице представлены данные, которые реализуют хэш-функцию алгоритмом SHA1.

Также в таблице представлено программное средство, которое выполняет генерацию и проверку ЭЦП файла с произвольным содержимым на базе алгоритма RSA с использованием для вычисления хеш-функции ранее реализованного алгоритма SHA-1.

|  |  |
| --- | --- |
| Текст | Some origin text message |
| Хэш-функция | 2be11e17d118b163fe99ddcf050f05d9ba10be63 |
| Шифрование алгоритмом RSA | 52660770317309676326134190170362611551475801441491085737287017917183464872416942965407911599430006842681922697310449367401534979821234817521659212123991439056582617297947168434047519663577475907401199475325404364993984321625717529451098684639624285638175476612951426034557193036401829991331237447848948238872 |
| Открытые ключи | 13  131935938005834047748455081027424928530285832264620796065141866609332415636573393817557262594925588900672529342609487843898723876424385956500248304428284764218765961269897340677164575219127163272757644402424051837109855878125574040361172634626506419130764910242356916074295330498387120584075219632601624937043 |
| Закрытый ключ | 27194516005193382079623042648021464313022746401314342182742906098171017344739055018684810012275294705541637070199409675274046570866476724084300898404041272002621754159399997516430103334032025724467275331741243948576711424999895109791326053180099745743814871278483191949854692792433509723434787602041296928183 |

**Вывод:** в ходе выполнения лабораторной работы была реализована электронная цифровая подпись, с помощью которой, происходит проверка на подлинность документа. В данной цифрой подписи присутствует реализация публичных и закрытых ключей, электронной подписи, и документа, который проверяется на подлинность. Отправитель генерирует хэш документа с помощью алгоритма SHA1, после этого хэш шифруется с помощью алгоритма RSA и закрытого ключа, который находится только у отправителя. Также создаются публичные ключи, которые может использовать кто угодно, для дешифровки подписи. С помощью публичных ключей происходит дешифровка, алгоритма RSA, и текст для проверки на подлинность, который отправитель отправил получателю. После этого происходит сверка результатов, при их соответствии - подлинность документа подтверждена.