Модуль 2. Электронная подпись как криптографический примитив

Задание № 1. Приведите протокол подписи одного и того же документа одновременно двумя пользователями с помощью хэш-функций при условии, что пользователи не доверяют друг другу.

Основной протокол подписи документа:

1. Абонент А создает необратимое хэш-значение документа.
2. Абонент А зашифровывает это значение своим закрытым ключом, тем самым подписывая документ.
3. Абонент А отправляет абоненту В документ и подписанное хэш-значение.
4. Абонент В генерирует необратимое хэш-значение документа, присланного абонентом А. Затем, используя алгоритм электронной подписи, абонент В расшифровывает подписанное хэшзначение документа с помощью открытого ключа абонента А. Если подписанное хэш-значение совпадает со сгенерированным — подпись достоверна.

Здесь должна использоваться только однонаправленная хэш-функция, в противном случае можно создать разные документы с одним и тем же значением хэш-функции, уязвимые к мошенничеству.

Следует добавить несколько элементов к этому протоколу, учитывая тот факт, что абоненты не доверяют друг другу.

- Добавить систему архивирования, которая будет использовать данный протокол для подтверждения существования документов без отражения их содержимого. В базе данных хрянятся значения хэш-функции файлов. Б.
- Возможность использование третьей стороны Т, через которую будет проходить обмен документами:
    1. Абонент А подписывает значение хэш-функции документа;
    2. Абонент В подписывает значение хэш-функции документа;
    3. Абонент В отправляет свою подпись абоненту А;
    4. Абонент А отправляет абоненту С сам документ, свою подпись и подпись абонента В;
    5. Абонент С проверяет подлинность подписи абонентов А и В В.
- Необходимо добавить использование меток времени для повышения уровня защищённости документа.

Задание № 2. Докажите, что в криптосистемах, основанных на открытых ключах, нельзя использовать одинаковые ключи для шифрования и электронной подписи.

- При использовании одного и того же ключа для шифрования и цифровой подписи возникает угроза компрометирования данных, по причине потенциального взлома системы, хранящей секретные ключи ассиметричной системы шифрования или взлома функции шифрования и подбора ключей. В этом случае злоумышленник, получив доступ к ключу, сможет нанести вред расшифровывая конфиденциальные документы и подписывая легальные документы.
- Секретный ключ может храниться на сервере организации, где к нему будут иметь доступ другие пользователи с административным уровнем доступа.
- Пользователь использующий ключ для шифрования документов и своей электронной подписи может иметь разные роли и уровни безопасности, здесь использование одного ключа равносильно использование физического ключа, чтобы открывать все двери в организации. Пользователь может быть директором компании, при этом состоять в группе единомышленников, иметь личную систему переписки с друзьями и членами семьи, во всех этих ситуациях ему необходимо создавать разные ключи шифрования, использование одного исключено.

Задание № 3. Напишите, что общего между собственноручной и электронной подписью и чем они различаются.

Свойства собственноручной подписи:

1. Подпись достоверна. Она убеждает получателя в том, что человек, подписавший документ, сделал это сознательно.
2. Подпись неподдельна. Она доказывает, что именно подписавший - и никто иной - сознательно подписал документ.
3. Подпись невозможно использовать повторно. Она является частью документа, и злоумышленник не может перенести её в другой документ.
4. Подписанный документ невозможно изменить.
5. От подписи нельзя отречься.
6. Подпись и документ материальны. Подписавший не сможет впоследствии утверждать, что он не подписывал документ.

Общие черты собственноручной и электронной подписей:

1. С электронной её роднит то, что обе являются средством подтверждения подлинности человека, поставившего подпись, то есть они удостоверяют документ.
2. При соответствующй нормативной базе возможно разнозначно использовать оба вида подписи.
3. Для обоих видов подписей существуют способы проверки подлинности.

Общие черты собственноручной и электронной подписей:

1. Собственноручные подписи ставят на физический документ, электронные на цифровой, используя технические средства.
2. Существует несколько видов электронной подписи в отличие от собственноручной: Простая, Усиленная (Неквалифицированная и Квалифицированная), использование который регламентируется Федеральным законом № 63-ФЗ «Об электронной подписи».
3. Разные способы проверки подлинности Собственноручной и Электронной (в силу разной природы)
4. ЭП сертифицированного типа намного труднее подделать, чем собственноручные.
5. Хранение документов с использованием данных типов подписей значительно отличается.