Раздел: Анализ Защищенности ПО (на веб)
Практическое задание: Модуль 2. Электронная подпись как криптографический примитив
Выполнил: Александр Ганицев

Задание.

Вы закончили второй модуль, посвящённый электронной подписи и особенностям её использования. Чтобы закрепить знания, предлагаем вам решить три задачи.

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

Формат сдачи
Напишите ответ в свободной форме. Он должен содержать описание протокола и обоснование указанного в задаче свойства.

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

Формат сдачи
Напишите ответ в свободной форме. Он должен содержать доказательство утверждения.

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

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 хэш-значение 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.

А. Надо 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. Так же есть 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. Также 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.

1. 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.

2. Секретный ключ может храниться на сервере организации, где к нему будут иметь доступ другие пользователи с административным уровнем доступал.

3. Пользователь использующий ключ для шифрования документов и своей электронной подписи может иметь разные роли и уровни доступа/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:

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

Сходства:

С электронной её роднит то, что обе являются средством подтверждения подлинности человека, поставившего подпись, то есть они удостоверяют документ.

При соответствующй нормативной базе возможно разнозначно использовать оба вида подписи.

Различия:

1. Собственноручные подписи ставят на физический документ, электронные на цифровой, используя различные технические средства.

2. ЭП существует несколько видов: Простая, Усиленная (Неквалифицированная и Квалифицированная), использование который регламентируется Федеральным законом № 63-ФЗ «Об электронной подписи».

3. Разные степени сложности проверки подлинности.

4. ЭП сертифицированного типа намного труднее подделать, чем собственноручные.

5. Хранение документов с использованием данных типов подписей значительно отличается.