Основы прикладной криптографии. ДПО Информационная безопасность

Основы прикладной криптографии

Модуль 2. Электронная подпись как криптографический примитив

5/6 5. Практическое задание

Выполнил Рыжов Всеволод

**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.***

**Решение:**

1) В данном случае, логично было бы, как написано в учебном модуле, ввести доверенную сторону С, которая бы удостоверяла бы правильность документа и подписи обоих сторон. Тогда решение выглядело бы так: Сначала документ подписывает абонент А, а затем абонент В подписывает подпись абонента А. Этот способ работает, однако позволяет проверить подлинность подписи абонента А только совместно с проверкой подписи абонента В. Задача многократного подписания документа решается с помощью однонаправленных хэш-функций:

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 подписи абонентов А и В

2) Допустим, что стороны не хотят вмешательства третьей стороны. В этом случае можно было бы поступить следующим образом:

1. Пользователь A и пользователь B соглашаются подписать один и тот же документ;
2. Пользователь A вычисляет хэш-значение документа (Hash\_A) с использованием хэш-функции;
3. Пользователь B вычисляет хэш-значение документа (Hash\_B) с использованием хэш-функции: Hash\_B = SHA-256(документ);
4. Пользователь A создает свою подпись (Sign\_A) для документа, используя свой секретный ключ;
5. Пользователь B создает свою подпись (Sign\_B) для документа, используя свой секретный ключ;
6. Стороны совместно подписывают документ итоговой подписью (Sign\_F), которая будет включать в себя документ, Hash\_A и Hash\_B, а также подписи обоих пользователей. Обе стороны A и B имеют доступ к ключам для верификации финальной подписи.;

**Проверка подписи:**

Для проверки подписи любой стороной (например, третьей стороной или одним из пользователей) необходимо выполнить следующие шаги:

1. Извлечь документ, Hash\_A, Hash\_B, Sign\_A и Sign\_B из итоговой подписи (Sign\_F);
2. Вычислить хэш-значения Hash\_A и Hash\_B для документа;
3. Проверить подписи Sign\_A и Sign\_B, используя заранее переданные друг другу открытые ключи PubKey\_A и PubKey\_B;
4. Убедиться, что Hash\_A и Hash\_B соответствуют вычисленным хэш-значениям для документа.

**Задание № 2**

***Докажите, что в криптосистемах, основанных на открытых ключах, нельзя использовать одинаковые ключи для шифрования и электронной подписи.***

**Решение:**

Нельзя использовать одинаковые ключи для шифрования и электронной подписи потому что:

1) При использовании открытого ключа для шифрования и проверки подписи (т. е. одного и того же ключа) злоумышленник сможет подделать электронную подпись на сообщении, а значит он также сможет расшифровать это сообщение, так как у него есть открытый ключ;

2) Если использовать один и тот же ключ для шифрования и подписи, то получатель должен будет знать ваш секретный ключ (используемый для создания подписи) для проверки подлинности сообщения и сможет подделать само сообщение, что нарушит его целостность;

**Задание № 3**

***Напишите, что общего между собственноручной и электронной подписью и чем они различаются.***

**Решение:**

Сходства:

1) что электронная подпись, что рукописная — являются средством подтверждения документа;

2) если использовать соответствующую нормативную базу и рукописная подпись и электронная будут средством удостоверения подлинности документа

Различия:

1) **По способу создания:** рукописную подпись пользователь наносит сам физически, электронную — с помощью технических средств, можно даже не видя документ, с помощью специализированного ПО и электронных устройств (компьютер, смартфон, флэш-карта)

2) **По среде применения:** рукописная подпись используется в физическом мире, тогда как электронная — в цифровом;

3) **По сложности определение подлинности: к**акая бы ни была замысловатая рукописная подпись, определить, подлинная она или нет, всегда будет процесс субъективный и сложный и трудоемкий (похожая / непохожая, нанесена чернилами или распечатана на принтере, отпечатана факсмиле). В случае с электронной подписью, при соблюдении всех норм и стандартов и применения необходимых технических средств, подлинность электронной подписи не будет вызывать сомнений и процесс верификации нетрудоемкий и быстрый;

4) **По уровню безопасности:** рукописную подпись, какая бы она ни была замысловатая, в принципе можно подделать. Электронную же подпись при соблюдении всех норм и стандартов и применения необходимых технических средств, подделать много труднее или невозможно вообще;

5) **По уровню контроля над документом:** Подписанный рукописной подписью документ легко контролировать: его можно поместить в сейф, в архив. Подписанный электронной подписью документ контролировать много сложнее. Как и любая информация в «цифровом мире» он может мгновенно распространяться: быть размещенным на сайте, по электронной почте, в сообщениях мессенджеров и т.д.