Электронная цифровая подпись

- Понятие электронной цифровой подписи.
- Однонаправленные хэш-функции.
- Алгоритмы электронной цифровой подписи

Особенности электронной цифровой подписи

- ЭЦП имеет логическую природу – это последовательность символов (кодов), которая однозначно позволяет связать автора документа, содержание документа и владельца ЭЦП.
- Логический характер цифровой подписи делает ее независимой от материальной природы документа.
- С ее помощью можно помечать, а затем и аутентифицировать документы, имеющие электронную природу.

Особенности электронной цифровой подписи

- **Сопоставимость защитных свойств.** При использовании защитных свойств ЭЦП защитные свойства электронной подписи выше, чем ручной.
- **Масштабируемость.** В гражданском документообороте возможно применение простейших средств ЭЦП, в служебном документообороте – применение сертифицированных средств ЭЦП, для классифицированной информации необходимо применение специальных средств ЭЦП.
- **Дематериализация документации.** При использовании ЭЦП возможны договорные отношения между удаленными юридическими и физическими лицами.
- **Равнозначность копий.** Снимается естественное различие между оригиналом и копиями документа.
- **Дополнительная функциональность.** В электронный документ, подписанный ЭЦП, нельзя внести изменения, не нарушив подпись, т.е. в отличие от ручной подписи, ЭЦП является не только средством идентификации, но и средством аутентификации.
- **Автоматизация.** Все стадии обслуживания ЭЦП (создание, применение, удостоверение и проверка) автоматизированы, что значительно повышает эффективность документооборота.

Техническое обеспечение цифровой подписи

Потребность в криптографии

- Будем рассматривать ***документ (сообщение)***, как уникальную последовательность символов.
- Любые способы транспортировки сообщения будем называть ***каналом связи.***
- Чтобы последовательность символов, могла однозначно идентифицировать ***ее автора, она должна обладать уникальными признаками, известными только отправителю и получателю сообщения.***
- В этом случае можно говорить о ***защищенном канале связи,*** который обеспечивает:
  - ***Идентификацию партнера***
  - ***Аутентификацию сообщения.***

  Достигается это с помощью шифрования (криптографии).

Метод и ключ шифрования

- ***Метод шифрования*** – это формальный алгоритм, описывающий порядок преобразования исходного сообщения в результирующее.
- ***Ключ шифрования*** – это набор параметров, необходимых для шифрования.
- **Ключевое слово** (например, 3-5-7).
- **Ключевая фраза** – несколько ключевых слов.
- ***Статический*** (используется многократно) и ***динамический*** (содержит в сообщении новый ключ) ключи.

Симметричный и несимметричный методы шифрования

- При ***симметричном шифровании*** информация зашифровывается и расшифровывается одним и тем же ключом,
- Поэтому необходимо передать ключ, т.е. проблема передачи информации возникает на новом уровне.
- Симметричное шифрование не годится для электронной коммерции!
- Однако оно получило применение в **гибридных системах**, сочетающих симметричное и несимметричное шифрование.

Симметричный и несимметричный методы шифрования

- ***Несимметричное шифрование*** использует два ключа – ***public*** (открытый ключ) и ***private*** (закрытый ключ).
- Они устроены таким образом, что сообщение, зашифрованное одним ключом можно расшифровать только другим ключом, и наоборот.
- Владелец пары ключей может оставить один себе, а другой опубликовать (рассылка с помощью электронной почты или выставить открытый ключ на WEB-сервере).

Симметричный и несимметричный методы шифрования

- 1. Использование закрытого ключа позволяет идентифицировать отправителя.
- 2. Использование открытого ключа позволяет аутентифицировать сообщение.
- 3. Обмен открытыми ключами позволяет создать защищенный канал связи.
- 4. Двойное последовательное шифрование сначала своим личным ключом, а затем открытым ключом другой стороны, позволяет создать защищенный направленный канал связи.

Понятие о компрометации ЭЦП

- Чтобы фальсифицировать ЭЦП, злоумышленник должен получить доступ к закрытому ключу.
- Закрытый ключ может быть скомпрометирован разными способами, которые классифицируют на ***традиционные и нетрадиционные.***
- Если для ***традиционных*** методов существует законодательная база, то для ***нетрадиционных методов***, основанных на реконструкции закрытого ключа, дело обстоит не так.

Традиционные методы:

- Хищение ключа путем копирования в результате прямого физического или удаленного сетевого доступа к оборудованию;
- Получение ключа в результате запроса , исполненного с признаками мошенничества и подлога;
- Хищение ключа, вытекающее из хищения оборудования;
- Хищение ключа в результате сговора с лицами, имеющими право на его использование.

Нетрадиционные методы компрометации закрытого ключа (реконструкция) основаны на следующем:

- Имеется легальный доступ к открытому ключу, а он связан с закрытым ключом некоторыми математическими соотношениями;
- Можно экспериментировать не со случайными, а специально подобранными сообщениями;
- Методы шифрования и дешифрования также известны, поскольку они широко публикуются для всеобщего тестирования.

Криптостойкость средств ЭЦП

- На криптостойкость ЭЦП влияют свойства пары ключей. Ключи создаются в результате применения средств ЭЦП. *Средство ЭЦП* – это аппаратное или программное обеспечение, генерирующее пару ключей по запросу пользователя. В основе этого средства лежит алгоритм.

- Существует несколько разновидностей алгоритмов для создания пары ключей. Некоторые безупречные на первый взгляд алгоритмы могут не всегда генерировать полностью криптостойкие ключи, причем пользователь никогда не узнает о дефектах, пока не потерпит ущерб в результате незаконного использования ключа.

Влияние размеров ключей на их криптостойкость

- Для симметричных ключей криптостойкость оценивается очень просто.
- Для симметричного ключа в 40 бит (слабое шифрование) надо перебрать всего 2 в 40 степени комбинаций, т.е. задача решается быстрее чем за сутки.
- При длине ключа в 64 бита необходима сеть из нескольких десятков специализированных компьютеров, и задача решается в течение нескольких недель.
- Это крайне дорого, но возможно технически.
- Сильным считается шифрование с длиной симметричного ключа 128 бит. На любом современном оборудовании эта задача решается за время, в миллиарды раз превышающее возраст Вселенной.

Влияние размеров ключей на их криптостойкость

- Для ключей ***несимметричного шифрования*** не удается получить столь простую формулу, как для симметричных ключей.
- Алгоритмы несимметричного шифрования еще не до конца изучены, поэтому при использовании несимметричного шифрования говорят об относительной криптоустойчивости ключей.
- Ее оценивают по эмпирическим данным.

Длина симметричного и несимметричного ключа при одинаковом уровне безопасности

Симметричный ключ	Несимметричный ключ
56 бит	384 бит
64 бит	512 бит
128 бит	2304 бит

Электронная печать

- Электронная печать несет в себе информацию об ее авторе, зашифрованную с помощью закрытого ключа.
- Кроме того имеется возможность включить в состав ЭЦП и данные, характеризующие само сообщение, чтобы исключить возможность внесения в него изменений в канале связи.
- Для этого используется понятие, называемое дайджестом сообщения.

Понятие о дайджесте сообщения

- ***Дайджест сообщения*** – это уникальная последовательность символов, однозначно соответствующая содержанию сообщения.
- Обычно дайджест имеет фиксированный размер, например, 128 или 168 бит и не зависит от длины самого сообщения.
- Дайджест вставляется в состав ЭЦП вместе со сведениями об авторе и шифруется вместе с ними.
- Простейший прием создания дайджеста можно рассмотреть на примере контрольной суммы:
  - Каждый символ сообщения представляется числовым кодом, то можно просуммировать все коды, и этот числовой параметр назовем контрольной суммой.
  - При изменении сообщения в канале связи изменится и контрольная сумма, что будет обнаружено принимающей стороной. Истинную контрольную сумму она узнает из подписи и обнаружит постороннее вмешательство.

  Однако, можно подобрать такой алгоритм, который позволит по известной контрольной сумме создать новое сообщение, отличное от исходного.

Хэш-функция

- В современной математике известны функции, не обладающие свойством обратимости.
- Они позволяют из одного сообщения получить другое сообщение таким образом, что обратное преобразование невозможно.
- Этот метод используется для аутентификации документов средствами ЭЦП.
- Исходное сообщение обрабатывается хэш-функцией, после чего образуется хэш-код, он является уникальным для данного сообщения. Это и есть дайджест сообщения.
- Дайджест (электронная печать) присоединяется к электронной подписи и далее является ее составной частью.

Дайджест сообщения

- Принимающая сторона расшифровывает сообщение, проверяет электронную подпись с помощью своей половины ключа, затем обрабатывает сообщение той же хэш-функцией, что и отправитель, после чего сличает полученный дайджест с тем, который содержался в подписи.
- Если дайджесты совпали, значит, сообщение не подверглось изменениям в канале связи.

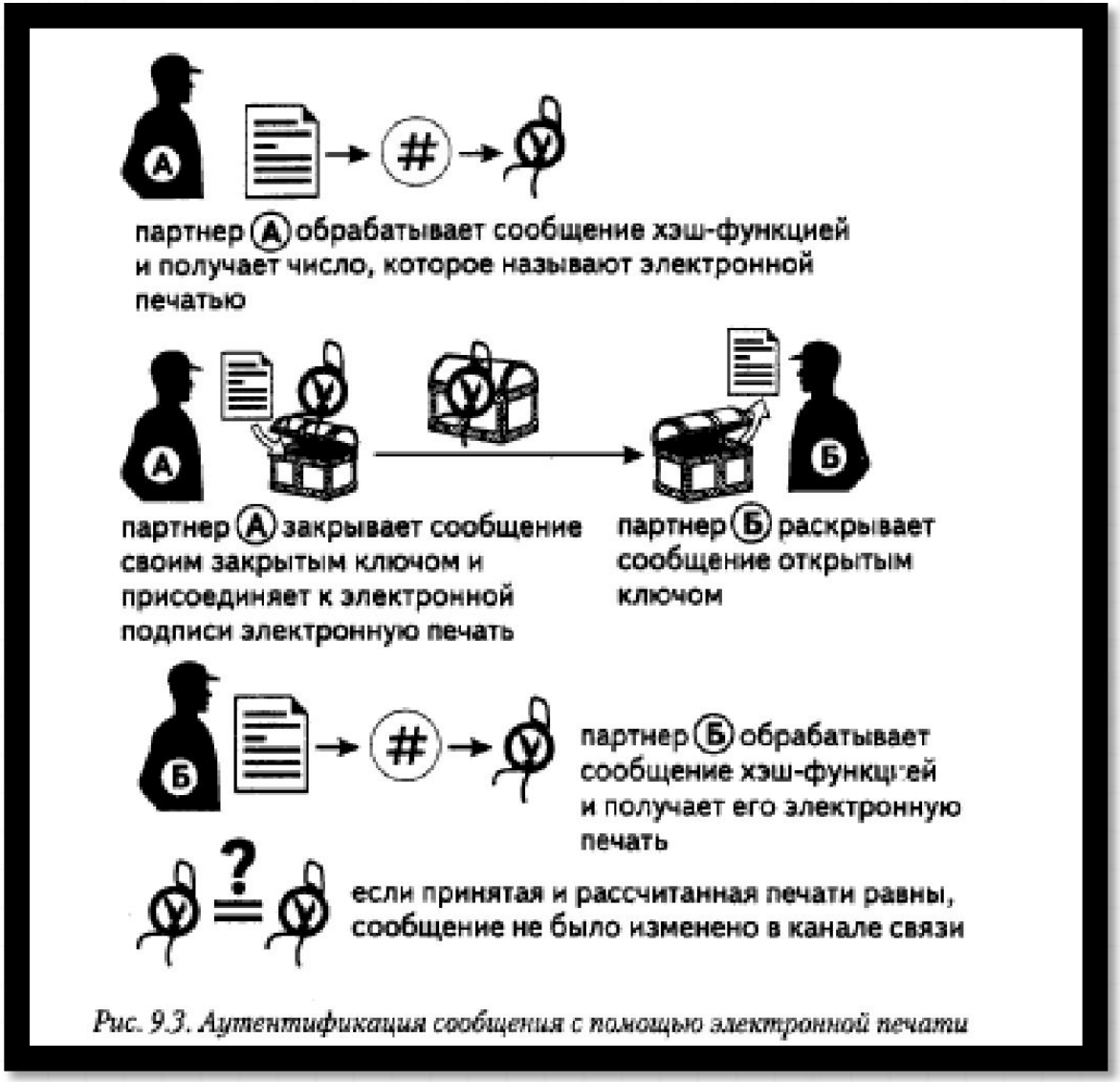

Рис. 9.3. Аутентификация сообщения с помощью электронной печати