МИНИСТЕРСТВО НАУКИ И ОБРАЗОВАНИЕ КЫРГЫЗСКОЙ РЕСПУБЛИКИ

ОШСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Факультет математики и информационных технологий

Кафедра ИТАС

Уровень образования 710100 бакалавриат

Направление подготовки/специальность Информатика и вычислительная техника

Группа ПОВ(б)-2-17(р)

Дата проведения откытого урока 24.11.2019

Тема урока : Электронная цифровая подпись и ее использование.

ПЛАН РАЗРАБОТКИ УРОКА

Адилбекова Н.А. *учитель кафедры ИТАС*

Урок

Тема: Электронная цифровая подпись и ее использование.

План урока:

1. Понятие ЭЦП
2. Назначение и применение ЭЦП
3. История возникновения
4. Алгоритмы
5. Использование хеш-функций
6. Симметричная схема
7. Асимметричная схема
8. Подведение итогов.
9. Домашнее задание

Цель учебного занятия: Рассмотреть определение цифровой подписи и ее предназначение.

Тип урока: комбинированный.

Оборудование урока:

1. Компьютеры
2. Мультимедийный проектор

Методическое обеспечение:

1. Конспект занятия
2. Презентация

Программное обеспечение:

Операционная система Windows10, Service Pack1, офисная программа Microsoft PowerPoint 2010.

Ход урока:

1. Организационный момент.
2. Сообщение темы и постановка задач.
3. Изучение материала

Понятие ЭЦП

Понятие ЭЦП приведено в законе "Об электронной цифровой подписи". Электронная цифровая подпись это реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе; Таким образом, понятие ЭЦП неразрывно связывается с понятием сертификата ключа, понятием криптографического преобразования и электронным документом. Следовательно, к системам ЭЦП следует относить только системы подтверждения подлинности электронных документов с использованием сертификатов и основанных на криптографических преобразованиях. Кроме того, использование ЭЦП согласно закону, возможно только для электронных документов. Закон не распространяет свое действие на применение ЭЦП к другим типам документов. Рассмотрим все признаки ЭЦП:

Сертификат ключа подписи - документ на бумажном носителе или электронный документ с электронной цифровой подписью уполномоченного лица удостоверяющего центра, которые включают в себя открытый ключ электронной цифровой подписи и которые выдаются удостоверяющим центром участнику информационной системы для подтверждения подлинности электронной цифровой подписи и идентификации владельца сертификата ключа подписи;

Строгое определение электронного документа сегодня отсутствует, тем не менее, на практике используется понятие, введенное в законе "Об информации, информатизации и защите информации". Документированная информация (документ) это зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать.

Какие именно **реквизиты** должны быть обязательны для документа:

- обозначение и наименование документа;
- даты создания, утверждения и последнего изменения;
- сведения о создателях;
- сведения о защите электронного документа;
- сведения о средствах электронной цифровой подписи или средствах кэширования, необходимых для проверки электронной цифровой подписи или контрольной характеристики данного электронного документа;
- сведения о технических и программных средствах, необходимых для воспроизведения электронного документа;
- сведения о составе электронного документа.

Назначение и применение ЭЦП

Электронная подпись предназначена для идентификации лица, подписавшего электронный документ. Кроме этого, использование электронной подписи позволяет осуществить:

- контроль целостности передаваемого документа: при любом случайном или преднамеренном изменении документа подпись станет недействительной, потому что вычислена она на основании исходного состояния документа и соответствует лишь ему.

- защиту от изменений (подделки) документа: гарантия выявления подделки при контроле целостности делает подделывание нецелесообразным в большинстве случаев.

- невозможность отказа от авторства. Так как создать корректную подпись можно, лишь зная закрытый ключ, а он должен быть известен только владельцу, то владелец не может отказаться от своей подписи под документом.

- доказательное подтверждение авторства документа: Так как создать корректную подпись можно, лишь зная закрытый ключ, а он должен быть известен только владельцу, то владелец пары ключей может доказать своё авторство подписи под документом. В зависимости от деталей определения документа могут быть подписаны такие поля, как "автор", "внесённые изменения", "метка времени" и т.д.

Все эти свойства ЭП позволяют использовать её для следующих целей:

- Декларирование товаров и услуг (таможенные декларации),
- Регистрация сделок по объектам недвижимости,
- Использование в банковских системах,
- Электронная торговля и госзаказы,
- Контроль исполнения государственного бюджета,
- В системах обращения к органам власти,
- Для обязательной отчетности перед государственными учреждениями,
- Организация юридически значимого электронного документооборота,
- В расчетных и трейдинговых системах.

История возникновения

В 1976 году Уитфилдом Диффи и Мартином Хеллманом было впервые предложено понятие "электронная цифровая подпись", хотя они всего лишь предполагали, что схемы ЭЦП могут существовать.

В 1977 году, Рональд Ривест, Ади Шамир и Леонард Адлеман разработали криптографический алгоритм RSA, который без дополнительных модификаций можно использовать для создания примитивных цифровых подписей.
Вскоре после RSA были разработаны другие ЭЦП, такие как алгоритмы цифровой подписи Рабина, Меркле.
В 1984 году Шафи Гольдвассер, Сильвио Микали и Рональд Ривест первыми строго определили требования безопасности к алгоритмам цифровой подписи. Ими были описаны модели атак на алгоритмы ЭЦП, а также предложена схема GMR, отвечающая описанным требованиям.

Алгоритмы

Существует несколько схем построения цифровой подписи:
На основе алгоритмов симметричного шифрования. Данная схема предусматривает наличие в системе третьего лица - арбитра, пользующегося доверием обеих сторон. Авторизацией документа является сам факт зашифрования его секретным ключом и передача его арбитру
На основе алгоритмов асимметричного шифрования. На данный момент такие схемы ЭП наиболее распространены и находят широкое применение.
Кроме этого, существуют другие разновидности цифровых подписей (групповая подпись, неоспоримая подпись, доверенная подпись), которые являются модификациями описанных выше схем. Их появление обусловлено разнообразием задач, решаемых с помощью ЭП.

Использование хеш-функций

Поскольку подписываемые документы - переменного (и как правило достаточно большого) объёма, в схемах ЭП зачастую подпись ставится не на сам документ, а на его хеш. Для вычисления хэша используются криптографические хеш-функции, что гарантирует выявление изменений документа при проверке подписи. Хеш-функции не являются частью алгоритма ЭП, поэтому в схеме может быть использована любая надёжная хеш-функция.
Использование хеш-функций даёт следующие преимущества:

- Вычислительная сложность. Обычно хеш цифрового документа делается во много раз меньшего объёма, чем объём исходного документа, и алгоритмы вычисления хеша являются более быстрыми, чем алгоритмы ЭП. Поэтому формировать хэш документа и подписывать его получается намного быстрее, чем подписывать сам документ.
- Совместимость. Большинство алгоритмов оперирует со строками бит данных, но некоторые используют другие представления. Хеш-функцию можно использовать для преобразования произвольного входного текста в подходящий формат.
- Целостность. Без использования хеш-функции большой электронный документ в некоторых схемах нужно разделять на достаточно малые блоки для применения ЭП. При верификации невозможно определить, все ли блоки получены и в правильном ли они порядке.

Стоит заметить, что использование хеш-функции не обязательно при электронной подписи, а сама функция не является частью алгоритма ЭП, поэтому хеш-функция может использоваться любая или не использоваться вообще.
В большинстве ранних систем ЭП использовались функции с секретом, которые по своему назначению близки к односторонним функциям. Такие системы уязвимы к атакам с использованием открытого ключа, так как, выбрав произвольную цифровую подпись и применив к ней алгоритм верификации, можно получить исходный текст. Чтобы избежать

этого, вместе с цифровой подписью используется хеш-функция, то есть, вычисление подписи осуществляется не относительно самого документа, а относительно его хеша. В этом случае в результате верификации можно получить только хеш исходного текста, следовательно, если используемая хеш-функция криптографически стойкая, то получить исходный текст будет вычислительно сложно, а значит атака такого типа становится невозможной.

Симметричная схема

Симметричные схемы ЭП менее распространены чем асимметричные, так как после появления концепции цифровой подписи не удалось реализовать эффективные алгоритмы подписи, основанные на известных в то время симметричных шифрах. Первыми, кто обратил внимание на возможность симметричной схемы цифровой подписи, были основоположники самого понятия ЭП Диффи и Хеллман, которые опубликовали описание алгоритма подписи одного бита с помощью блочного шифра. Асимметричные схемы цифровой подписи опираются на вычислительно сложные задачи, сложность которых еще не доказана, поэтому невозможно определить, будут ли эти схемы сломаны в ближайшее время, как это произошло со схемой, основанной на задаче об укладке ранца. Также для увеличения криптостойкости нужно увеличивать длину ключей, что приводит к необходимости переписывать программы, реализующие асимметричные схемы, и в некоторых случаях перепроектировать аппаратуру. Симметричные схемы основаны на хорошо изученных блочных шифрах.

В связи с этим симметричные схемы имеют следующие преимущества:

Стойкость симметричных схем ЭП вытекает из стойкости используемых блочных шифров, надежность которых также хорошо изучена.

Если стойкость шифра окажется недостаточной, его легко можно будет заменить на более стойкий с минимальными изменениями в реализации.

Однако у симметричных ЭП есть и ряд недостатков:

Нужно подписывать отдельно каждый бит передаваемой информации, что приводит к значительному увеличению подписи. Подпись может превосходить сообщение по размеру на два порядка.

Сгенерированные для подписи ключи могут быть использованы только один раз, так как после подписывания раскрывается половина секретного ключа.

Из-за рассмотренных недостатков симметричная схема ЭЦП Диффи-Хелмана не применяется, а используется её модификация, разработанная Березиным и Дорошкевичем, в которой подписывается сразу группа из нескольких бит. Это приводит к уменьшению размеров подписи, но к увеличению объема вычислений. Для преодоления проблемы "одноразовости" ключей используется генерация отдельных ключей из главного ключа

Асимметричная схема

Схема, поясняющая алгоритмы подписи и проверки.

Асимметричные схемы ЭП относятся к криптосистемам с открытым ключом. В отличие от асимметричных алгоритмов шифрования, в которых зашифрование производится с помощью открытого ключа, а расшифрование - с помощью закрытого, в схемах цифровой подписи подписывание производится с применением закрытого ключа, а проверка - с применением открытого.

Общепризнанная схема цифровой подписи охватывает три процесса:

· Генерация ключевой пары. При помощи алгоритма генерации ключа равновероятным образом из набора возможных закрытых ключей выбирается закрытый ключ, вычисляется соответствующий ему открытый ключ.
· Формирование подписи. Для заданного электронного документа с помощью закрытого ключа вычисляется подпись.
· Проверка (верификация) подписи. Для данных документа и подписи с помощью открытого ключа определяется действительность подписи.
Для того, чтобы использование цифровой подписи имело смысл, необходимо выполнение двух условий:
· Верификация подписи должна производиться открытым ключом, соответствующим именно тому закрытому ключу, который использовался при подписании.
· Без обладания закрытым ключом должно быть вычислительно сложно создать легитимную цифровую подпись.
Следует отличать электронную цифровую подпись от кода аутентичности сообщения (MAC).

Подведение итогов. Фронтальный опрос.
Домашнее задание: Выучить основные определения. Подготовиться к самостоятельной работе по теме: Электронная цифровая подпись и ее использование.