Министерство образования и науки РФ

Уральский Государственный Лесотехнический Университет

Факультет экономики и управления

Заочное отделение

Курсовая работа

дисциплина: Технологии интернета

на тему: Цифровая подпись

Екатеринбург 2011

**Введение**

Информационные технологии шагают по планете. Сейчас сложно найти организацию, предприятие или фирму, офис которой не освещали бы экраны мониторов. Печатные машинки ушли в прошлое, уступив место компьютерам. Секретари хранят подготовленные шаблоны документов и перед распечаткой лишь подставляют нужные данные вместо того, чтобы всякий раз «отстукивать» полный текст. В то же самое время исследования, которые были проведены в странах с развитой информационной инфраструктурой, показали не уменьшение, а, наоборот, увеличение расхода бумаги. И дело не только в том, что современные принтеры в случае небольшой опечатки, допущенной сотрудником в тексте договора или платежного документа, позволяют производить макулатуру со скоростью от 12 листов в минуту. Ведь документ можно было бы вообще не распечатывать, ошибку исправить прямо в файле и передать партнерам или банку файл с конкретным документом — и никакой бумаги. Прочитать документ можно и с экрана монитора. Однако, ведя дела таким образом, можно попасть в ситуацию, когда недобросовестный партнер исправит в подготовленном договоре сумму сделки и предъявит этот файл как исходный со всеми печатями и подписями.

Говорят, что в старые времена разрубали монету и давали по одной половинке двум гонцам. Даже если они не были знакомы между собой, при встрече они могли сложить имеющиеся у них части монеты и убедиться, что служат общему делу. Предположим, что кто-то хочет передать вам конфиденциальное сообщение таким образом, чтобы прочесть его мог только адресат. В этом случае ему достаточно узнать ваш открытый ключ, а потом выполнить шифрование сообщения с его помощью. Полученный шифротекст может быть передан вам по открытым каналам связи. В соответствии со свойствами криптографии по открытому ключу исходное сообщение может быть восстановлено из такого шифротекста только обладателем секретного ключа. Предположим, что файл имеет достаточно большой размер. Конечно, его можно расшифровать с помощью открытого ключа (заодно проверив целостность), но удобнее все-таки иметь перед глазами открытый текст. Для этих целей используются так называемые шифрующие преобразования, которые из текста произвольной длины позволяют получить текст фиксированной длины существенно меньше исходного текста. А основным свойством таких преобразований является то, что при небольших изменениях исходного текста результаты преобразования меняются очень сильно, так что практически невозможно для двух различных осмысленных исходных текстов получить одинаковые шифр - преобразования. Как этим воспользоваться? Выполняется шифрование исходного текста, а уже результат шифруется асимметричным алгоритмом с использованием секретного ключа. Для проверки подлинности предъявляются шифротекст, открытый ключ и исходный текст. Во-первых, по исходному тексту тем же самым способом вычисляется шифр - преобразование, во-вторых, шифротекст расшифровывается с помощью открытого ключа. Если оба результата идентичны — значит, текст не претерпел изменений. Никто, кроме владельца секретного ключа, не сможет создать такой шифротекст. Этот факт позволяет использовать его в качестве личной подписи владельца секретного ключа под файлом с текстом документа — электронной цифровой подписи.

**Электронно-цифровая подпись**

Электронно-цифровая подпись (***ЭЦП***) — электронный аналог собственноручной подписи — используемый в системах электронного документооборота для придания электронному документу юридической силы, равной бумажному документу, подписанного собственноручной подписью правомочного лица и/или скрепленного печатью. Документ (файл), подписанный ЭЦП, гарантированно защищен от изменений — проверка подписи мгновенно выявит расхождение. ЭЦП обеспечивает проверку целостности документов, конфиденциальность, установление лица, отправившего документ. Это позволяет усовершенствовать процедуру подготовки, доставки, учета и хранения документов, гарантировать их достоверность. Главное преимущество использование ЭЦП — значительное сокращение временных и финансовых затрат на оформление и обмен документацией. Таким образом, по функциональности ЭЦП даже превосходит обычную подпись. Предположим, что две стороны (назовем их условно «А» и «Б») решили организовать между собой обмен документами на машинных носителях. Как должен выстраиваться документооборот между этими сторонами? В первую очередь, стороны должны договориться об использовании средств ЭЦП. Лучше, если это будет программный или программно-аппаратный комплекс, сертифицированный в нашей стране. После того, как средство ЭЦП выбрано, стороны должны выполнить генерирование ключей — по открытому и секретному (личному) ключу ЭЦП для каждой стороны.

Чтобы каждая сторона могла удостовериться в подлинности ЭЦП, поставленной под документом другой стороной, они должны обменяться открытыми ключами. Однако этот процесс не так прост, как может показаться. Ведь в случае конфликтной ситуации одна из сторон может заявить, что тот открытый ключ, который был использован при проверке ЭЦП под документом, не ее, а неизвестно чей. Сначала для документа должна быть выработана ЭЦП с использованием соответствующих технических средств и секретного ключа стороны «А».

Из исходного текста документа и его ЭЦП формируется электронный документ. Здесь нужно понимать, что электронный документ — это не просто файл на магнитном носителе с текстом документа, а файл, состоящий из двух частей: общей (в которой содержится текст) и особенной, содержащей все необходимые ЭЦП (рис. 3). Текст документа без ЭЦП — это не более чем обычный текст, который не имеет юридической силы. Его можно распечатать, передать по электронной почте, отредактировать, но нельзя установить его подлинность. ЭЦП без текста документа вообще представляет собой непереводимую игру букв. Восстановить документ по ЭЦП невозможно точно так же, как невозможно восстановить дворец по найденному кирпичу. ЭЦП сама по себе не имеет ни ценности, ни смысла.

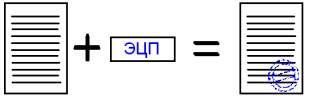


Рис. 3. Текст документа + ЭЦП = электронный документ

Чтобы обеспечить конфиденциальность при передаче по открытым каналам, он может быть зашифрован с использованием открытого ключа корреспондента — стороны «Б» (рис. 4).

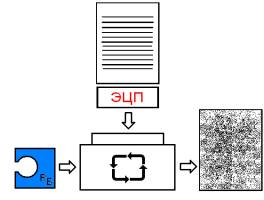


Рис. 4. Шифрование электронного документа с использованием открытого ключа получателя

Получившийся зашифрованный текст может быть безопасно передан стороне «Б», например, по электронной почте через Интернет. Сторона «Б», в свою очередь, должна сначала расшифровать полученный документ, используя свой секретный ключ (рис. 5).

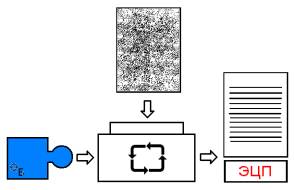


Рис. 5. Расшифровка электронного документа с использованием секретного ключа получателя

Расшифровав текст, его можно прочитать, однако, чтобы убедиться в том, что он передан именно стороной «A», нужно проверить цифровую подпись, пришедшую вместе с текстом электронного документа (рис. 6).

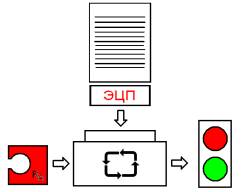


Рис. 6. Проверка ЭЦП с использованием открытого ключа отправителя.

Так выглядит схема передачи файла из пункта «А» в пункт «Б». Если осуществляется передача в обратном направлении, в описанных шагах нужно поменять местами ключи отправителя и получателя. Но это не единственное приложение криптографии с открытым ключом. Например, две стороны хотят составить договор в электронном виде и защитить его от внесения изменений. Поскольку стороны равны перед законом, каждая из них должна подписать один и тот же документ (файл) с использованием своего личного (секретного) ключа, после чего обменяться полученными цифровыми подписями. В этом случае (при наличии заверенных карточек открытых ключей каждой из сторон) проверить подлинность файла не составит труда. Выполняется проверка ЭЦП точно так же, как было описано в примере с передачей сообщений. Итак, чтобы установить доверительные отношения в электронном документообороте, стороны должны: 1. Заключить соглашение об использовании электронных документов. 2. Сгенерировать ключи в соответствии с документацией на выбранный комплекс средств ЭЦП. 3. Принять меры к защите личного (секретного) ключа ЭЦП от компрометации (разглашения). Носитель, на котором хранится личный ключ, определяется используемыми средствами ЭЦП и может представлять жесткий диск компьютера, гибкий диск (дискету) или устройство хранения на базе энергонезависимой памяти. Как правило, личный ключ дополнительно шифруется, и для его использования нужно ввести пароль или PIN-код. В любом случае, если ключ хранится на несъемном диске, нужно ограничить доступ к компьютеру со средствами ЭЦП. Если же ключ хранится на съемном носителе, это устройство следует хранить, например, в сейфе вместе с печатью организации. 4. Обменяться открытыми ключами ЭЦП и заверенными карточками открытого ключа ЭЦП.

**Общая схема электронной подписи**

Схема электронной подписи обычно включает в себя:

1) Алгоритм генерации ключевых пар пользователя;

2) Функцию вычисления подписи;

3) Функцию проверки подписи.

Функция вычисления подписи на основе документа и секретного ключа пользователя вычисляет собственно подпись. В зависимости от алгоритма функция вычисления подписи может быть детерминированной (точной) или вероятностной. Детерминированные функции всегда вычисляют одинаковую подпись по одинаковым входным данным.

Вероятностные функции вносят в подпись элемент случайности, что усиливает криптостойкость алгоритмов ЭЦП. Однако, для вероятностных схем необходим надёжный источник случайности (либо аппаратный генератор шума, либо криптографически надёжный генератор псевдослучайных бит), что усложняет реализацию.

В настоящее время детерминированные схемы практически не используются. Даже в изначально детерминированные (точные) алгоритмы сейчас внесены модификации, превращающие их в вероятностные (так, в алгоритм подписи **RSA** вторая версия стандарта PKCS#1 добавила предварительное преобразование данных (OAEP), включающее в себя, среди прочего, зашумление). **RSA** стал первым алгоритмом такого типа, пригодным и для шифрования и для цифровой подписи. Алгоритм используется в большом числе криптографических приложений.

**История RSA**

Описание **RSA** было опубликовано в 1977 году Рональдом Райвестом (Ronald Linn Rivest), Ади Шамиром (Adi Shamir) и Леонардом Адлеманом (Leonard Adleman) из Массачусетского Технологического Института (MIT).Британский математик Клиффорд Кокс (Clifford Cocks), работавший в центре правительственной связи (GCHQ) Великобритании, описал аналогичную систему в 1973 году во внутренних документах центра, но эта работа не была раскрыта до 1977 года и Райвест, Шамир и Адлеман разработали RSA независимо от работы Кокса.

***Описание алгоритма:*** Безопасность алгоритма электронной подписи **RSA** основана на трудности задачи разложения на множители. Алгоритм использует два ключа — открытый (public) и секретный (private), вместе открытый и соответствующий ему секретный ключи образуют пару ключей (keypair). Открытый ключ не требуется сохранять в тайне, он используется для зашифровывания данных. Если сообщение было зашифровано открытым ключом, то расшифровать его можно только соответствующим секретным ключом.

**Применение RSA**

Система RSA используется для защиты программного обеспечения и в схемах цифровой подписи. Также она используется в открытой системе шифрования PGP.

Из-за низкой скорости шифрования (около 30 кбит/с при 512 битном ключе на процессоре 2 ГГц), сообщения обычно шифруют с помощью более производительных симметричных алгоритмов со случайным ключом (сеансовый ключ), а с помощью RSA шифруют лишь сам ключ.

**Алгоритм DSA** (**Digital Signature Algorithm**):

Алгоритм с использованием открытого ключа для создания электронной подписи, но не для шифрования. Секретное создание шифр - значения и публичная проверка ее означает, что только один человек может создать шифр - значение сообщения, но любой может проверить ее корректность. Основан алгоритм на вычислительной сложности взятия логарифмов в конечных полях.

**История DSA:**

Алгоритм был предложен Национальным Институтом Стандартов и Технологий (США) в августе 1991 и является запатентованным U.S. Patent 5231668 (англ.), но институт сделал этот патент доступным для использования без лицензионных отчислений.

**Симметричные криптосистемы**

Симметричные криптосистемы (также симметричное шифрование, симметричные шифры) — способ шифрования, в котором для зашифровывания и расшифровывания применяется один и тот же криптографический ключ. До изобретения схемы асимметричного шифрования единственным существовавшим способом являлось симметричное шифрование. Ключ алгоритма должен сохраняться в секрете обеими сторонами. Ключ алгоритма выбирается сторонами до начала обмена сообщениями.

В настоящее время симметричные шифры - это:

**1. *Блочные шифры*** - обрабатывают информацию блоками определенной длины (обычно 64, 128 бит), применяя к блоку ключ в установленном порядке, как правило, несколькими циклами перемешивания и подстановки, называемыми раундами. Результатом повторения раундов является лавинный эффект - нарастающая потеря соответствия битов между блоками открытых и зашифрованных данных.

**2. *Поточные шифры*** - в которых шифрование проводится над каждым битом либо байтом исходного (открытого) текста с использованием гаммирования. Поточный шифр может быть легко создан на основе блочного (например, ГОСТ 28147-89 в режиме гаммирования), запущенного в специальном режиме.

**Криптографическая система с открытым ключом**

Криптографическая система с открытым ключом (или Асимметричное шифрование, Асимметричный шифр) — система шифрования информации, при которой ключ, которым зашифровывается сообщение и само зашифрованное сообщение передаётся по открытому, (то есть незащищённому, доступному для наблюдения) каналу. Для генерации открытого ключа и для прочтения зашифрованного сообщения получатель использует секретный ключ. Криптографические системы с открытым ключом в настоящее время широко применяются в различных сетевых протоколах, в частности, в протоколе SSL и основанных на нём протоколах прикладного уровня HTTPS, SSH и т. д.

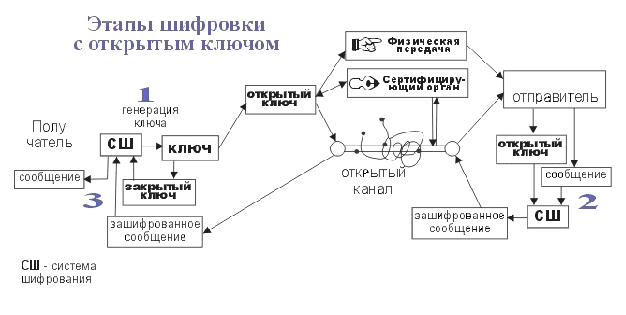


Рис. 7. Этапы шифровки с открытым ключом.

**Этапы шифровки с открытым ключом**

1. Получатель генерирует ключ. Ключ разбивается на открытую и закрытую часть. При этом открытый ключ не должен передаваться по открытому каналу. Либо его подлинность должна быть гарантирована некоторым сертифицирующим органом.

2.Отправитель с помощью открытого ключа шифрует сообщение.

3.Получатель с помощью закрытого ключа дешифрует сообщение.

Недостаток метода: хотя сообщение надежно шифруется, но «засвечиваются» получатель и отправитель самим фактом пересылки шифрованного сообщения.

Общая идея криптографической системы с открытым ключом заключается в использовании при зашифровке сообщения такой функции от открытого ключа и сообщения (шифр -функции), которую алгоритмически очень трудно обратить, то есть вычислить по значению функции её аргумент, даже зная значение ключа.

**Особенности системы**

***Преимущество*** асимметричных шифров перед симметричными шифрами состоит в отсутствии необходимости передачи секретного ключа. Сторона, желающая принимать зашифрованные тексты, в соответствии с используемым алгоритмом вырабатывает пару «открытый ключ — закрытый ключ». Значения ключей связаны между собой, однако вычисление одного значения из другого должно быть невозможным с практической точки зрения. Открытый ключ публикуется в открытых справочниках и используется для шифрования информации контрагентом. Закрытый ключ держится в секрете и используется для расшифровывания сообщения, переданного владельцу пары ключей. Начало асимметричным шифрам было положено в 1976 году в работе Уитфилда Диффи и Мартина Хеллмана «Новые направления в современной криптографии». Они предложили систему обмена общим секретным ключом на основе проблемы дискретного логарифма. Вообще, в основу известных асимметричных криптосистем кладётся одна из сложных математических проблем, которая позволяет строить односторонние функции и функции-ловушки. Например, криптосистема Ривеста-Шамира-Адельмана использует проблему факторизации больших чисел, а криптосистемы Меркля-Хеллмана и Хора-Ривеста опираются на так называемую задачу об укладке рюкзака.

Недостатки ***-*** асимметричные криптосистемы требуют существенно больших вычислительных ресурсов. Кроме того, необходимо обеспечить аутентичность (подлинность) самих публичных ключей, для чего обычно используют сертификаты.

Гибридная (или комбинированная) криптосистема — это система шифрования, обладающая всеми достоинствами криптосистемы с открытым ключом, но лишенная ее основного недостатка — низкой скорости шифрования.

***Принцип:*** Криптографические системы используют преимущества двух основных криптосистем: симметричной и асимметричной криптографии. На этом принципе построены такие программы, как PGP и GnuPG.

Основной недостаток асимметричной криптографии состоит в низкой скорости из-за сложных вычислений, требуемых ее алгоритмами, в то время как симметричная криптография традиционно показывает блестящую скорость работы. Однако симметричные криптосистемы имеет один существенный недостаток — её использование предполагает наличие защищенного канала для передачи ключей. Для преодоления этого недостатка прибегают к асимметричным криптосистемам, которые используют пару ключей: открытый и закрытый.

***Шифрование:*** Большинство шифровальных систем работают следующим образом. Для симметричного алгоритма (3DES, IDEA, AES или любого другого) генерируется случайный ключ. Такой ключ, как правило, имеет размер от 128 до 512 бит (в зависимости от алгоритма). Затем используется симметричный алгоритм для шифрования сообщения. В случае блочного шифрования необходимо использовать режим шифрования (например, CBC), что позволит шифровать сообщение с длиной, превышающей длину блока. Что касается самого случайного ключа, он должен быть зашифрован с помощью открытого ключа получателя сообщения, и именно на этом этапе применяется криптосистема с открытым ключом (RSA или Алгоритм Диффи — Хеллмана). Поскольку случайный ключ короткий, его шифрование занимает немного времени. Шифрование набора сообщений с помощью асимметричного алгоритма — это задача вычислительно более сложная, поэтому здесь предпочтительнее использовать симметричное шифрование. Затем достаточно отправить сообщение, зашифрованное симметричным алгоритмом, а также соответствующий ключ в зашифрованном виде. Получатель сначала расшифровывает ключ с помощью своего секретного ключа, а затем с помощью полученного ключа получает и всё сообщение.

**Цифровая подпись обеспечивает:**

**\*** Удостоверение источника документа. В зависимости от деталей определения документа могут быть подписаны такие поля, как «автор», «внесённые изменения», «метка времени» и т. д.

\* Защиту от изменений документа. При любом случайном или преднамеренном изменении документа (или подписи) изменится шифр, следовательно, подпись станет недействительной.

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

**Возможны следующие угрозы цифровой подписи:**

\*Злоумышленник может попытаться подделать подпись для выбранного им документа.

\*Злоумышленник может попытаться подобрать документ к данной подписи, чтобы подпись к нему подходила.

При использовании надёжной шифр - функции, вычислительно сложно создать поддельный документ с таким же шифром, как у подлинного. Однако, эти угрозы могут реализоваться из-за слабостей конкретных алгоритмов кэширования, подписи, или ошибок в их реализациях. Тем не менее, возможны ещё такие угрозы системам цифровой подписи:

\*Злоумышленник, укравший закрытый ключ, может подписать любой документ от имени владельца ключа.

\*Злоумышленник может обманом заставить владельца подписать какой-либо документ, например используя протокол слепой подписи.

\*Злоумышленник может подменить открытый ключ владельца на свой собственный, выдавая себя за него.

**Управление ключами от ЭЦП**

Важной проблемой всей криптографии с открытым ключом, в том числе и систем ЭЦП, является управление открытыми ключами. Необходимо обеспечить доступ любого пользователя к подлинному открытому ключу любого другого пользователя, защитить эти ключи от подмены злоумышленником, а также организовать отзыв ключа в случае его компрометации.

Задача защиты ключей от подмены решается с помощью сертификатов. Сертификат позволяет удостоверить заключённые в нём данные о владельце и его открытый ключ подписью какого-либо доверенного лица. В централизованных системах сертификатов используются центры сертификации, поддерживаемые доверенными организациями. В децентрализованных системах путём перекрёстного подписывания сертификатов знакомых и доверенных людей каждым пользователем строится сеть доверия.

Управлением ключами занимаются центры распространения сертификатов. Обратившись к такому центру, пользователь может получить сертификат какого-либо пользователя, а также проверить, не отозван ли ещё тот или иной открытый ключ.

**Использование ЭЦП в России**

После становления ЭЦП при использовании в электронном документообороте между кредитными организациями и кредитными бюро в 2005-м году активно стала развиваться инфраструктура электронного документооборота между налоговыми органами и налогоплательщиками. Начали работать приказ Министерства по налогам и сборам Российской Федерации от 2 апреля 2002 г. N БГ-3-32/169 «Порядок представления налоговой декларации в электронном виде по телекоммуникационным каналам связи». Порядок представления налоговой декларации в электронном виде по телекоммуникационным каналам связи определяет общие принципы организации информационного обмена при представлении налогоплательщиками налоговой декларации в электронном виде по телекоммуникационным каналам связи.

**Использование ЭЦП в других странах**

Система электронных подписей широко используется в Эстонской Республике, где введена программа ID-карт, которыми снабжены 3/4 населения страны. При помощи электронной подписи в марте этого года были проведены выборы в местный парламент — Рийгикогу. При голосовании электронную подпись использовали 400 000 человек. Кроме того, при помощи электронной подписи можно отправить налоговую декларацию, таможенную декларацию, различные анкеты как в местные самоуправления, так и в государственные органы. В крупных городах при помощи ID-карты возможна покупка месячных автобусных билетов. Все это осуществляется через центральный гражданский портал Eesti.ee . Эстонская ID-карта является обязательной для всех жителей с 15 лет, проживающих временно или постоянно на территории Эстонии.

**Заключение**

электронный цифровой подпись криптографический шифр

В России юридически значимый сертификат электронной подписи выдаёт удостоверяющий центр на основании государственной лицензии. Правовые условия использования электронной цифровой подписи в электронных документах регламентирует Федеральный закон от 10.01.2002 N 1-ФЗ «Об электронной цифровой подписи» Еще до вступления в силу этого закона термин "электронная цифровая подпись" содержится более чем в полусотне нормативных актов, но лишь этот закон содержит комплексную правовую базу для широкого ее использования в предпринимательской деятельности и развития электронной коммерции в нашей стране. В соответствии с Законом владельцем может быть только физическое лицо. Такой подход принят и в европейском законодательстве. Естественно, как и в случае с собственноручной подписью, физическое лицо может действовать от имени юридического лица, но на такое полномочие обязательно должно быть указано в сертификате ключа подписи. В законодательстве других стран, например США, допускается принадлежность электронной подписи не только физическим, но и юридическим лицам. "Американский" подход неудачен, поскольку при этом возрастает вероятность несанкционированного использования электронной подписи юридического лица, при котором сложно установить конкретное физическое лицо, осуществившее подписание электронного документа.

**Список литературы**

1. Петров А.А Компьютерная безопасность. Криптографические методы защиты.

2. "Методы и средства защиты информации" (курс лекций) Авторские права: Беляев А.В.

3. Криптография

4. Александр Володин «Кто заверит ЭЦП» - журнал «Банковские системы» - ноябрь 2000

5. Теоретические основы - Безопасность информационных систем – Криптографические системы

6. Криптографические алгоритмы с открытым ключом

7. Современные кpиптогpафические методы защиты информации.