Содержание

Введение

Криптография - наука о защите информации от прочтения ее посторонними. Защита достигается шифрованием, т.е. преобразованием, которые делают защищенные входные данные труднораскрываемыми по входным данным без знания специальной ключевой информации - ключа. Под ключом понимается легко изменяемая часть криптосистемы, хранящаяся в тайне и определяющая, какое шифрующие преобразование из возможных выполняется в данном случае. Криптосистема - семейство выбираемых с помощью ключа обратимых преобразований, которые преобразуют защищаемый открытый текст в шифрограмму и обратно.

Желательно, чтобы методы шифрования обладали минимум двумя свойствами:

- законный получатель сможет выполнить обратное преобразование и расшифровать сообщение;
- криптоаналитик противника, перехвативший сообщение, не сможет восстановить по нему исходное сообщение без таких затрат времени и средств, которые сделают эту работу нецелесообразной.

Цель курсовой работы: познакомиться с основами криптографической защиты информации. Для достижения данной цели в работе рассмотрены:

1. история криптографии, в которую включены основные задачи криптографии;
2. основные понятия криптографии (конфиденциальность, целостность, аутентификация, цифровая подпись);
3. криптографические средства защиты (криптосистемы, принципы работы криптосистемы, распространение ключей, алгоритмы шифрования и т.д.).

1.Экскурс в историю электронной криптографии

Появление в середине двадцатого столетия первых электронно-вычислительных машин кардинально изменило ситуацию в области шифрования (криптографии). С проникновением компьютеров в различные

сферы жизни возникла принципиально новая отрасль - информационная индустрия. В 60-х и частично в 70-х годах проблема защиты информации решалась достаточно эффективно применением в основном организационных мер. К ним относились, прежде всего, режимные мероприятия, охрана, сигнализация и простейшие программные средства защиты информации. Эффективность использования указанных средств достигалась за счет концентрации информации на вычислительных центрах, как правило, автономных, что способствовало обеспечению защиты относительно малыми средствами. "Рассосредоточение" информации по местам ее хранения и обработки, чему в немалой степени способствовало появление в огромных количествах дешевых персональных компьютеров и построенных на их основе локальных и глобальных национальных и транснациональных сетей ЭВМ, использующих спутниковые каналы связи, создание высокоэффективных систем разведки и добычи информации, обострило ситуацию с защитой информации.

Проблема обеспечения необходимого уровня защиты информации оказалась (и это предметно подтверждено как теоретическими исследованиями, так и опытом практического решения) весьма сложной, требующей для своего решения не просто осуществления некоторой совокупности научных, научно-технических и организационных мероприятий и применения специфических средств и методов, а создания целостной системы организационных мероприятий и применения специфических средств и методов по защите информации.

Объем циркулирующей в обществе информации стабильно возрастает. Популярность всемирной сети Интернет в последние годы способствует удваиванию информации каждый год. Фактически, на пороге нового тысячелетия человечество создало информационную цивилизацию, в которой от успешной работы средств обработки информации зависит благополучие и даже выживание человечества в его нынешнем качестве.

Произошедшие за этот период изменения можно охарактеризовать следующим образом:

-объемы обрабатываемой информации возросли за полвека на несколько порядков;

-доступ к определенным данным позволяет контролировать значительные материальные и финансовые ценности;

-информация приобрела стоимость, которую даже можно подсчитать;

-характер обрабатываемых данных стал чрезвычайно многообразным и более не сводится к исключительно текстовым данным;

-информация полностью "обезличилась", т.е. особенности ее материального представления потеряли свое значение - сравните письмо прошлого века и современное послание по электронной почте;

-характер информационных взаимодействий чрезвычайно усложнился, и наряду с классической задачей защиты передаваемых текстовых сообщений от несанкционированного прочтения и искажения возникли новые задачи сферы защиты информации, ранее стоявшие и решавшиеся в рамках используемых "бумажных" технологий - например, подпись под электронным документом и вручение электронного документа "под расписку" - речь о подобных "новых" задачах криптографии еще впереди;

-субъектами информационных процессов теперь являются не только люди, но и созданные ими автоматические системы, действующие по заложенной в них программе;

-вычислительные "способности" современных компьютеров подняли на совершенно новый уровень как возможности по реализации шифров, ранее немыслимых из-за своей высокой сложности, так и возможности аналитиков по их взлому. Перечисленные выше изменения привели к тому, что очень быстро после распространения компьютеров в деловой сфере практическая криптография сделала в своем развитии огромный скачок, причем сразу по нескольким направлениям:

Во-первых, были разработаны стойкие блочные с секретным ключом, предназначенные для решения классической задачи - обеспечения секретности и целостности, передаваемых или хранимых данных, они до сих пор остаются "рабочей лошадкой" криптографии, наиболее часто используемыми средствами криптографической защиты;

Во-вторых, были созданы методы решения новых, нетрадиционных задач сферы защиты информации, наиболее известными из которых являются задача подписи цифрового документа и открытого распределения ключей. В современном мире информационный ресурс стал одним из наиболее мощных рычагов экономического развития. Владение информацией необходимого качества в нужное время и в нужном месте является залогом успеха в любом виде хозяйственной деятельности. Монопольное обладание определенной информацией оказывается зачастую решающим преимуществом в конкурентной борьбе и предопределяет, тем самым, высокую цену "информационного фактора".

Широкое внедрение персональных ЭВМ вывело уровень "информатизации" деловой жизни на качественно новую ступень. Ныне трудно представить себе фирму или предприятие (включая самые мелкие), которые не были бы вооружены современными средствами обработки и передачи информации. В ЭВМ на носителях данных накапливаются значительные объемы информации, зачастую носящей конфиденциальный характер или представляющей большую ценность для ее владельца.

1.1. Основные задачи криптографии.

Задача криптографии, т.е. тайная передача, возникает только для информации, которая нуждается в защите. В таких случаях говорят, что информация содержит тайну или является защищаемой, приватной, конфиденциальной, секретной. Для наиболее типичных, часто встречающихся ситуаций такого типа введены даже специальные понятия:

- государственная тайна;
- военная тайна;

- коммерческая тайна;
- юридическая тайна;
- врачебная тайна и т. д.

Далее мы будем говорить о защищаемой информации, имея в виду следующие признаки такой информации:

1. имеется какой-то определенный круг законных пользователей, которые имеют право владеть этой информацией;
2. имеются незаконные пользователи, которые стремятся овладеть этой информацией с тем, чтобы обратить ее себе во благо, а законным пользователям во вред.

1.2. Криптография сегодня

Криптография - это наука об обеспечении безопасности данных. Она занимается поисками решений четырех важных проблем безопасности - конфиденциальности, аутентификации, целостности и контроля участников взаимодействия. Шифрование - это преобразование данных в нечитабельную форму, используя ключи шифрования-расшифровки. Шифрование позволяет обеспечить конфиденциальность, сохраняя информацию в тайне от того, кому она не предназначена.

2. Основные понятия.

Целью настоящего раздела является определение основных понятий криптографии.

2.1. Криптография.

В переводе с греческого языка слово *криптография* означает тайнопись. Смысл этого термина выражает основное предназначение криптографии – защитить или сохранить в тайне необходимую информацию.

Криптография дает средства для защиты информации, и поэтому она является частью деятельности по обеспечению безопасности информации.

Существуют различные методы *защиты информации* . Можно, например, физически ограничить доступ к информации путем хранения ее в надежном сейфе или строго охраняемом помещении. При хранении информации такой метод удобен, однако при ее передаче приходится использовать другие средства.

Можно воспользоваться одним из известных методов сокрытия информации:

· скрыть канал передачи информации, используя нестандартный способ передачи сообщений;

· замаскировать канал передачи закрытой информации в открытом канале связи, например, спрятав информацию в безобидном «контейнере» с использованием тех или других стенографических способов либо обмениваясь открытыми сообщениями, смысл которых согласован заранее;

· существенно затруднить возможность перехвата, противником передаваемых сообщений, используя специальные методы передачи по широкополосным каналам, сигнала под уровнем шумов, либо с использованием «прыгающих» несущих частот и т.п.

В отличие от перечисленных методов криптография не «прячет» передаваемые сообщения, а преобразует их в форму, недоступную для понимания противником. При этом обычно исходят из предположения о полном контроле противником канала связи. Это означает, что противник

может не только пассивно перехватывать передаваемые сообщения для последующего их анализа, но и активно изменять их, а также отправлять поддельные сообщения от имени одного из абонентов.

Также существуют и другие проблемы защиты передаваемой информации. Например, при полностью открытом обмене возникает проблема достоверности полученной информации. Для ее решения необходимо обеспечить:

· проверку и подтверждение подлинности содержания источника сообщения;

· предотвращение и обнаружение обмана и других умышленных нарушений со стороны самих участников информационного обмена.

Для решения этой проблемы обычные средства, применяемые при построении систем передачи информации, подходят далеко не всегда. Именно криптография дает средства для обнаружения обмана в виде подлога или отказа от ранее совершенных действий, а также других неправомерных действий.

Поэтому, современная *криптография* является областью знаний, связанной с решением таких проблем безопасности информации, как конфиденциальность, целостность, аутентификация и невозможность отказа сторон от авторства. Достижение этих требований и составляет основные цели криптографии.

Обеспечение *конфиденциальности* –решение проблемы защиты информации от ознакомления с ее содержанием со стороны лиц, не имеющих права доступа к ней.

Обеспечение *целостности* –гарантирование невозможности несанкционированного изменения информации. Для гарантии целостности необходим простой и надежный критерий обнаружения любых манипуляций с данными. Манипуляции с данными включают вставку, удаление и замену.

Обеспечение *аутентификации* -разработка методов подтверждения подлинности сторон (идентификация) и самой информации в процессе информационного взаимодействия. Информация, передаваемая по каналу

связи, должна быть аутентифицирована по источнику, времени создания, содержанию данных, времени пересылки и т.д.

Обеспечение *невозможности отказа от авторства или приписывания авторства* -предотвращение возможности отказа субъектов от некоторых из совершенных ими действий. Рассмотрим средства для достижения этих целей более подробно.

2.2 Конфиденциальность

Традиционной задачей криптографии является проблема обеспечения конфиденциальности информации при передаче сообщений по контролируемому противником каналу связи. В простейшем случае эта задача описывается взаимодействием трех субъектов (сторон). Владелец информации, называемый обычно *отправителем* , осуществляет преобразование исходной (*открытой*) информации (сам процесс преобразования называется *шифрованием*) в форму передаваемых *получателю* по открытому каналу связи *шифрованных* сообщений с целью ее защиты от противника.

Рис. 1. Передача шифрованной информации

Отправитель Противник Получатель

Под *противником* понимается любой субъект, не имеющий права ознакомления с содержанием передаваемой информации. В качестве противника может выступать *криптоаналитик* , владеющий методами раскрытия шифров. Законный получатель информации осуществляет *расшифрование* полученных сообщений. Противник пытается овладеть защищаемой информацией (его действия обычно называют *атаками*). При этом он может совершать как пассивные, так и активные действия. *Пассивные* атаки связаны с прослушиванием, анализом трафика, перехватом, записью передаваемых шифрованных сообщений, *дешифрованием* , т.е. попытками «взломать» защиту с целью овладения информацией.

При проведении *активных* атак противник может прерывать процесс передачи сообщений, создавать поддельные (сфабрикованные) или модифицировать передаваемые шифрованные сообщения. Эти активные действия называют *имитации* и *подмены* соответственно.

Под *шифром* обычно понимается семейство обратимых преобразований, каждое из которых определяется некоторым параметром, называемым ключом, а также порядком применения данного преобразования, называемым *режимом преобразования*. Формальное определение шифра будет дано ниже.

Ключ - это важнейший компонент шифра, отвечающий за выбор преобразования, применяемого для зашифрования конкретного сообщения. Обычно ключ представляет собой некоторую буквенную или числовую последовательность. Эта последовательность как бы «настраивает» алгоритм шифрования.

Каждое преобразование однозначно определяется ключом и описывается некоторым *криптографическим алгоритмом*. Один и тот же криптографический алгоритм может применяться для шифрования в различных режимах. Тем самым реализуются различные способы шифрования (простая замена, гаммирование т.п.). Каждый режим шифрования имеет как свои преимущества, так и недостатки. Поэтому выбор режима зависит от конкретной ситуации. При расшифровании используется криптографический алгоритм, который в общем случае может отличаться от алгоритма, применяемого для зашифрования сообщения. Соответственно могут различать ключи зашифрования и расшифрования. Пару алгоритмов зашифрования и расшифрования обычно называют *шифрсистемой*, а реализующие их устройства - *шифртехникой*.

2.3. Целостность

Наряду с конфиденциальностью не менее важной задачей является обеспечение целостности информации, другими словами,- неизменности ее в процессе передачи или хранении. Решение этой задачи предполагает

разработку средств, позволяющих обнаруживать не столько случайные искажения (для этой цели вполне подходят методы теории кодирования с обнаружением и исправлением ошибок), сколько целенаправленное навязывание противником ложной информации. Для этого в передаваемую информацию вносится избыточность. Как правило, это достигается добавлением к сообщению некоторой проверочной комбинации, вычисляемой с помощью специального алгоритма и играющей роль контрольной суммы для проверки целостности полученного сообщения. Главное отличие такого метода от методов теории кодирования состоит в том, что алгоритм выработки проверочной комбинации является «криптографическим», то есть зависящим от секретного ключа. Без знания секретного ключа вероятность успешного навязывания противником искаженной или ложной информации мала. Такая вероятность служит мерой *имитостойкости* шифра, то есть способности самого шифра противостоять активным атакам со стороны противника.

2.4. Аутентификация

Аутентификация - установление подлинности. В общем случае этот термин может относиться ко всем аспектам информационного взаимодействия: сеансу связи, сторонам, передаваемым сообщениям и т.д.

Установление подлинности (то есть проверка и подтверждение) всех аспектов информационного взаимодействия является важной составной частью проблемы обеспечения достоверности получаемой информации. Особенно остро эта проблема стоит в случае не доверяющих друг другу сторон, когда источником угроз может служить не только третья сторона (противник), но и сторона, с которой осуществляется взаимодействие.

Рассмотрим эти вопросы.

Применительно к сеансу связи (транзакции) аутентификация означает проверку: целостности соединения, невозможности повторной передачи данных противником и своевременности передачи данных. Для этого, как правило, используют дополнительные параметры, позволяющие «сцепить»

передаваемые данные в легко проверяемую последовательность. Это достигается, например, путем вставки в сообщения некоторых специальных чисел или *меток времени* . Они позволяют предотвратить попытки повторной передачи, изменения порядка следования или обратной отсылки части переданных сообщений. При этом такие вставки в передаваемом сообщении необходимо защищать (например, с помощью шифрования) от возможных подделок и искажений.

Применительно к сторонам взаимодействия аутентификация означает проверку одной из сторон того, что взаимодействующая сторона - именно та, за которую она себя выдает. Часто аутентификацию сторон называют также *идентификацией* .

Основным средством для проведения идентификации являются *протоколы идентификации* , позволяющие осуществлять идентификацию (и аутентификацию) каждой из участвующих во взаимодействии и не доверяющих друг другу сторон. Различают *протоколы односторонней* и *взаимной идентификации* .

Протокол - это распределенный алгоритм, определяющий последовательность действий каждой из сторон. В процессе выполнения протокола идентификации каждая из сторон не передает никакой информации о своем секретном ключе, а хранит его у себя и использует для формирования ответных сообщений на запросы, поступающие при выполнении протокола.

Наконец, применительно к самой информации аутентификация означает проверку того, что информация, передаваемая по каналу, является подлинной по содержанию, источнику, времени создания, времени пересылки и т.д.

Проверка подлинности содержания информации сводится, по сути, к проверке ее неизменности (с момента создания) в процессе передачи или хранения, то есть проверке целостности.

Аутентификация источника данных означает подтверждение того, что исходный документ был создан именно заявленным источником.

Заметим, что если стороны доверяют друг другу и обладают общим секретным ключом, то аутентификацию сторон можно обеспечить применением кода аутентификации. Действительно, каждое успешно декорированное получателем сообщение может быть создано только отправителем, так как только он знает их общий секретный ключ. Для не доверяющих друг другу сторон решение подобных задач с использованием общего секретного ключа становится невозможным. Поэтому при аутентификации источника данных нужен механизм цифровой подписи, который будет рассмотрен ниже.

В целом, аутентификация источника данных выполняет ту же роль, что и протокол идентификации. Отличие заключается только в том, что в первом случае имеется некоторая передаваемая информация, авторство которой требуется установить, а во втором требуется просто установить сторону, с которой осуществляется взаимодействие.

2.5. Цифровая подпись

В некоторых ситуациях, например в силу изменившихся обстоятельств, отдельные лица могут отказаться от ранее принятых обстоятельств. В связи с этим необходим некоторый механизм, препятствующий подобным попыткам.

Так как в данной ситуации предполагается, что стороны не доверяют друг другу, то использование общего секретного ключа для решения поставленной проблемы становится невозможным. Отправитель может отказаться от факта передачи сообщения, утверждая, что его создал сам получатель (*отказ от авторства*). Получатель легко может модифицировать, подменить или создать новое сообщение, а затем утверждать, что оно получено от отправителя (*приписывание авторства*). Ясно, что в такой ситуации арбитр при решении спора не будет иметь возможность установить истину.

Основным механизмом решения этой проблемы является так называемая *цифровая подпись* .

Схема цифровой подписи включает два алгоритма, один - для вычисления, а второй - для проверки подписи. Вычисление подписи может быть выполнено только автором подписи. Алгоритм проверки должен быть общедоступным, чтобы проверить правильность подписи мог каждый.

Для создания схемы цифровой подписи можно использовать симметричные шифрсистемы. В этом случае подписью может служить само зашифрованное на секретном ключе сообщение. Однако основной недостаток таких подписей состоит в том, что они являются одноразовыми: после каждой проверки секретный ключ становится известным. Единственный выход из этой ситуации в рамках использования симметричных шифрсистем - это введение доверенной третьей стороны, выполняющей функции посредника, которому доверяют обе стороны. В этом случае вся информация пересылается через посредника, он осуществляет перешифрование сообщений с ключа одного из абонентов на ключ другого. Естественно, эта схема является крайне неудобной.

Два подхода к построению системы цифровой подписи при использовании шифрсистем с открытым ключом:

1. В преобразовании сообщения в форму, по которой можно восстановить само сообщение и тем самым проверить правильность «подписи». В данном случае подписанное сообщение имеет ту же длину, что и исходное сообщение. Для создания такого «подписанного сообщения» можно, например, произвести зашифрование исходного сообщения на секретном ключе автора подписи. Тогда каждый может проверить правильность подписи путем расшифрования подписанного сообщения на открытом ключе автора подписи;

2. Подпись вычисляется и передается вместе с исходным сообщением. Вычисление подписи заключается в преобразовании исходного сообщения в некоторую цифровую комбинацию (которая и является подписью). Алгоритм вычисления подписи должен зависеть от секретного ключа пользователя. Это необходимо для того, чтобы воспользоваться подписью мог бы только

владелец ключа. В свою очередь, алгоритм проверки правильности подписи должен быть доступен каждому. Поэтому этот алгоритм зависит от открытого ключа пользователя. В данном случае длина подписи не зависит от длины подписываемого сообщения.

С проблемой цифровой подписи возникла проблема построения бесключевых криптографических *хэш-функций*. Дело в том, что при вычислении цифровой подписи оказывается более удобным осуществить сначала хэш-функции, то есть свертку текста в некоторую комбинацию фиксированной длины, а затем уже подписывать полученную комбинацию с помощью секретного ключа. При этом функция хэширования, хотя и не зависит от ключа и является открытой, должна быть «криптографической». Имеется в виду свойство *односторонности* этой функции: по значению комбинации- свертки никто не должен иметь возможность подобрать соответствующее сообщение.

В настоящее время имеются стандарты на криптографические хэш-функции, утверждаемые независимо от стандартов на криптографические алгоритмы и схемы цифровой подписи.

3. **Криптографические средства защиты.**

Криптографическими средствами защиты называются специальные средства и методы преобразования информации, в результате которых маскируется ее содержание. Основными видами криптографического закрытия являются шифрование и кодирование защищаемых данных. При этом шифрование есть такой вид закрытия, при котором самостоятельному преобразованию подвергается каждый символ закрываемых данных; при кодировании защищаемые данные делятся на блоки, имеющие смысловое значение, и каждый такой блок заменяется цифровым, буквенным или комбинированным кодом. При этом используется несколько различных систем шифрования: заменой, перестановкой, гаммированием, аналитическим преобразованием шифруемых данных. Широкое распространение получили комбинированные шифры, когда исходный текст последовательно преобразуется с использованием двух или даже трех различных шифров.

3.1 Криптосистемы

Криптосистема работает по определенной методологии (процедуре). Она состоит из :

- одного или более алгоритмов шифрования (математических формул);
- ключей, используемых этими алгоритмами шифрования;
- системы управления ключами;
- незашифрованного текста;
- и зашифрованного текста (шифртекста).

Ключ Ключ

Текст алгоритм шифртекст алгоритм Текст

шифрования расшифровки

Методология

Согласно методологии сначала к тексту применяются алгоритм шифрования и ключ для получения из него шифртекста. Затем шифртекст передается к месту назначения, где тот же самый алгоритм используется для его расшифровки, чтобы получить снова текст. Также в методологию входят

процедуры создания ключей и их распространения (не показанные на рисунке).

3.2 Принципы работы Криптосистемы.

Типичный пример изображения ситуации, в которой возникает задача криптографии (шифрования) изображён на рис. 1:

A B

П

Рис.2

На рис.2. А и В - законные пользователи защищённой информации, они хотят обмениваться информацией по общедоступному каналу связи. П - незаконный пользователь (*противник* , *хакер*), который хочет перехватывать передаваемые по каналу связи сообщения и попытаться извлечь из них интересную для него информацию. Эту простую схему можно считать моделью типичной ситуации, в которой применяются криптографические методы защиты информации или просто шифрование. Исторически в криптографии закрепились некоторые военные слова (противник, атака на шифр и др.). Они наиболее точно отражают смысл соответствующих криптографических понятий. Вместе с тем широко известная военная терминология, основанная на понятии кода (военно-морские коды, коды Генерального штаба, кодовые книги, кодобозначения и т. п.), уже не применяется в теоретической криптографии. Дело в том, что за последние десятилетия сформировалась *теория кодирования* - большое научное направление, которое разрабатывает и изучает методы защиты информации от случайных искажений в каналах связи.

Криптография занимается методами преобразования информации, которые бы не позволили противнику извлечь ее из перехватываемых сообщений. При этом по каналу связи передается уже не сама защищаемая информация, а результат ее преобразования с помощью шифра, и для противника возникает сложная задача вскрытия шифра. *Вскрытие* (*взламывание*) *шифра* - процесс

получения защищаемой информации из шифрованного сообщения без знания примененного шифра.

Противник может пытаться не получить, а уничтожить или модифицировать защищаемую информацию в процессе ее передачи. Это - совсем другой тип угроз для информация, отличный от перехвата и вскрытия шифра. Для защиты от таких угроз разрабатываются свои специфические методы.

Следовательно, на пути от одного законного пользователя к другому информация должна защищаться различными способами, противостоящими различным угрозам. Возникает ситуация цепи из разнотипных звеньев, которая защищает информацию. Естественно, противник будет стремиться найти самое слабое звено, чтобы с наименьшими затратами добраться до информации. А значит, и законные пользователи должны учитывать это обстоятельство в своей стратегии защиты: бессмысленно делать какое-то звено очень прочным, если есть заведомо более слабые звенья ("принцип равнопрочности защиты").

Придумывание хорошего шифра дело трудоемкое. Поэтому желательно увеличить время жизни хорошего шифра и использовать его для шифрования как можно большего количества сообщений. Но при этом возникает опасность, что противник уже разгадал (вскрыл) шифр и читает защищаемую информацию. Если же в шифре сеть сменный ключ то, заменив ключ, можно сделать так, что разработанные противником методы уже не дают эффекта.

3.2.1 Методология с использованием ключа

В этой методологии алгоритм шифрования объединяет ключ с текстом для создания шифртекста. Безопасность систем шифрования такого типа зависит от конфиденциальности ключа, используемого в алгоритме шифрования, а не от хранения в тайне самого алгоритма. Многие алгоритмы шифрования общедоступны и были хорошо проверены благодаря этому (например, DES). Но основная проблема, связанная с этой методологией, состоит в том, как сгенерировать и безопасно передать ключи участникам взаимодействия. Как

установить безопасный канал передачи информации между участниками взаимодействия до передачи ключей?

Другой проблемой является аутентификация. При этом существуют две серьезных проблемы:

· Сообщение шифруется кем-то, кто владеет ключом в данный момент. Это может быть владелец ключа;

· Но если система скомпрометирована, это может быть другой человек.

· Когда участники взаимодействия получают ключи, откуда они могут узнать, что эти ключи на самом деле были

· созданы и посланы уполномоченным на это лицом?

Существуют две методологии с использованием ключей - симметричная (с секретным ключом) и асимметричная (с открытым ключом). Каждая методология использует свои собственные процедуры, свои способы распределения ключей, типы ключей и алгоритмы шифрования и расшифровки ключей. Так как терминология, используемая этими методологиями, может показаться непонятной, дадим определения основным терминам:

Термин	**Значение**	**Замечания**
Симметричная методология	Используется один ключ, с помощью которого производится как шифрование, так и расшифровка с использованием одного и того алгоритма симметричного шифрования. Этот ключ передается двум участникам взаимодействия безопасным образом до передачи зашифрованных данных.	Часто называется с методологией с секретным ключом.
Асимметричная	Использует алгоритмы	Часто называется

методология	симметричного шифрования и симметричные ключи для шифрования данных. Использует алгоритмы асимметричного шифрования и асимметричные ключи для шифрования симметричного ключа. Создаются два взаимосвязанных асимметричных ключа. Симметричный ключ, зашифрованный с использованием одного асимметричного ключа и алгоритма асимметричного шифрования, должен расшифровываться с использованием другого ключа и другого алгоритма шифрования. Создаются два взаимосвязанных асимметричных ключа. Один должен быть безопасно передан его владельцу, а другой - тому лицу, которое отвечает за хранение этих ключей (CA-сертификационному центру ключей), до начала их использования.	методологией с открытым ключом.
Секретный ключ	Симметричная методология.	Использует один ключ, с

(1)		помощью которого производится как шифрование, так и расшифровка. См. выше.
Секретный ключ (2)	Секретный ключ симметричного шифрования.	Симметричный секретный ключ.
Секретный ключ (3)	Секретный ключ асимметричного шифрования	Асимметричный ключ. Асимметричные ключи создаются парами, так как связаны друг с другом. Выражение «секретный ключ» часто используют для одного из пары асимметричных ключей, который должен держаться в секрете. Асимметричный секретный ключ не имеет ничего общего с симметричным секретным ключом.
Открытый ключ (1)	Асимметричная методология	Использует пару ключей, которые совместно создаются и связаны друг с другом. Все, что зашифровано одним ключом, может быть расшифровано только другим ключом этой пары.
Открытый ключ (2)	Открытый ключ асимметричного шифрования	Асимметричные ключи создаются парами, каждый

		из двух ключей связан с другим. Выражение "открытый ключ" часто используют для одного из пары асимметричных ключей, который должен быть всем известен.
Сеансовый ключ	Симметричный (секретный) ключ шифрования	Используется в асимметричной методологии для шифрования самих данных с помощью симметричных методологий. Это просто симметричный секретный ключ (см. выше).
Алгоритм шифрования	Математическая формула	Для симметричных алгоритмов требуются симметричные ключи. Для асимметричных алгоритмов требуются асимметричные ключи. Вы не можете использовать симметричные ключи для асимметричных алгоритмов и наоборот.
Секретные криптосистемы	Используют симметричные алгоритмы и симметричные (секретные) ключи для шифрования данных.	

Открытые криптосистемы	Использует асимметричные алгоритмы и асимметричные ключи для шифрования сеансовых ключей. Используют симметричные алгоритмы и симметричные (секретные) ключи для шифрования данных.	

Важной проблемой всей криптографии с открытым ключом, в том числе и систем ЭП, является управление открытыми ключами. Так как открытый ключ доступен любому пользователю, то необходим механизм проверки того, что этот ключ принадлежит именно своему владельцу. 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. Существуют системы сертификатов двух типов: централизованные и децентрализованные. В децентрализованных системах путём перекрёстного подписывания сертификатов знакомых и доверенных людей каждым пользователем строится сеть доверия. В централизованных системах сертификатов используются центры сертификации, поддерживаемые доверенными организациями. Центр сертификации формирует закрытый ключ и собственный сертификат, формирует сертификаты конечных пользователей и удостоверяет их аутентичность своей цифровой подписью. Также центр проводит отзыв истекших и компрометированных сертификатов и ведет базы выданных и отозванных сертификатов. Обратившись в сертификационный центр,

можно получить собственный сертификат открытого ключа, сертификат другого пользователя и узнать, какие ключи отозваны.

3.2.1.1 Симметричная (секретная) методология

В этой методологии и для шифрования, и для расшифровки отправителем и получателем применяется один и тот же ключ, об использовании которого они договорились до начала взаимодействия. Если ключ не был скомпрометирован, то при расшифровке автоматически выполняется аутентификация отправителя, так как только отправитель имеет ключ, с помощью которого можно зашифровать информацию, и только получатель имеет ключ, с помощью которого можно расшифровать информацию. Так как отправитель и получатель - единственные люди, которые знают этот симметричный ключ, при компрометации ключа будет скомпрометировано только взаимодействие этих двух пользователей. Проблемой, которая будет актуальна и для других криптосистем, является вопрос о том, как безопасно распространять симметричные (секретные) ключи. Алгоритмы симметричного шифрования используют ключи не очень большой длины и могут быстро шифровать большие объемы данных.

Порядок использования систем с симметричными ключами:

1. Безопасно создается, распространяется и сохраняется симметричный секретный ключ.
2. Отправитель создает электронную подпись с помощью расчета хэш-функции для текста и присоединения полученной строки к тексту.
3. Отправитель использует быстрый симметричный алгоритм шифрования-расшифровки вместе с секретным симметричным ключом к полученному пакету (тексту вместе с присоединенной электронной подписью) для получения зашифрованного текста. Неявно, таким образом, производится аутентификация, так как только отправитель знает симметричный секретный ключ и может зашифровать этот пакет.
4. Только получатель знает симметричный секретный ключ и может расшифровать этот пакет.

5. Отправитель передает зашифрованный текст. Симметричный секретный ключ никогда не передается по незащищенным каналам связи.

6. Получатель использует тот же самый симметричный алгоритм шифрования-расшифровки вместе с тем же самым симметричным ключом (который уже есть у получателя) к зашифрованному тексту для восстановления исходного текста и электронной подписи. Его успешное восстановление аутентифицирует кого-то, кто знает секретный ключ.

7. Получатель отделяет электронную подпись от текста.

8. Получатель создает другую электронную подпись с помощью расчета хэш-функции для полученного текста.

9. Получатель сравнивает две этих электронных подписи для проверки целостности сообщения (отсутствия его искажения).

Доступными сегодня средствами, в которых используется симметричная методология, являются:

· Kerberos, который был разработан для аутентификации доступа к ресурсам в сети, а не для верификации данных. Он использует центральную базу данных, в которой хранятся копии секретных ключей всех пользователей.

· Сети банкоматов (ATM Banking Networks). Эти системы являются оригинальными разработками владеющих ими банков и не продаются. В них также используются симметричные методологии.

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

3.2.1.2 Асимметричная (открытая) методология

В этой методологии ключи для шифрования и расшифровки разные, хотя и создаются вместе. Один ключ делается известным всем, а другой держится в тайне. Хотя можно шифровать и расшифровывать обоими ключами, данные, зашифрованные одним ключом, могут быть расшифрованы только другим ключом. Все асимметричные криптосистемы являются объектом атак путем прямого перебора ключей, и поэтому в них должны использоваться гораздо более длинные ключи, чем те, которые используются в симметричных

криптосистемах, для обеспечения эквивалентного уровня защиты. Это сразу же сказывается на вычислительных ресурсах, требуемых для шифрования, хотя алгоритмы шифрования на эллиптических кривых могут смягчить эту проблему.

Брюс Шнейер в книге "Прикладная криптография: протоколы, алгоритмы и исходный текст на С" приводит следующие данные об эквивалентных длинах ключей.

Длина симметричного ключа	**Длина открытого ключа**
56 бит	384 бит
64 бита	512 бит
80 бит	768 бит
112 бит	1792 бита
128 бит	2304 бита

Для того чтобы избежать низкой скорости алгоритмов асимметричного шифрования, генерируется временный симметричный ключ для каждого сообщения и только он шифруется асимметричными алгоритмами. Само сообщение шифруется с использованием этого временного сеансового ключа и алгоритма шифрования/расшифровки, описанного в пункте 2.2.1.1. Затем этот сеансовый ключ шифруется с помощью открытого асимметричного ключа получателя и асимметричного алгоритма шифрования. После этого этот зашифрованный сеансовый ключ вместе с зашифрованным сообщением передается получателю. Получатель использует тот же самый асимметричный алгоритм шифрования и свой секретный ключ для расшифровки сеансового ключа, а полученный сеансовый ключ используется для расшифровки самого сообщения. В асимметричных криптосистемах важно, чтобы сеансовые и асимметричные ключи были сопоставимы в отношении уровня безопасности, который они обеспечивают. Если используется короткий сеансовый ключ (например, 40-битовый DES), то не имеет значения, насколько велики асимметричные ключи. Хакеры будут атаковать не их, а сеансовые ключи. Асимметричные открытые ключи

уязвимы к атакам прямым перебором отчасти из-за того, что их тяжело заменить. Если атакующий узнает секретный асимметричный ключ, то будет скомпрометирован не только текущее, но и все последующие взаимодействия между отправителем и получателем.

Порядок использования систем с асимметричными ключами:

1. Безопасно создаются и распространяются асимметричные открытые и секретные ключи (см. раздел 2.2 ниже). Секретный асимметричный ключ передается его владельцу. Открытый асимметричный ключ хранится в базе данных X.500 и администрируется центром выдачи сертификатов (по-английски - Certification Authority или CA). Подразумевается, что пользователи должны верить, что в такой системе производится безопасное создание, распределение и администрирование ключами. Более того, если создатель ключей и лицо или система, администрирующие их, не одно и то же, то конечный пользователь должен верить, что создатель ключей на самом деле уничтожил их копию.
2. Создается электронная подпись текста с помощью вычисления его хэш-функции. Полученное значение шифруется с использованием асимметричного секретного ключа отправителя, а затем полученная строка символов добавляется к передаваемому тексту (только отправитель может создать электронную подпись).
3. Создается секретный симметричный ключ, который будет использоваться для шифрования только этого сообщения или сеанса взаимодействия (сеансовый ключ), затем при помощи симметричного алгоритма шифрования/расшифровки и этого ключа шифруется исходный текст вместе с добавленной к нему электронной подписью - получается зашифрованный текст (шифр-текст).
4. Теперь нужно решить проблему с передачей сеансового ключа получателю сообщения.
5. Отправитель должен иметь асимметричный открытый ключ центра выдачи сертификатов (CA). Перехват незашифрованных запросов на получение этого

открытого ключа является распространенной формой атаки. Может существовать целая система сертификатов, подтверждающих подлинность открытого ключа CA. Стандарт X.509 описывает ряд методов для получения пользователями открытых ключей CA, но ни один из них не может полностью защитить от подмены открытого ключа CA, что наглядно доказывает, что нет такой системы, в которой можно было бы гарантировать подлинность открытого ключа CA.

6. Отправитель запрашивает у CA асимметричный открытый ключ получателя сообщения. Этот процесс уязвим к атаке, в ходе которой атакующий вмешивается во взаимодействие между отправителем и получателем и может модифицировать трафик, передаваемый между ними. Поэтому открытый асимметричный ключ получателя "подписывается" CA. Это означает, что CA использовал свой асимметричный секретный ключ для шифрования асимметричного открытого ключа получателя. Только CA знает асимметричный секретный ключ CA, поэтому есть гарантии того, что открытый асимметричный ключ получателя получен именно от CA.

7. После получения асимметричный открытый ключ получателя расшифровывается с помощью асимметричного открытого ключа CA и алгоритма асимметричного шифрования/расшифровки. Естественно, предполагается, что CA не был скомпрометирован. Если же он оказывается скомпрометированным, то это выводит из строя всю сеть его пользователей. Поэтому можно и самому зашифровать открытые ключи других пользователей, но где уверенность в том, что они не скомпрометированы?

8. Теперь шифруется сеансовый ключ с использованием асимметричного алгоритма шифрования-расшифровки и асимметричного ключа получателя (полученного от CA и расшифрованного).

9. Зашифрованный сеансовый ключ присоединяется к зашифрованному тексту (который включает в себя также добавленную ранее электронную подпись).

10. Весь полученный пакет данных (зашифрованный текст, в который входит помимо исходного текста его электронная подпись, и зашифрованный сеансовый ключ) передается получателю. Так как зашифрованный сеансовый ключ передается по незащищенной сети, он является очевидным объектом различных атак.

11. Получатель выделяет зашифрованный сеансовый ключ из полученного пакета.

12. Теперь получателю нужно решить проблему с расшифровкой сеансового ключа.

13. Получатель должен иметь асимметричный открытый ключ центра выдачи сертификатов (CA).

14. Используя свой секретный асимметричный ключ и тот же самый асимметричный алгоритм шифрования получатель расшифровывает сеансовый ключ.

15. Получатель применяет тот же самый симметричный алгоритм шифрования-расшифровки и расшифрованный симметричный (сеансовый) ключ к зашифрованному тексту и получает исходный текст вместе с электронной подписью.

16. Получатель отделяет электронную подпись от исходного текста.

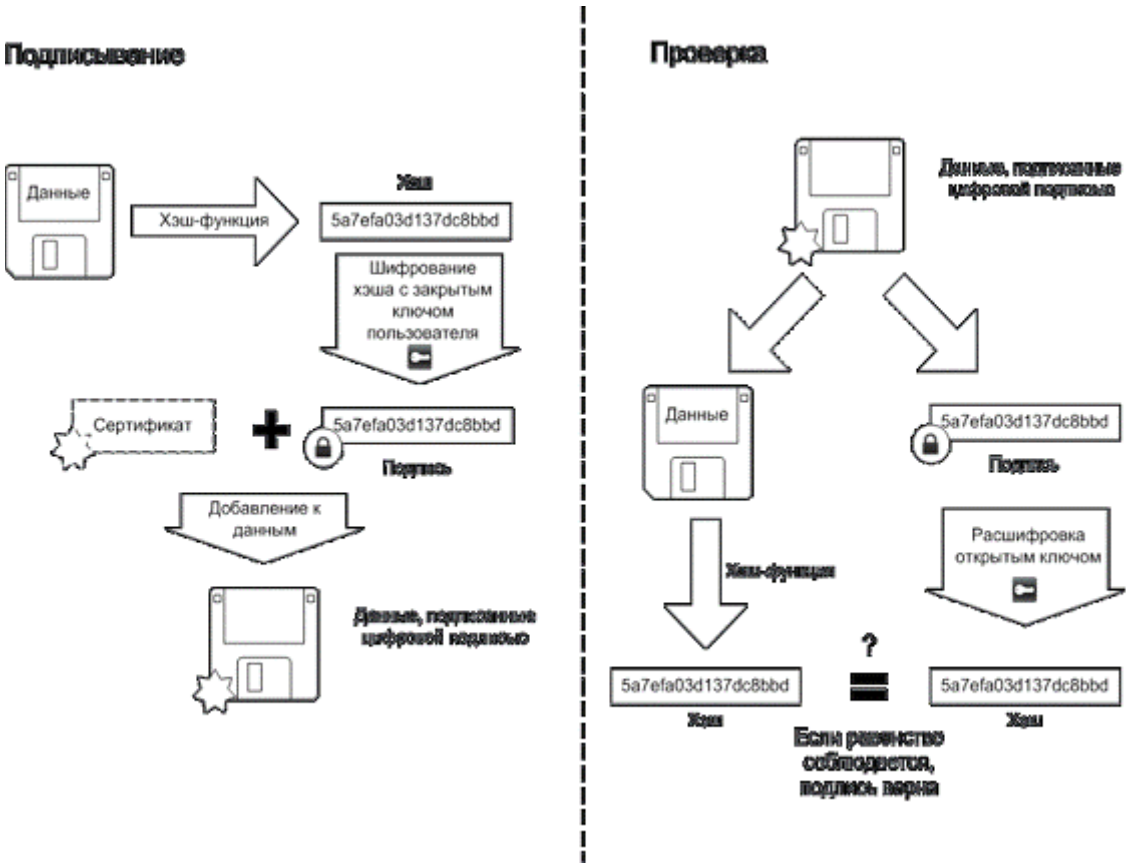
17. Получатель запрашивает у CA асимметричный открытый ключ отправителя.

18. Как только этот ключ получен, получатель расшифровывает его с помощью открытого ключа CA и соответствующего асимметричного алгоритма шифрования-расшифровки.

19. Затем расшифровывается хэш-функция текста с использованием открытого ключа отправителя и асимметричного алгоритма шифрования-расшифровки.

20. Повторно вычисляется хэш-функция полученного исходного текста.

21. Две эти хэш-функции сравниваются для проверки того, что текст не был изменен.



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).
Чтобы применение ЭП имело смысл, необходимо, чтобы вычисление легитимной подписи без знания закрытого ключа было вычислительно сложным процессом. Обеспечение этого во всех асимметричных алгоритмах цифровой подписи опирается на следующие вычислительные задачи: · Задачу дискретного логарифмирования (EGSA) · Задачу факторизации, то есть разложения числа на простые множители (RSA) Вычисления тоже могут производиться двумя способами: на базе математического аппарата эллиптических кривых (ГОСТ Р 34.10-2001) и на базе полей Галуа (DSA) [9]. В настоящее время самые быстрые алгоритмы дискретного логарифмирования и факторизации являются субэкспоненциальными. Принадлежность самих задач к классу NP-полных не доказана. Алгоритмы ЭП подразделяются на обычные цифровые подписи и на цифровые подписи с восстановлением документа. При верификации цифровых подписей с восстановлением документа тело документа восстанавливается автоматически, его не нужно прикреплять к подписи. Обычные цифровые подписи требуют присоединение документа к подписи. Ясно, что все алгоритмы, подписывающие хеш документа, относятся к обычным ЭП. К ЭП с восстановлением документа относится, в частности, RSA. Схемы электронной подписи могут быть одноразовыми и многоразовыми. В одноразовых схемах после проверки подлинности подписи необходимо провести замену ключей, в многоразовых схемах это делать не требуется. Также алгоритмы ЭП делятся на детерминированные и вероятностные. Детерминированные ЭП при одинаковых входных данных вычисляют одинаковую подпись. Реализация вероятностных алгоритмов более сложна, так как требует надежный источник энтропии, но при одинаковых входных данных подписи могут быть различны, что увеличивает криптостойкость. В

настоящее время многие детерминированные схемы модифицированы в вероятностные. В некоторых случаях, таких как потоковая передача данных, алгоритмы ЭП могут оказаться слишком медленными. В таких случаях применяется быстрая цифровая подпись. Ускорение подписи достигается алгоритмами с меньшим количеством модульных вычислений и переходом к принципиально другим методам расчета.

3.3 Распространение ключей

Ясно, что в обеих криптосистемах нужно решать проблему распространения ключей.

В симметричных методологиях эта проблема стоит более остро, и поэтому в них ясно определяется, как передавать ключи между участниками взаимодействия до начала взаимодействия. Конкретный способ выполнения этого зависит от требуемого уровня безопасности. Если не требуется высокий уровень безопасности, то ключи можно рассылать с помощью некоторого механизма доставки (например, с помощью простой почты или курьерской службы). Банки, например, используют почту для рассылки PIN-кодов. Для обеспечения более высокого уровня безопасности более уместна ручная доставка ключей ответственными за это людьми, возможно по частям несколькими людьми.

Асимметричные методологии пытаются обойти эту проблему с помощью шифрования симметричного ключа и присоединения его в таком виде к зашифрованным данным. А для распространения открытых асимметричных ключей, используемых для шифрования симметричного ключа, в них используются центры сертификации ключей. CA, в свою очередь, подписывают эти открытые ключи с помощью секретного асимметричного ключа CA. Пользователи такой системы должны иметь копию открытого ключа CA. Теоретически это означает, что участникам взаимодействия не нужно знать ключей друг друга до организации безопасного взаимодействия.

Сторонники асимметричных систем считают, что такого механизма достаточно для обеспечения аутентичности абонентов взаимодействия. Но проблема все равно остается. Пара асимметричных ключей должна создаваться совместно. Оба ключа, независимо от того, доступны они всем или нет, должны быть безопасно посланы владельцу ключа, а также центру сертификации ключей. Единственный способ сделать это - использовать какой-либо способ доставки при невысоких требованиях к уровню безопасности, и доставлять их вручную - при высоких требованиях к безопасности.

Проблема с распространением ключей в асимметричных системах состоит в следующем:

· X.509 подразумевает, что ключи безопасно раздаются, и не описывает способ решения этой проблемы - а только указывает на существование этой проблемы. Не существует стандартов для решения этого. Для безопасности ключи должны доставляться вручную (независимо от того, симметричные они или асимметричные).

· Нет надежного способа проверить, между какими компьютерами осуществляется взаимодействие. Есть вид атаки, при котором атакующий маскируется под CA и получает данные, передаваемые в ходе взаимодействия. Для этого атакующему достаточно перехватить запрос к центру сертификации ключей и подменить его ключи своими. Эта атака может успешно продолжаться в течение длительного времени.

· Электронная подпись ключей центром сертификации ключей не всегда гарантирует их аутентичность, так как ключ самого CA может оказаться скомпрометированным. X.509 описывает способ электронной подписи ключей CA центрами сертификации ключей более высокого уровня и называет его "путь сертификации". X.509 рассматривает проблемы, связанные с проверкой корректности открытого ключа, предполагая, что эта проблема может быть решена только при отсутствии разрыва в цепочке

доверенных мест в распределенном справочнике открытых ключей пользователей. Нет способа обойти это.

· X.509 предполагает, что пользователь уже имеет доступ к открытому ключу CA. Как это осуществляется, в нем не определяется.

· Компрометация центра сертификации ключей весьма реальная угроза. Компрометация CA означает. Что все пользователи этой системы будут скомпрометированы. И никто не будет знать об этом. X.509 предполагает, что все ключи, включая ключи самого CA, хранятся в безопасном месте. Внедрение системы справочников X.509 (где хранятся ключи) довольно сложно, и уязвимо к ошибкам в конфигурации. В настоящее время слишком мало людей обладают техническими знаниями, необходимыми для правильного администрирования таких систем. Более того, понятно, что на людей, занимающих такие важные должности, может быть оказано давление.

· CA могут оказаться узким местом. Для обеспечения устойчивости к сбоям X.509 предлагает, чтобы база данных CA была реплицирована с помощью стандартных средств X.500; это значительно увеличит стоимость криптосистемы. А при маскараде под CA будет трудно определить, какая система была атакована. Более того, все данные из базы данных CA должны посылаться по каналам связи каким-то образом.

· Система справочников X.500 сложна в установке, конфигурировании и администрировании. Доступ к этому справочнику должен предоставляться либо с помощью дополнительной службы подписки, либо организации придется самой ее организовывать. Сертификат X.509 предполагает, что каждый человек имеет уникальное имя. Выделение имен людям - задача еще одной доверенной службы - службы именования.

· Сеансовые ключи, несмотря на то, что шифруются, все-таки передаются по незащищенным каналам связи.

Несмотря на все эти серьезные недостатки, пользователь должен неявно доверять асимметричной криптосистеме.

Управлением ключами называется их распределение, аутентификация и регламентация порядка использования. Независимо от вида используемой криптосистемы ключами надо управлять. Безопасные методы управления ключами очень важны, так как многие атаки на криптосистемы имеют объектом атаки процедуры управления ключами.

Процедура	**Комментарии**
Физическая раздача ключей	Курьеры и ручная выдача - вот два распространенных примера этой процедуры. Конечно, из них двоих лучше ручная выдача. Серьезные организации имеют инструкции, описывающие порядок выдачи ключей. Раздача ключей может аудироваться и протоколироваться, но это все-таки не защитит ее до конца от компрометации отдельными людьми. Используется как симметричными, так и асимметричными криптосистемами. Несмотря на заявления о том, что в асимметричных криптосистемах не возникает проблем, связанных с физической доставкой ключей, на самом деле они есть. X.509 предполагает, что создатель ключей будет передавать асимметричный секретный ключ пользователю (и/или асимметричный открытый ключ CA) физически безопасным способом, и что предприняты соответствующие меры физической безопасности, чтобы защитить создателя и проводимые им операции с данными от атак.
Выдача общего ключа участникам взаимодействия центром выдачи ключей	Может использоваться как симметричными, так и асимметричными криптосистемами. Так как при данном способе каждый пользователь должен каким-то образом безопасно взаимодействовать с центром выдачи ключей в самом начале работы, то это просто еще один случай, когда начальный обмен ключами является проблемой. Если центр скомпрометирован, то обеспечение

	безопасности последующих запросов на выдачу ключей проблематично, а безопасность ранее выданных ключей зависит от криптосистемы.
Предоставление центром сертификации ключей доступа к открытым ключам пользователей и выдача секретных ключей пользователям	Предоставление центром сертификации ключей доступа к открытым ключам пользователей и выдача секретных ключей пользователям
Сеть доверия	Используется в асимметричных криптосистемах. Пользователи сами распространяют свои ключи и следят за ключами других пользователей; доверие заключатся в неформальном способе обмена ключами.
Метод Диффи-Хеллмана	Обмен секретным ключом по незащищенным каналам связи между двумя пользователями, которые до этого не имели общего секретного ключа. Не может использоваться для шифрования или расшифровки сообщений. Основывается на сложности взятия логарифма в конечных полях. При правильном выборе достаточно больших элементов полей решить проблему расчета дискретного логарифма невозможно. Уязвим к атаке "активное вмешательство в соединение". Запатентован PKP (Public Key Partners)

3.4 Алгоритмы шифрования

Алгоритмы шифрования с использованием ключей предполагают, что данные не сможет прочитать никто, кто не обладает ключом для их

расшифровки. Они могут быть разделены на два класса, в зависимости от того, какая методология криптосистем напрямую поддерживается ими.

Асимметричные схемы: · FDH (Full Domain Hash), вероятностная схема RSA-PSS (Probabilistic Signature Scheme), схемы стандарта PKCS#1 и другие схемы, основанные на алгоритме RSA · Схема Эль-Гамаля · Американские стандарты электронной цифровой подписи: DSA, ECDSA (DSA на основе аппарата эллиптических кривых) · Российские стандарты электронной цифровой подписи: ГОСТ Р 34.10-94 (в настоящее время не действует), ГОСТ Р 34.10-2001 · Схема Диффи-Лампорта · Украинский стандарт электронной цифровой подписи ДСТУ 4145-2002 · Белорусский стандарт электронной цифровой подписи СТБ 1176.2-99 · Схема Шнорра · Pointcheval-Stern signature algorithm · Вероятностная схема подписи Рабина · Схема BLS (Boneh-Lynn-Shacham) · Схема GMR (Goldwasser-Micali-Rivest) На основе асимметричных схем созданы модификации цифровой подписи, отвечающие различным требованиям: · Групповая цифровая подпись · Неоспоримая цифровая подпись · "Слепая" цифровая подпись и справедливая "слепая" подпись · Конфиденциальная цифровая подпись · Цифровая подпись с доказуемостью подделки · Доверенная цифровая подпись · Разовая цифровая подпись.

3.4.1 Симметричные алгоритмы

Для шифрования и расшифровки используются одни и те же алгоритмы. Один и тот же секретный ключ используется для шифрования и расшифровки. Этот тип алгоритмов используется как симметричными, так и асимметричными криптосистемами.

Тип	**Описание**
DES (Data Encryption Standard)	Популярный алгоритм шифрования, используемый как стандарт шифрования данных правительством США. Шифруется блок из 64 бит, используется 64-битовый ключ

	(требуется только 56 бит), 16 проходов. Может работать в 4 режимах: · Электронная кодовая книга (ECB-Electronic Code Book) - обычный DES, использует два различных алгоритма. · Цепочечный режим (CBC-Cipher Block Chaining), в котором шифрование блока данных зависит от результатов шифрования предыдущих блоков данных. · Обратная связь по выходу (OFB-Output Feedback), используется как генератор случайных чисел. Обратная связь по шифратору (CFB-Cipher Feedback), используется для получения кодов аутентификации сообщений.
3-DES или тройной DES	64-битный блочный шифратор, использует DES 3 раза с тремя различными 56-битными ключами. Достаточно стоек ко всем атакам
Каскадный 3-DES	Стандартный тройной DES, к которому добавлен механизм обратной связи, такой как CBC, OFB или CFB. Очень стоек ко всем атакам.
FEAL (быстрый алгоритм шифрования)	Блочный шифратор, используемый как альтернатива DES. Вскрыт, хотя после этого были предложены новые версии.
IDEA (международный алгоритм шифрования)	64-битный блочный шифратор, 128-битовый ключ, 8 проходов. Предложен недавно; хотя до сих пор не прошел полной проверки, чтобы считаться надежным, считается более лучшим, чем DES
Skipjack	Разработано АНБ в ходе проектов правительства США "Clipper" и "Capstone". До недавнего времени был секретным, но его стойкость не зависела только от того, что он был секретным. 64-битный блочный шифратор, 80-битовые ключи используются в режимах ECB, CFB, OFB

	или CBC, 32 прохода
RC2	64-битный блочный шифратор, ключ переменного размера. Приблизительно в 2 раза быстрее, чем DES. Может использоваться в тех же режимах, что и DES, включая тройное шифрование. Конфиденциальный алгоритм, владельцем которого является RSA Data Security
RC4	Потоковый шифр, байт-ориентированный, с ключом переменного размера. Приблизительно в 10 раз быстрее DES. Конфиденциальный алгоритм, которым владеет RSA Data Security
RC5	Имеет размер блока 32, 64 или 128 бит, ключ с длиной от 0 до 2048 бит, от 0 до 255 проходов. Быстрый блочный шифр. Алгоритм, которым владеет RSA Data Security
CAST	64-битный блочный шифратор, ключи длиной от 40 до 64 бит, 8 проходов. Неизвестно способов вскрыть его иначе как путем прямого перебора.
Blowfish.	64-битный блочный шифратор, ключ переменного размера до 448 бит, 16 проходов, на каждом проходе выполняются перестановки, зависящие от ключа, и подстановки, зависящие от ключа и данных. Быстрее, чем DES. Разработан для 32-битных машин
Устройство с одноразовыми ключами	Шифратор, который нельзя вскрыть. Ключом (который имеет ту же длину, что и шифруемые данные) являются следующие 'n' бит из массива случайно созданных бит, хранящихся в этом устройстве. У отправителя и получателя имеются одинаковые устройства. После использования биты разрушаются, и в следующий раз используются другие биты.
Поточные шифры	Быстрые алгоритмы симметричного шифрования, обычно

	оперирующие битами (а не блоками бит). Разработаны как аналог устройства с одноразовыми ключами, и хотя не являются такими же безопасными, как оно, по крайней мере практичны.

3.4.2 Асимметричные алгоритмы

Асимметричные алгоритмы используются в асимметричных криптосистемах для шифрования симметричных сеансовых ключей (которые используются для шифрования самих данных).

Используется два разных ключа - один известен всем, а другой держится в тайне. Обычно для шифрования и расшифровки используется оба этих ключа. Но данные, зашифрованные одним ключом, можно расшифровать только с помощью другого ключа.

Тип	**Описание**
RSA	Популярный алгоритм асимметричного шифрования, стойкость которого зависит от сложности факторизации больших целых чисел.
ECC (криптосистема на основе эллиптических кривых)	Использует алгебраическую систему, которая описывается в терминах точек эллиптических кривых, для реализации асимметричного алгоритма шифрования. Является конкурентом по отношению к другим асимметричным алгоритмам шифрования, так как при эквивалентной стойкости использует ключи меньшей длины и имеет большую производительность. Современные его реализации показывают, что эта система гораздо более эффективна, чем другие системы с открытыми ключами. Его производительность приблизительно на порядок выше, чем производительность RSA, Диффи-Хеллмана и DSA.
Эль-Гамаль.	Вариант Диффи-Хеллмана, который может быть использован как для шифрования, так и для электронной

	подписи.

3.5 Хэш-функции

Хэш-функции являются одним из важных элементов криптосистем на основе ключей. Их относительно легко вычислить, но почти невозможно расшифровать. Хэш-функция имеет исходные данные переменной длины и возвращает строку фиксированного размера (иногда называемую дайджестом сообщения - MD), обычно 128 бит. Хэш-функции используются для обнаружения модификации сообщения (то есть для электронной подписи).

Тип	**Описание**
MD2	Самая медленная, оптимизирована для 8-битовых машин
MD4	Самая быстрая, оптимизирована для 32-битных машин. Не так давно взломана
MD5	Наиболее распространенная из семейства MD-функций. Похожа на MD4, но средства повышения безопасности делают ее на 33% медленнее, чем MD4. Обеспечивает целостность данных. Считается безопасной
SHA (Secure Hash Algorithm)	Создает 160-битное значение хэш-функции из исходных данных переменного размера. Предложена NIST и принята правительством США как стандарт. Предназначена для использования в стандарте DSS

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.

3.6 Механизмы аутентификации

Эти механизмы позволяют проверить подлинность личности участника взаимодействия безопасным и надежным способом.

Тип	Описание

Пароли или PIN-коды (персональные идентификационные номера)	Что-то, что знает пользователь и что также знает другой участник взаимодействия. Обычно аутентификация производится в 2 этапа. Может организовываться обмен паролями для взаимной аутентификации.
Одноразовый пароль	Пароль, который никогда больше не используется. Часто используется постоянно меняющееся значение, которое базируется на постоянном пароле.
CHAP (протокол аутентификации запрос-ответ)	Одна из сторон инициирует аутентификацию с помощью посылки уникального и непредсказуемого значения "запрос" другой стороне, а другая сторона посылает вычисленный с помощью "запроса" и секрета ответ. Так как обе стороны владеют секретом, то первая сторона может проверить правильность ответа второй стороны.
Встречная проверка (Callback)	Телефонный звонок серверу и указание имени пользователя приводит к тому, что сервер затем сам звонит по номеру, который указан для этого имени пользователя в его конфигурационных данных.

3.7 Электронные подписи и временные метки

Электронная подпись позволяет проверять целостность данных, но не обеспечивает их конфиденциальность. Электронная подпись добавляется к сообщению и может шифроваться вместе с ним при необходимости сохранения данных в тайне. Добавление временных меток к электронной подписи позволяет обеспечить ограниченную форму контроля участников взаимодействия.

Тип	**Комментарии**
DSA (Digital Signature	Алгоритм с использованием открытого ключа для создания электронной подписи, но не для шифрования.

Authorization)	Секретное создание хэш-значения и публичная проверка ее - только один человек может создать хэш-значение сообщения, но любой может проверить ее корректность. Основан на вычислительной сложности взятия логарифмов в конечных полях.
RSA	Запатентованная RSA электронная подпись, которая позволяет проверить целостность сообщения и личность лица, создавшего электронную подпись. Отправитель создает хэш-функцию сообщения, а затем шифрует ее с использованием своего секретного ключа. Получатель использует открытый ключ отправителя для расшифровки хэша, сам рассчитывает хэш для сообщения, и сравнивает эти два хэша.
MAC (код аутентификации сообщения)	Электронная подпись, использующая схемы хэширования, аналогичные MD или SHA, но хэш-значение вычисляется с использованием, как данных сообщения, так и секретного ключа.
DTS (служба электронных временных меток)	Выдает пользователям временные метки, связанные с данными документа, криптографических стойким образом.

В 1994 году Главным управлением безопасности связи Федерального агентства правительственной связи и информации при Президенте Российской Федерации был разработан первый российский стандарт ЭЦП - ГОСТ Р 34.10-94. В 2002 году для обеспечения большей криптостойкости алгоритма взамен ГОСТ Р 34.10-94 был введен стандарт ГОСТ Р 34.10-2001, основанный на вычислениях в группе точек эллиптической кривой. В соответствии с этим стандартом, термины "электронная цифровая подпись" и "цифровая подпись" являются синонимами. Простая электронная подпись (ПЭП); Усиленная

электронная подпись (УЭП); Усиленная неквалифицированная электронная подпись (НЭП); Усиленная квалифицированная электронная подпись (КЭП).

3.8. Стойкость шифра.

Способность шифра противостоять всевозможным атакам на него называют *стойкостью шифра. Под атакой* на шифр понимают попытку вскрытия этого шифра. Понятие стойкости шифра является центральным для криптографии. Хотя качественно понять его довольно легко, но получение строгих доказуемых оценок стойкости для каждого конкретного шифра - проблема нерешенная. Это объясняется тем, что до сих пор нет необходимых для решения такой проблемы математических результатов. Поэтому стойкость конкретного шифра оценивается только путем всевозможных попыток его вскрытия и зависит от квалификации криптоаналитиков, атакующих шифр. Такую процедуру иногда называют проверкой стойкости. Важным подготовительным этапом для проверки стойкости шифра является продумывание различных предполагаемых возможностей, с помощью которых противник может атаковать шифр. Появление таких возможностей у противника обычно не зависит от криптографии, это является некоторой внешней подсказкой и существенно влияет на стойкость шифра. Поэтому оценки стойкости шифра всегда содержат те предположения о целях и возможностях противника, в условиях которых эти оценки получены. Прежде всего, как это уже отмечалось выше, обычно считается, что противник знает сам шифр и имеет возможности для его предварительного изучения. Противник также знает некоторые характеристики открытых текстов, например, общую тематику сообщений, их стиль, некоторые стандарты, форматы и т.д.

Из более специфических приведем еще три примера возможностей противника:

1. противник может перехватывать все шифрованные сообщения, но не имеет соответствующих им открытых текстов;

2. противник может перехватывать все шифрованный сообщения и добывать соответствующие им открытые тексты;

3. противник имеет доступ к шифру (но не к ключам!) и поэтому может зашифровывать и дешифровывать любую информацию.

Заключение

Криптография сегодня - это важнейшая часть всех информационных систем: от электронной почты до сотовой связи, от доступа к сети Internet до электронной наличности. Криптография обеспечивает подотчетность, прозрачность, точность и конфиденциальность. Она предотвращает попытки мошенничества в электронной коммерции и обеспечивает юридическую силу финансовых транзакций. Криптография помогает установить вашу личность, но и обеспечивает вам анонимность. Она мешает хулиганам испортить сервер и не позволяет конкурентам залезть в ваши конфиденциальные документы. А в будущем, по мере того как коммерция и коммуникации будут все теснее связываться с компьютерными сетями, криптография станет жизненно важной. Но присутствующие на рынке криптографические средства не обеспечивают того уровня защиты, который обещан в рекламе. Большинство продуктов разрабатывается и применяется отнюдь не в сотрудничестве с криптографами. Этим занимаются инженеры, для которых криптография - просто еще один компонент программы. Но криптография - это не компонент. Нельзя обеспечить безопасность системы, «вставляя» криптографию после ее разработки. На каждом этапе, от замысла до инсталляции, необходимо осознавать, что и зачем вы делаете.

Для того чтобы грамотно реализовать собственную криптосистему, необходимо не только ознакомится с ошибками других, и понять причины, по которым они произошли, но и, возможно, применять особые защитные приемы программирования и специализированные средства разработки. На обеспечение компьютерной безопасности тратятся миллиарды долларов, причем большая часть денег выбрасывается на негодные продукты. К сожалению, коробка со слабым криптографическим продуктом выглядит так же, как коробка со стойким. Два криптопакета для электронной почты могут иметь схожий пользовательский интерфейс, но один обеспечит безопасность, а второй допустит подслушивание. Сравнение может указывать сходные

черты двух программ, но в безопасности одной из них при этом зияют дыры, которых лишена другая система. Опытный криптограф сможет определить разницу между этими системами. То же самое может сделать и злоумышленник. На сегодняшний день компьютерная безопасность - это карточный домик, который в любую минуту может рассыпаться. Очень многие слабые продукты до сих пор не были взломаны только потому, что они мало используются. Как только они приобретут широкое распространение, они станут притягивать к себе преступников. Пресса тут же придаст огласке эти атаки, подорвав доверие публики к этим криптосистемам. В конце концов, победу на рынке криптопродуктов определит степень безопасности этих продуктов.

Список литературы

1. Поисковая система. Википедия (ЭЦП) . Федеральный закон от 6 апреля 2011 г. № 63-ФЗ "Об электронной подписи" . Петров А. А Компьютерная безопасность. Криптографические методы защиты. . Теоретические основы - Безопасность информационных систем - Криптографические системы . В.Е. Фигурнов Интернет для пользователя. Краткий курс. - М.: ИНФРА-М, 1999 г.