Тесты кафедры анатомии человека МГМСУ им. А.И. Евдокимова

ГОУ ВПО «Донецкий Национальный университет»
Физико-технический факультет
Кафедра радиофизики и инфокоммуникационных технологий
Реферат
на тему «Криптографические методы»
по дисциплине: «Основы информационной безопасности»
Выполнил: студент 1 курса
Моисеев О.И.
Преподаватель: Белик Т.В.
Донецк 2017
План

Введение

Проблема защиты информации путем ее преобразования, исключающего ее прочтение посторонним лицом, волновала человеческий ум с давних времен. 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.
Среди всего спектра методов защиты данных от нежелательного доступа особое место занимают криптографические методы. История криптографии - ровесница истории человеческого языка. Более того, первоначально письменность сама по себе была криптографической системой, так как в древних обществах ею владели только избранные. Священные книги Древнего Египта, Древней Индии тому примеры.
С широким распространением письменности криптография стала формироваться как самостоятельная наука.
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.
1. Понятие криптографии, её цели и требования к ней

Криптография (в пер. с гр. - «тайнопись») - это набор методов защиты информационных взаимодействий от отклонений от их нормального, штатного протекания, вызванных злоумышленными действиями различных субъектов, методов, базирующихся на секретных алгоритмах преобразования информации, включая алгоритмы, не являющиеся собственно секретными, но использующие секретные параметры. Исторически первой задачей криптографии была защита передаваемых текстовых сообщений от несанкционированного ознакомления с их содержанием, что нашло отражение в самом названии этой дисциплины, эта защита базируется на использовании "секретного языка", известного только отправителю и получателю, все методы шифрования являются лишь развитием этой философской идеи. С усложнением информационных взаимодействий в человеческом обществе возникли и продолжают возникать новые задачи по их защите, некоторые из них были решены в рамках криптографии, что потребовало развития принципиально новых подходов и методов.
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. алгоритм аутентификация ключ криптография

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:

1. обеспечение конфиденциальности - решение проблемы защиты информации от ознакомления с ее содержанием со стороны лиц, не имеющих права доступа к ней;
2. 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;
3. 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.;
4. обеспечение невозможности отказа от авторства или приписывания авторства - предотвращение возможности отказа субъектов от некоторых из совершенных ими действий.

2. Криптографические средства и методы защиты информации

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, т.е. преобразования, которые делают защищенные входные данные трудно раскрываемыми по входным данным без знания специальной ключевой информации - ключа.
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.
Основные направления использования криптографических методов - передача конфиденциальной информации по каналам связи (например, электронная почта), установление подлинности передаваемых сообщений, хранение информации (документов, баз данных) на носителях в зашифрованном виде.
Криптографические методы можно разбить на два класса:
1)обработка информации путем замены и перемещения букв, при котором объем данных не меняется (шифрование);
2)сжатие информации с помощью замены отдельных сочетаний букв, слов или фраз (кодирование).
По способу реализации криптографические методы возможны в аппаратном и программном исполнении.
Для защиты текстовой информации при передачах на удаленные станции телекоммуникационной сети используются аппаратные способы шифрования и кодирования.
Для обмена информацией между ЭВМ по телекоммуникационной сети, а также для работы с локальными абонентами возможны как аппаратные, так и программные способы.
Для хранения информации на магнитных носителях применяются программные способы шифрования и кодирования.
Аппаратные способы шифрования информации применяются для передачи защищенных данных по телекоммуникационной сети.
Для реализации шифрования с помощью смешанного алфавита используется

перестановка отдельных разрядов в пределах одного или нескольких символов. Программные способы применяются для шифрования информации, хранящейся на магнитных носителях (дисках, лентах). Это могут быть данные различных информационно-справочных систем АСУ, АСОД и др. программные способы шифрования сводятся к операциям перестановки, перекодирования и сложения по модулю 2 с ключевыми словами. Особое место в программах обработки информации занимают операции кодирования.

Преобразование информации, в результате которого обеспечивается изменение объема памяти, занимаемой данными, называется кодированием.

На практике кодирование всегда используется для уменьшения объема памяти, так как экономия памяти ЭВМ имеет большое значение в информационных системах. Кроме того, кодирование можно рассматривать как криптографический метод обработки информации.

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.

3. Понятие и принцип работы криптосистемы

Криптосистема - семейство выбираемых с помощью ключа обратимых преобразований, которые преобразуют защищаемый открытый текст в шифрограмму и обратно. Любая современная криптографическая система основана (построена) на использовании криптографических ключей. Она работает по определенной методологии (процедуре), состоящей из: одного или более алгоритмов шифрования (математических формул); ключей, используемых этими алгоритмами шифрования; системы управления ключами; незашифрованного текста; зашифрованного текста (шифртекста).

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.

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.
Под ключом в криптографии понимают сменный элемент шифра, который применяется для шифрования конкретного сообщения. В последнее время безопасность защищаемой информации стала определяться в первую очередь ключом. Сам шифр, шифрмашина или принцип шифрования стали считать известными противнику и доступными для предварительного изучения, но в них появился неизвестный для противника ключ, от которого существенно зависят применяемые преобразования информации. Теперь законные пользователи, прежде чем обмениваться шифрованными сообщениями, должны тайно от противника обменяться ключами или установить одинаковый ключ на обоих концах канала связи. А для противника появилась новая задача - определить ключ, после чего можно легко прочитать зашифрованные на этом ключе сообщения.
Отметим теперь, что не существует единого шифра, подходящего для всех случаев. Выбор способа шифрования зависит от особенностей информации, ее ценности и возможностей владельцев по защите своей информации.
4. Методология использования криптосистем и распространение ключей к ним

4.1 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.

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 методология

Использует алгоритмы 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.

Часто называется методологией с открытым ключом.

Секретный ключ (1)

Симметричная методология.

Использует один ключ, с помощью которого производится как шифрование, так и расшифровка.

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.

4.1.1 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.

4.1.2 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. 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. 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.
4.2 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 СА 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 СА может оказаться скомпрометированным. X.509 описывает способ электронной подписи ключей СА 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 СА. Как это осуществляется, в нем не определяется;
· компрометация центра сертификации ключей весьма реальная угроза. Компрометация СА означает. Что все пользователи этой системы будут скомпрометированы. И никто не будет знать об этом. X.509 предполагает, что все ключи, включая ключи самого СА, 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;
· СА могут оказаться узким местом. Для обеспечения устойчивости к сбоям X.509 предлагает, чтобы база данных СА была реплицирована с помощью стандартных средств X.500; это значительно увеличит стоимость криптосистемы. А при маскараде под СА будет трудно определить, какая система была атакована. Более того, все данные из базы данных СА 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)

4.3 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.

4.3.1 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.

4.3.2 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.

4.4 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

4.5 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.

4.6 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 Authorization)

Алгоритм с использованием открытого ключа для создания электронной подписи, но не для шифрования. 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.

4.7 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:
- противник может перехватывать все шифрованные сообщения, но не имеет соответствующих им открытых текстов;
- противник может перехватывать все шифрованный сообщения и добывать соответствующие им открытые тексты;
- противник имеет доступ к шифру (но не к ключам!) и поэтому может зашифровывать и дешифровывать любую информацию.
5. Современные криптографические устройства и системы

Ряд фирм выпускает криптографические устройства ориентированные на работу в сетях, например, шифратор ScaNet фирмы Dowty Network Systems (Великобритания), шифратор Datacryptor-64 фирмы Racal Datacom (США) для пользователей сети с пакетной коммутацией по протоколу X.25 МККТТ.
Фирма NFT (Норвегия) разработала серию криптомодулей со скоростями до 10 Мбит/с, предназначенных для засекречивания потоков и применения в локальных сетях. Фирма Xerox (США) создала блок высококачественного шифрования данных Xerox Encription Unit, обеспечивающий защиту особо секретной информации, в локальной сети.
Фирма PE Systems (США) поставляет систему GILLAROO для передачи цифровой подписи и защиты секретной информации, передаваемой в сетях и каналах связи.
Фирма Calmes Semiconductor Inc. (США) производит криптопроцессор СЛ34С168 для блочного шифрования на скорости до 300 Кбит/с. За последнее время предложены новые алгоритмы шифрования, например NEWDES и FEAL, рассчитанные на шифрование потоков со скоростями до 1 Гбит/с.
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 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. В конце концов, победу на рынке криптопродуктов определит степень безопасности этих продуктов....