РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук

Кафедра прикладной информатики и теории вероятностей

РЕФЕРАТ

СОВРЕМЕННЫЕ МЕТОДЫ КРИПТОГРАФИИ.

дисциплина: Операционные системы

Студент: Петрова Мария Евгеньевна

Группа: НФИбд-02-21

МОСКВА

2022 г.

Содержание:

1.Введениие	3
2.Криптография	4
3.Криптографические методы защиты информации	5
4.Управление криптографическими ключами	7
5.Симметричная (секретная) методология	9
6.Асимметричная (открытая) методология	11
7.Электронные подписи	15
8.Заключение	18
Литература	20

Введение

Проблема защиты информации путем ее преобразования, исключающего ее прочтение посторонним лицом, волновала человеческий ум с давних времен. 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.

Проблемой защиты информации путем ее преобразования занимается криптология (kryptos - тайный, logos - наука). Криптология разделяется на два направления - криптографию и криптоанализ. Цели этих направлений прямо противоположны.

Криптография занимается поиском и исследованием математических методов преобразования информации.

Сфера интересов криптоанализа - исследование возможности расшифровывания информации без знания ключей.

Терминология

Криптография дает возможность преобразовать информацию таким образом, что ее прочтение (восстановление) возможно только при знании ключа.

В качестве информации, подлежащей шифрованию и дешифрованию, будут рассматриваться тексты, построенные на некотором алфавите. Под этими терминами понимается следующее.

Алфавит - конечное множество используемых для кодирования информации знаков.

Текст - упорядоченный набор из элементов алфавита.

Шифрование - преобразовательный процесс: исходный текст, который носит также название открытого текста, заменяется шифрованным текстом.

Дешифрование - обратный шифрованию процесс. На основе ключа шифрованный текст преобразуется в исходный.

Ключ - информация, необходимая для беспрепятственного шифрования и дешифрования текстов.

Криптографическая система представляет собой семейство T преобразований открытого текста. Члены этого семейства индексируются, или обозначаются символом k; параметр k является ключом.
Пространство ключей K - это набор возможных значений ключа. Обычно ключ представляет собой последовательный ряд букв алфавита.

Криптография

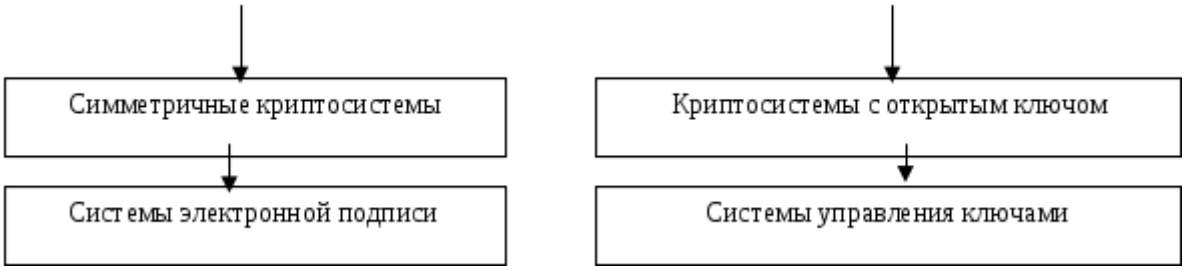
Криптография - это набор методов защиты информационных взаимодействий от отклонений от их нормального, штатного протекания, вызванных злоумышленными действиями различных субъектов, методов, базирующихся на секретных алгоритмах преобразования информации, включая алгоритмы, не являющиеся собственно секретными, 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.

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: замена, перестановка, гаммирование, аналитическое преобразование шифруемых данных. Широкое распространение получили комбинированные шифры, когда исходный текст последовательно преобразуется с использованием двух или даже трех различных шифров.

Криптографические методы защиты информации

Современная криптография включает в себя четыре крупных раздела**:**



Криптографическими средствами защиты называются специальные средства и методы преобразования информации, в результате которых маскируется ее содержание.

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.

Управление криптографическими ключами

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.
Вернемся к формальному описанию основного объекта криптографии

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. Прежде всего подчеркнем большое разнообразие видов защищаемой информации: документальная, телефонная, телевизионная, компьютерная и т.д. Каждый вид информации имеет свои специфические особенности, и эти особенности сильно влияют на выбор методов шифрования информации. Большое значение имеют объемы и требуемая скорость передачи шифрованной информации. Выбор вида шифра и его параметров существенно зависит от характера защищаемых секретов или тайны.

Некоторые тайны (например, государственные, военные и др.) должны сохраняться десятилетиями, а некоторые (например, биржевые) - уже через несколько часов можно разгласить. Необходимо учитывать также и возможности того противника, от которого защищается данная информация. Одно дело - противостоять одиночке или даже банде уголовников, а другое дело - мощной государственной структуре.
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; и зашифрованного текста (шифртекста).

Симметричная 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 аудентификация, так как только отправитель знает симметричный секретный ключ и может зашифровать этот пакет. Только получатель знает симметричный секретный ключ и может расшифровать этот пакет.

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

5. 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.

6. Получатель отделяет электронную подпись от текста.

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

8. 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.

Ассимметричная методология

В этой методологии ключи для шифрования и расшифровки разные, хотя и создаются вместе. Один ключ делается известным всем, а другой держится в тайне. 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.

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, ранее описанного. 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. 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 и администрируется центром выдачи сертификатов. 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. Перехват незашифрованных запросов на получение этого открытого ключа является распространенной формой атаки. Может существовать целая система сертификатов, подтверждающих подлинность открытого ключа.

6. Отправитель запрашивает у центра сертификатов 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" у центра сертификатов. Это означает, что центр сертификатов использовал свой асимметричный секретный ключ для шифрования асимметричного открытого ключа получателя. Только центр сертификатов знает асимметричный секретный ключ, поэтому есть гарантии того, что открытый асимметричный ключ получателя получен именно от него.

7. После получения асимметричный открытый ключ получателя расшифровывается с помощью асимметричного открытого ключа и

алгоритма асимметричного шифрования/расшифровки. Естественно, предполагается, что центр сертификатов 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 центр сертификатов 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.

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 центр сертификатов асимметричный открытый ключ отправителя.

18. Как только этот ключ получен, получатель расшифровывает его с помощью открытого ключа центр сертификатов 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.

Электронные подписи

Электронная (цифровая) подпись есть нечто, связанное с электронным документом, что выполняет функции, подобные функциям собственноручной подписи. Она может использоваться для того, чтобы подтвердить получателю сообщения, что это сообщение пришло именно от того, кто

назван отправителем данного сообщения ("аутентичность"). Другое важное применение электронной подписи заключается в установлении того, что сообщение не подверглось фальсификации ("целостность").

Цифровая подпись зависит от содержания подписываемого документа и некоего секретного элемента (ключа), которым обладает только лицо, участвующее в защищенном обмене. Такой механизм должен обеспечивать следующее:

1. цифровая подпись должна подтверждать, что подписывающее лицо не случайно подписало электронный документ.
2. цифровая подпись должна подтверждать, что только подписывающее лицо, и только оно, подписало электронный документ.
3. цифровая подпись должна зависеть от содержания подписываемого документа и времени его подписания.
4. подписывающее лицо не должно иметь возможности в последствии отказаться от факта подписи документа.

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.

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. Методические указания по выполнению и темы курсовых работ по дисциплине “Информатика”// ВЗФЭИ, - 2006г
2. Основы криптографии: Учебное пособие.// Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. // 3-е изд., испр. и доп. - М.: -2005г - 480с.
3. Введение в криптографию //Под общ. ред. В. В. Ященко --- М., МЦНМО, 1998, 1999, 2000 - 272 с.
4. Основы защиты информации: Учебник для вузов. // М. Герасименко В.А., Малюк А.А./Изд-во ООО «Инкомбанк», -1997г