УВАЖАЕМЫЕ СТУДЕНТЫ! Изучите приведенную лекцию, законспектируйте основные понятия, дайте ответы на контрольные вопросы.

Ответы на вопросы, фотоотчет, предоставить преподавателю на e-mail: r.bigangel@gmail.com до 13.03.2023.

При возникновении вопросов по приведенному материалу обращаться по следующему номеру телефона: (072)111-37-59, (Viber, WhatsApp), vk.com: https://vk.com/daykini

ВНИМАНИЕ!!! При отправке работы, не забывайте указывать ФИО студента, наименование дисциплины, дата проведения занятия (по расписанию).

Лекция 42 (продолжение)

Тема: Криптографические методы защиты информации

Цель: Изучить основные криптографические методы защиты информации

Рассматриваемые вопросы:

1. История развития криптографии.
2. Основные понятия и элементы криптографии (алгоритм, ключ, шифр).
   2.1. Симметричные криптосистемы
   2.2. Асимметричные криптосистемы
3. Требования к криптосистемам.

1. История развития криптографии

В данной лекции описаны основные «строительные кирпичики» шифрования, которое применяется в любой корпоративной сети и входит в более сложные технологии безопасности.

Почему проблема использования криптографических методов в информационных системах (ИС) стала в настоящий момент особо актуальна?

С одной стороны, расширилось использование компьютерных сетей, в частности глобальной сети Интернет, по которым передаются большие объемы информации государственного, военного, коммерческого и частного характера, не допускающего возможность доступа к ней посторонних лиц.

С другой стороны, появление новых мощных компьютеров, технологий сетевых и нейронных вычислений сделало возможным дискредитацию

криптографических систем еще недавно считавшихся практически не раскрываемыми.

Проблема защиты информации путем ее преобразования, исключающего ее прочтение посторонним лицом, волновала человеческий ум с давних времен. 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. Первые криптосистемы встречаются уже в начале нашей эры. Так, Цезарь в своей переписке использовал уже более менее систематический шифр, получивший его имя.

Бурное развитие криптографические системы получили в годы первой и второй мировых войн. Начиная с послевоенного времени и по нынешний день появление вычислительных средств ускорило разработку и совершенствование криптографических методов.

Тайна сопровождает всю историю человечества. Она была, есть и будет.

Начиная с ***личной*** тайны, она переходит в тайны ***семьи***, ***клана, рода*** и так далее. С образованием государств высшей формой тайны становится тайна ***государственная***.

Появляются различные виды **тайны**: политическая, военная, дипломатическая, экономическая, ремесленническая, коммерческая, медицинская, криминальная, религиозно-мистическая и так далее.

Если есть тайна, то необходимы и способы ее защиты.

И они, естественно, сразу же появились и стали активно развиваться. Одновременно развивались и способы проникновения в «чужую» тайну, методы преодоления защитных мер. Следует особо подчеркнуть, что с возникновением специальных разведывательных служб государств деятельность в области обеспечения информационной безопасности государственных структур стала активно опираться на разведывательные органы, порой в немалой степени диктуя им «линию поведения». Подкуп, шантаж, кража, внедрение агента и так далее прочно вошли в арсенал средств «информационной войны» государств.

Исторический процесс развития средств и методов защиты тайных посланий выработал ***три основных способа такой защиты.***

Первый способ защиты информации — это ***физическая защита*** от противника материального носителя информации (пергамент, бумага, магнитная лента, физические каналы передачи: проводная линия связи, радиоканал, вибро-акустический канал и так далее).

Одновременно появляются приемы и способы, затрудняющие перехват сообщений. Главную роль здесь играет выбор канала связи, труднодоступного для перехвата (ласточки, голуби, специальный курьер, кабельные линии связи, специальные виды радиопередач, волоконно-оптические линии связи и так далее).

Наряду с физической защитой носителя информации предусматриваются и другие меры. В их числе можно отметить следующие.

При реальной угрозе захвата противником материального носителя информации и наличии сомнений по поводу достойного отражения этой угрозы предпринимаются меры по ***быстрому и эффективному уничтожению носителя информации (или самой информации, записанной на нем).***

Спектр действий здесь достаточно широк: выбросить носитель в недоступное для «захватчиков» место, разорвать, стереть, проглотить и так далее. Естественно, сам физический носитель информации и способ ее записи в этом случае должны соответствовать требованиям эффективного уничтожения. В настоящее время, как впрочем и в древние времена, этой проблеме уделялось и уделяется достойное внимание.

Важной задачей при физической защите информации является своевременное ***обнаружение факта «утечки» секретной информации.*** Это обнаружение позволяет принять меры к локализации негативных последствий от действий противника, обладающего этой информацией. Поэтому необходимо предусматривать меры по обнаружению перехвата.

Нападающая сторона, со своей стороны, должна принимать меры к безуликовости перехвата и, к сокрытию факта наличия у нее полученной информации. Особенно строго следует сохранять тайну источника информации.

Второй способ защиты информации — Используется для определения метода защиты, основанного на попытке сокрытия от противника самого факта наличия интересующей его информации. Такую защиту можно было бы осуществить несколькими принципиально различными способами.

Во-первых, можно было бы попытаться сделать «невидимым» для противника сам физический носитель информации. В современных условиях к таким способам относится, например, использование так называемой «микроточки— микрофотографии» (размером в «точку» письменного текста), подклеиваемой под клапан конверта, почтовую марку и так далее. На этой микроточке фотографическим способом передается защищаемый текст. Сюда же относятся исторически древние приемы: ***«запрятывание»*** носителя информации в корешках книг, в каблуках, в пломбе зуба, в медицинских препаратах и так далее. Здесь фантазия не ограничена. **(На голове раба, которая брилась наголо, записывалось нужное сообщение. И когда волосы его достаточно отрастали, раба отправляли к адресату, который снова брил его голову и считывал полученное сообщение)**

Во-вторых, можно было бы попытаться поступить таким образом, чтобы противник, даже имея в руках носитель секретной информации, ***саму эту информацию не увидел. В*** этом направлении наибольшее распространение получили так называемые ***симпатические (химические) чернила***. Текст, написанный этими чернилами между строк «невинного» послания, невидим; он проявляется только в результате применения определенной технологии проявления.

В-третьих, на носителе информации, попадающим в руки противника, ***нет ничего, кроме того текста, рисунка, графика и так далее, который он видит.*** Однако истинное секретное сообщение скрывается в буквах, точках рисунка, графика и так далее, стоящих на заранее оговоренных местах «невинного» сообщения.

В целом нужно отметить, что сегодня имеется огромный спектр ***стеганографических*** методов защиты информации.

Третий способ защиты информации — наиболее надежный и распространенный в наши дни — ***криптография***, (в переводе с греческого это слово также означает «тайнопись»). В этом случае в перехваченном сообщении противник ***видит хаотический набор знаков, так что смысл сообщения ему остается неясным.***

Следует отметить, что наиболее эффективная защищенность информации достигается при комплексном использовании всех указанных выше способов.

История знает многочисленные примеры такой комплексной защиты. Следует также заметить, что в историческом плане даже незашифрованный текст (тем более на иностранном языке) сам по себе уже определяет первую ступень защиты. В то время, когда подавляющее большинство населения было безграмотно, прочтение таких текстов «простолюдинами» было затруднительным. С древних времен использовались различные ***украшения букв*** текста, которые также затрудняли его понимание и делали это возможным лишь для «посвященных» (к которым в первую очередь относился сам автор: жрец, философ и так далее). Первые видоизменения письма не были связаны с целью засекречивания текста. Автор привлекал к себе внимание, вызывал удивление своим талантом, придавал «важность и авторитетность» своему письму и так далее.

К таким видоизмененным письменам прибегали некоторые писцы древнего Египта еще во 2 тысячелетии до н. э. В их письменности некоторые иероглифы заменялись на символические знаки, напоминающие иероглифы. В связи с этим нельзя не упомянуть о возможных ***«грамматических» ошибках***, меняющих письмо и наталкивающих на мысль о наличии сознательного видоизменения текста. Но затем видоизменения письма стали преследовать уже другую цель — защиту секретной информации. При этом естественным образом возникла проблема точного понимания секретного послания лицом, к которому оно обращено.

Эти письмена еще не являлись тайнописью, но уже демонстрировали возможности умышленного преобразования письма

Однако перечисленные методы записи сообщений можно отнести собственно не к их защите, а лишь к **«*маскировке*»,** к попыткам создать способ записи, совместимый со скоростью речи оратора, чьи высказывания фиксируются. Секрета здесь нет, нужно лишь освоить соответствующие навыки записи текстов.

Одно из требований, предъявляемое к методам и средствам защиты, — это требование оперативности связи.

Использование средств защиты не должно существенным образом задерживать передачу сообщения. С другой стороны, нападающая сторона также

должна учитывать временной фактор. Информация «стареет», и ее получение с большим запозданием может свести все усилия по ее добыванию «на нет».

Известно, что лучшей формой защиты является нападение. Это относится и к защите информации. В частности, нападающей стороне можно «подсунуть» дезинформацию и тем самым заставить нападающего действовать вопреки своим интересам.

Наряду с государственными методами защиты информации развивались и негосударственные.

К защите информации прибегали ***оппозиционеры*** («диссиденты») правящего режима, ***уголовный мир, религиозно-мистические общества, коммерсанты, ученые, скрывающие свои идеи от преследования государства и церкви и так далее***. К защите прибегали и частные лица, желающие сохранить в тайне от окружающих, от постороннего взгляда передаваемую информацию (например, *любовного содержания*). Иногда вклад таких дилетантов в историю криптографии был весьма заметным.

Необходимо отметить одно существенное обстоятельство. Исторические исследования в области криптографии опираются на изучение дошедших до наших дней материалов. Однако государственная криптографическая деятельность всегда велась под покровом великой тайны. Как правило, все секретные материалы уничтожались.

Эволюция криптографической деятельности в различных странах обычно не является прямолинейной. Как правило, здесь имеются ***взлеты и падения,*** вызванные конкретной исторической обстановкой. Нередко оригинальные методы защиты информации забывались и изобретались заново через столетия. Иногда плодотворные идеи возникали параллельно в различных странах. Имеются определенные объективные трудности в сопоставлении уровня развития криптографии в различных странах.

Криптография в историческом аспекте развивалась не «сама по себе». Внимание, уделяемое развитию криптографии, зависело от активности деятельности государства в различных сферах: политической, дипломатической, военной, экономической и так далее.

Криптография выполняла заказы государства и развивалась при его соответствующей поддержке.

Успехи в дешифровании шифров приводили к разработке новых шифров; в свою очередь, разработка новых шифров — к поиску новых методов их дешифрования.

Огромное влияние на развитие криптографии во всей истории ее существования оказывали достижения научно-технического прогресса.

Криптография (в современном понимании этого слова) появилась практически сразу же после появления письменности. Мощный импульс ее развитию дало изобретение алфавитной письменности.

К проблемам в настоящее время относятся такие, как

- защита от имитации («дезинформации под шифром»),
- идентификация абонентов («электронная подпись»),
- проблема создания различных криптографических протоколов обмена информацией и так далее.

Во все времена учитывались затраты на защиту информации и на реализацию методов нападения.

Вопрос о том, что и как защищается (и какой ценой), что и как достается (и какой ценой) — это очень серьезный вопрос.

Один древний мудрец сказал: ***«Нельзя ловить рыбу на золотой крючок».***

Потеря крючка не окупается стоимостью выловленной рыбы.

Постепенно появилось понимание того, что криптографической деятельностью в государстве должны заниматься не только талантливые одиночки —самоучки (их оказалось явно недостаточно), но и специально подготовленные к этой деятельности специалисты — криптографы.

История учит не только прошлому, но и пониманию настоящего, а также прогнозированию будущего.

По утверждению ряда специалистов, криптография по возрасту — ровесник египетских пирамид. В документах древних цивилизаций — Индии, Египта, Месопотамии — есть сведения о системах и способах составления шифрованных писем.

Один из самых старых шифрованных текстов из ***Месопотамии*** представляет собой глиняную табличку, написанную клинописью и содержащую рецепт для изготовления глазури в гончарном производстве ((XX в. до н. э. Для его написания были использованы редко употребляемые клинописные знаки, игнорировались некоторые гласные и согласные и употреблялись числа вместо имен.)

Шифрованные тексты Древнего Египта — это чаще всего религиозные тексты и медицинские рецепты. Древним египтянам была известна и стеганография. Они использовали так называемое «загадочное», или «играющее», письмо.

Древние египтяне использовали и символический язык. Так, в 1998 г. был дешифрован текст, записанный на каменных плитах. Этому тексту более 6 000 лет, он получил название ***Великие Арканы Таро***. В нем в символической форме трактуются принципы мироздания, говорится об абсолютной и относительной истине и своеобразно обсуждаются законы диалектики, с которой, как выяснилось, древние египтяне были знакомы.

Наиболее полные и достоверные сведения о шифрах относятся к Древней Греции. Подчеркнем, что европейская криптография (в современном понимании этого слова) появилась в Греции. И это понятно. Именно в Греции зародились современная наука, живопись, архитектура и так далее. Мощным толчком к развитию криптографии послужил и тот факт, что в Греции впервые окончательно сформировалось европейское алфавитное письмо (VIII в. до н. э.). Греческий алфавит в дальнейшем породил латинский и русский алфавиты. Зачатки алфавитного письма имели место в Древнем Египте, затем у семитов, но европейское алфавитное письмо в полном объеме появилось именно в Греции. До этого момента были распространены письменности (пиктография, идеографическое и иероглифическое письмо и др.), слабо пригодные для практического применения шифров.

Греческий философ, историк Плутарх (I в. н. э.) отмечал, что древнеегипетские жрецы хранили свои прорицания в тайнописной (шифрованной) форме.

Во времена средневековья европейская криптография приобрела сомнительную славу, отголоски которой слышатся и в наши дни. ***Криптографию стали отождествлять с черной магией***, с некоторой формой оккультизма, астрологией, алхимией, еврейской каббалой. К шифрованию информации призывались мистические силы.

2. Основные понятия и элементы криптографии (алгоритм, ключ, шифр)

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.

Криптография является основой любой защищенной связи, и поэтому так важно познакомиться с тремя основными криптографическими функциями: симметричным шифрованием, асимметричным шифрованием и односторонними хэш-функциями.

Все существующие технологии аутентификации, целостности и конфиденциальности созданы на основе именно этих трех функций.

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

В этой лекции основное внимание будет уделено криптографическим методам.

Современная криптография включает в себя четыре крупных раздела:

1. Симметричные криптосистемы.
2. Криптосистемы с открытым ключом.
3. Системы электронной подписи.
4. Управление ключами.

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.

Итак, 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.

В качестве примеров алфавитов, используемых в современных ИС можно привести следующие:

- алфавит Z33 - 32 буквы русского алфавита и пробел;
- алфавит Z256 - символы, входящие в стандартные коды ASCII и КОИ-8;
- бинарный алфавит - Z2 = {0,1};
- восьмеричный алфавит или шестнадцатеричный алфавит;

Шифрование - преобразовательный процесс: исходный текст, который носит также название открытого текста, заменяется шифрованным текстом (Рис. 1).

Рис. 1. Процесс шифрования

Дешифрование - обратный шифрованию процесс. На основе ключа шифрованный текст преобразуется в исходный (Рис. 2).

Рис. 2. Процесс дешифрования

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.

Криптосистемы разделяются на **симметричные** и **ассиметричные** (с открытым ключом).

В симметричных криптосистемах и для шифрования, и для дешифрования используется один и тот же ключ.

В системах с открытым ключом используются два ключа - открытый и закрытый, которые математически связаны друг с другом. Информация шифруется с помощью открытого ключа, который доступен всем желающим, а расшифровывается с помощью закрытого ключа, известного только получателю сообщения.

Хэш-функцией называется функция, которую легко рассчитать, но обратное восстановление которой требует больших усилий (например, возведение в степень и логарифмирование).

Входящее сообщение пропускается через математическую функцию (хэш-функцию), и в результате на выходе мы получаем некую последовательность битов. Эта последовательность называется «хэш» (или результат обработки). Хэширование обычно сочетается с технологией открытых ключей.

Термины распределение ключей и управление ключами относятся к процессам системы обработки информации, содержанием которых является составление и распределение ключей между пользователями.

Электронной (цифровой) подписью называется присоединяемое к тексту его криптографическое преобразование (или зашифрованный хэш), которое позволяет при получении текста другим пользователем проверить авторство и подлинность сообщения.

Криптостойкостью называется характеристика шифра, определяющая его стойкость к дешифрованию без знания ключа (т.е. криптоанализу). Имеется несколько показателей криптостойкости, среди которых: количество всех возможных ключей и среднее время, необходимое для криптоанализа.

Преобразование Tk определяется соответствующим алгоритмом и значением параметра k. Эффективность шифрования с целью защиты информации зависит от сохранения тайны ключа и криптостойкости шифра.

Процесс криптографического закрытия данных может осуществляться как программно, так и аппаратно. Аппаратная реализация отличается существенно большей стоимостью, однако ей присущи и преимущества: высокая производительность, простота, защищенность и т.д. Программная реализация более практична, допускает известную гибкость в использовании.

Для современных криптографических систем защиты информации сформулированы следующие общепринятые требования:

- зашифрованное сообщение должно поддаваться чтению только при наличии ключа;

- число операций, необходимых для определения использованного ключа шифрования по фрагменту шифрованного сообщения и соответствующего ему открытого текста, должно быть не меньше общего числа возможных ключей;

- число операций, необходимых для расшифровывания информации путем перебора всевозможных ключей должно иметь строгую нижнюю оценку и выходить за пределы возможностей современных компьютеров (с учетом возможности использования сетевых вычислений);

- знание алгоритма шифрования не должно влиять на надежность защиты;

- незначительное изменение ключа должно приводить к существенному изменению вида зашифрованного сообщения даже при использовании одного и того же ключа;

- структурные элементы алгоритма шифрования должны быть неизменными;

- дополнительные биты, вводимые в сообщение в процессе шифрования, должен быть полностью и надежно скрыты в шифрованном тексте;

- длина шифрованного текста должна быть равной длине исходного текста;

- не должно быть простых и легко устанавливаемых зависимостей между ключами, последовательно используемыми в процессе шифрования;

- любой ключ из множества возможных должен обеспечивать надежную защиту информации;

- алгоритм должен допускать как программную, так и аппаратную реализацию, при этом изменение длины ключа не должно вести к качественному ухудшению алгоритма шифрования.

Симметричные и асимметричные криптосистемы

Симметричные криптосистемы

Симметричное шифрование, которое часто называют шифрованием с помощью секретных ключей, в основном используется для обеспечения конфиденциальности данных.

На Рис. 3 показаны два пользователя, Алиса и Боб, которые хотят установить между собой конфиденциальную связь. Для этого Алиса и Боб должны совместно выбрать единый математический алгоритм, который будет использоваться для шифрования и расшифровки данных. Кроме того, им нужно выбрать общий ключ (секретный ключ), который будет использоваться с принятым ими алгоритмом шифрования/расшифровки.

Рис. 3. Симметричное шифрование с использованием одного секретного ключа

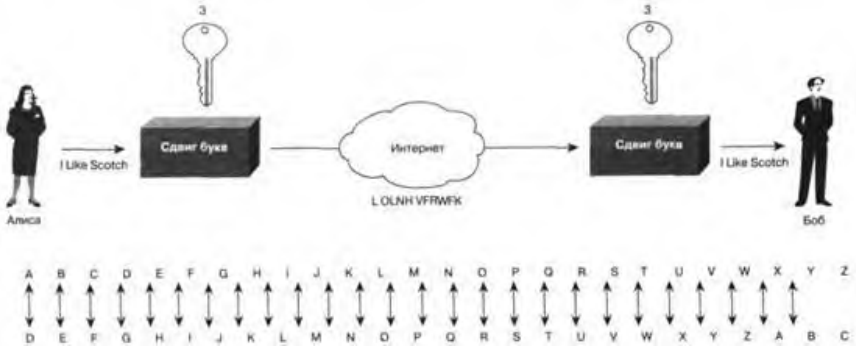

Рис. 4. Шифр Цезаря

Весьма упрощенным примером алгоритма секретного ключа является так называемый шифр Цезаря, представленный на Рис. 4. Этот метод шифрования заключается в том, что каждая буква в тексте заменяется на другую букву, находящуюся на определенном расстоянии от нее в алфавите. При шифровании или расшифровке этот алгоритм как бы сдвигает буквы вверх и вниз по алфавиту. Ключом в этом примере являются три буквы.

Совершенно ясно, что если кто-нибудь получит зашифрованное этим способом сообщение и будет знать алгоритм (куда сдвигать буквы – вверх или вниз по алфавиту), он сможет легко раскрыть ключ методом простого перебора, который заключается в том, что человек перебирает все возможные комбинации алгоритма до тех пор, пока не получит в результате расшифрованный текст. Обычно, чем длиннее ключ и чем сложнее алгоритм, тем труднее решить задачу расшифровки простым перебором вариантов.

Сегодня широко используются такие алгоритмы секретных ключей, как Data Encryption Standard (DES), 3DES (или «тройной DES») и International Data Encryption Algorithm (IDEA). Эти алгоритмы шифруют сообщения блоками по 64 бита. Если объем сообщения превышает 64 бита (как это обычно и бывает), необходимо разбить его на блоки по 64 бита в каждом, а затем каким-то образом свести их воедино. Такое объединение, как правило, происходит одним из следующих четырех методов: электронной кодовой книги (ECB), цепочки зашифрованных блоков (CBC), x-битовой зашифрованной обратной связи (CFB-x) или выходной обратной связи (OFB).

В настоящее время все чаще говорят о неоправданной сложности и невысокой криптостойкости. На практике приходится использовать его модификации.

Более эффективным является отечественный стандарт шифрования данных ГОСТ 28147-89. Он рекомендован к использованию для защиты любых данных, представленных в виде двоичного кода, хотя не исключаются и другие методы шифрования. Данный стандарт формировался с учетом мирового опыта, и в частности, были приняты во внимание недостатки и нереализованные возможности алгоритма DES, поэтому использование стандарта ГОСТ предпочтительнее.

Шифрование с помощью секретного ключа чаще всего используется для поддержки конфиденциальности данных и очень эффективно реализуется с помощью неизменяемых «вшитых» программ (firmware). Этот метод можно использовать для аутентификации и поддержания целостности данных, но метод цифровой подписи (о котором мы скажем позже) является более эффективным. С методом секретных ключей связаны следующие проблемы:

1. Необходимо часто менять секретные ключи, поскольку всегда существует риск их случайного раскрытия.

2. Трудно обеспечить безопасное генерирование и распространение секретных ключей.

3. Для получения и безопасного распространения секретных ключей обычно используется алгоритм Диффи-Хеллмана (Diffie-Hellman), который описывается ниже.

Все многообразие существующих симметричных криптографических методов можно свести к следующим классам преобразований (Рис. 5):

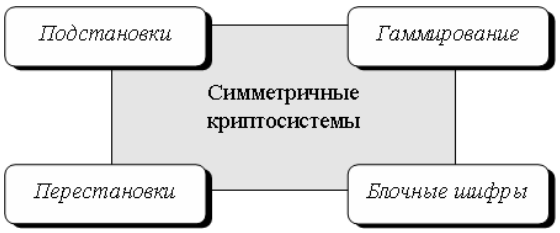

Рис. 5. Классы преобразований существующих симметричных криптографических методов

Моно- и многоалфавитные подстановки

Наиболее простой вид преобразований, заключающийся в замене символов исходного текста на другие (того же алфавита) по, более или менее, сложному правилу. Для обеспечения высокой криптостойкости требуется использование больших ключей.

Перестановки

Также несложный метод криптографического преобразования. Используется, как правило, в сочетании с другими методами.

Гаммирование

Этот метод заключается в наложении на исходный текст некоторой псевдослучайной последовательности, генерируемой на основе ключа.

Блочные шифры

Представляют собой последовательность (с возможным повторением и чередованием) основных методов преобразования, применяемую к блоку (части) шифруемого текста. Блочные шифры на практике встречаются чаще, чем «чистые» преобразования того или иного класса в силу их более высокой криптостойкости. Российский и американский стандарты шифрования основаны именно на этом классе шифров.

Применение технологии шифрования с симметричным ключом

Технология шифрования часто используется в приложениях, связанных с управлением ключами и аутентификацией. Эти приложения описаны ниже.

Алгоритм Диффи-Хеллмана

Алгоритм Диффи-Хеллмана позволяет двум сторонам, Алисе и Бобу, создать общий для них секретный ключ, известный только им двоим, несмотря на то, что связь между ними осуществляется по незащищенному каналу. Затем этот секретный ключ используется для шифрования данных с помощью алгоритма секретного ключа. На Рис. 6 показан пример использования алгоритма Диффи-Хеллмана в сочетании с алгоритмом DES для создания секретных ключей и последующего использования этих ключей для поддержки конфиденциальности данных.

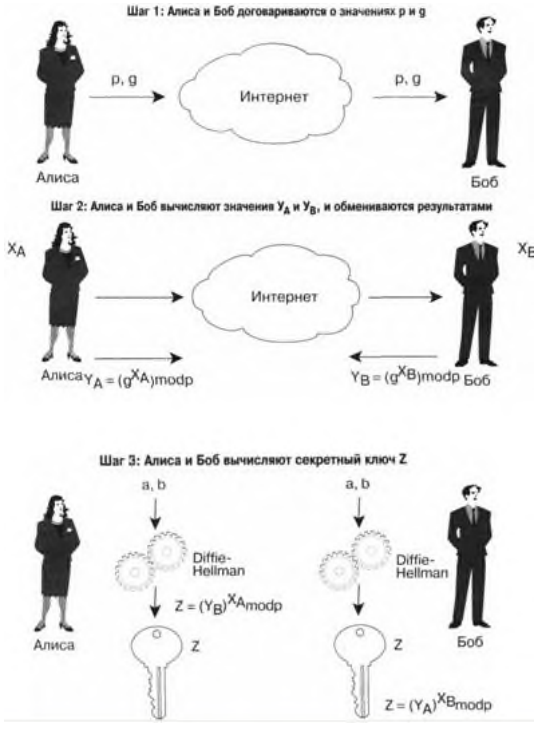

Рис. 6. Алгоритм Диффи-Хеллмана с ключом DES

Два числа, p (простое число) и g (меньшее, чем p, но с некоторыми исключениями), используются совместно. И Алиса, и Боб генерируют (каждый для себя) большое случайное число. Эти числа (XA и XB) держатся в секрете. Далее используется алгоритм Диффи-Хеллмана. И Алиса, и Боб проводят вычисления с помощью этого алгоритма и обмениваются их результатами. Окончательным результатом является общая величина Z. Этот ключ Z используется как ключ DES для шифрования и расшифровки данных. Человек, который знает величину p или g, не сможет легко рассчитать общую величину Z из-за трудностей с факторизацией очень больших простых чисел.

Асимметричные криптосистемы

Как бы ни были сложны и надежны криптографические системы - их слабое место при практической реализации - проблема распределения ключей. Для того, чтобы был возможен обмен конфиденциальной информацией между двумя субъектами ИС, ключ должен быть сгенерирован одним из них, а затем каким-то образом опять же в конфиденциальном порядке передан другому. Т.е. в общем случае для передачи ключа опять же требуется использование какой-то криптосистемы.

Для решения этой проблемы на основе результатов, полученных классической и современной алгеброй, были предложены асимметричные криптосистемы (системы с открытым ключом).

Суть их состоит в том, что каждым адресатом ИС генерируются два ключа, связанные между собой по определенному правилу. Один ключ объявляется открытым (общим), а другой закрытым (частным, секретным). Открытый ключ публикуется и доступен любому, кто желает послать сообщение адресату. Секретный ключ сохраняется в тайне.

Исходный текст шифруется открытым ключом адресата и передается ему. Зашифрованный текст, в принципе, не может быть расшифрован тем же открытым ключом. Дешифрование сообщение возможно только с использованием закрытого ключа, который известен только самому адресату.

Таким образом, асимметричное шифрование часто называют шифрованием с помощью общего ключа, при котором используются разные, но взаимно

дополняющие друг друга ключи и алгоритмы шифрования и расшифровки. Этот механизм полагается на два взаимосвязанных ключа: общий ключ и частный ключ. Если Алиса и Боб хотят установить связь с использованием шифрования через общий ключ, обоим нужно получить два ключа: общий и частный (Рис. 7). Для шифрования и расшифровки данных Алиса и Боб будут пользоваться разными ключами.

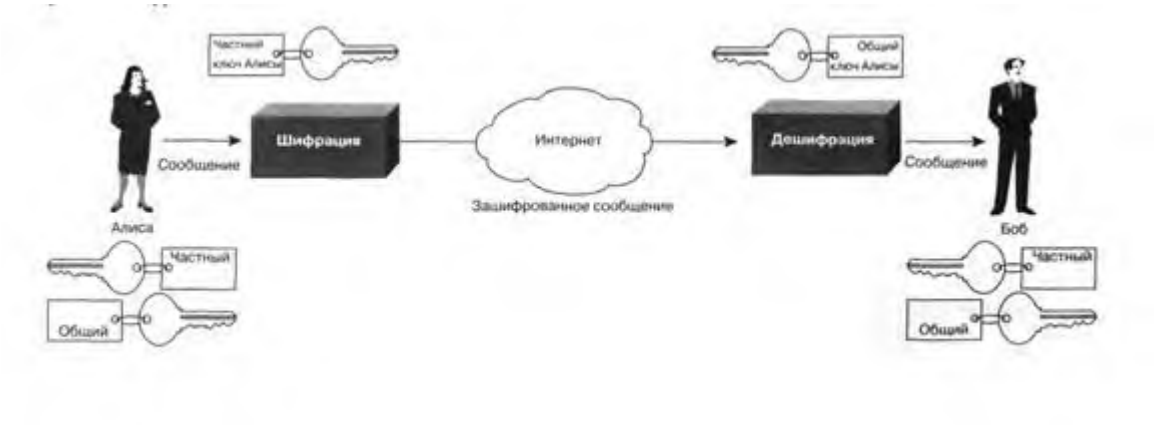

Рис. 7. Асимметричное шифрование с помощью общего ключа

Асимметричные системы для преобразования ключей (что нужно для необратимости процесса шифрования даже для отправителя сообщения) используют так называемые необратимые или односторонние функции (безопасные хэш-функции), которые обладают следующим свойством: при заданном значении x относительно просто вычислить значение f(x), однако если y=f(x), то нет простого пути для вычисления значения x.

Другими словами, безопасной хэш-функцией называется функция, которую легко рассчитать, но обратное восстановление которой требует непропорционально больших усилий. Входящее сообщение пропускается через математическую функцию (хэш-функцию), и в результате на выходе мы получаем некую последовательность битов. Эта последовательность называется «хэш» (или «результат обработки сообщения»). Этот процесс практически невозможно восстановить. Другими словами, имея выходные данные, невозможно получить входные. Хэш-функцию можно сравнить с кофемолкой. Если сообщение – это кофейные зерна, а хэш на выходе – это размолотый кофе, то, имея такой размолотый кофе, вы не сможете восстановить кофейные зерна.

Хэш-функция принимает сообщение любой длины и выдает на выходе хэш фиксированной длины. Наиболее известные из хэш-функций (поддерживаемые современными операционными системами):

- алгоритм Message Digest 2 (MD2);
- алгоритм Message Digest 4 (MD4);
- алгоритм Message Digest 5 (MD5);
- алгоритм безопасного хэша (Secure Hash Algorithm – SHA).

Три алгоритма серии MD разработаны Ривестом в 1989-м, 90-м и 91-м году соответственно. Все они преобразуют текст произвольной длины в 128-битную сигнатуру (кодовую комбинацию).

Алгоритм MD2 предполагает:

- дополнение текста до длины, кратной 128 битам;
- вычисление 16-битной контрольной суммы (старшие разряды отбрасываются);
- добавление контрольной суммы к тексту;
- повторное вычисление контрольной суммы.

Алгоритм MD4 предусматривает:

- дополнение текста до длины, равной 448 бит по модулю 512;
- добавляется длина текста в 64-битном представлении;
- 512-битные блоки подвергаются процедуре Damgard-Merkle (в отличие от хэш-функции - этот класс преобразований предполагает вычисление для аргументов фиксированной длины также фиксированных по длине значений), причем каждый блок участвует в трех разных циклах.

В алгоритме MD4 довольно быстро были найдены «дыры», поэтому он был заменен алгоритмом MD5, в котором каждый блок участвует не в трех, а в четырех различных циклах.

Алгоритм SHA (Secure Hash Algorithm) разработан NIST (National Institute of Standard and Technology) и повторяет идеи серии MD. В SHA используются тексты более 264 бит, которые закрываются сигнатурой длиной 160 бит.

Множество классов необратимых функций и порождает все разнообразие систем с открытым ключом. Однако не всякая необратимая функция годится для использования в реальных ИС.

В самом определении необратимости присутствует неопределенность. Под необратимостью понимается не теоретическая необратимость, а практическая невозможность вычислить обратное значение используя современные вычислительные средства за обозримый интервал времени.

Поэтому чтобы гарантировать надежную защиту информации, к асимметричным системам с открытым ключом (СОК) предъявляются два важных и очевидных требования:

1. Преобразование исходного текста должно быть необратимым и исключать его восстановление на основе открытого ключа.

2. Определение закрытого ключа на основе открытого также должно быть невозможным на современном технологическом уровне. При этом желательна точная нижняя оценка сложности (количества операций) раскрытия шифра.

Вообще же все предлагаемые сегодня криптосистемы с открытым ключом опираются на один из следующих типов необратимых преобразований:

1. Разложение больших чисел на простые множители.

2. Вычисление логарифма в конечном поле.

3. Вычисление корней алгебраических уравнений.

Здесь же следует отметить, что алгоритмы криптосистемы с открытым ключом (СОК) можно использовать в трех назначениях.

1. Как самостоятельные средства защиты передаваемых и хранимых данных, в целях обеспечения конфиденциальности данных.

2. Как средства для распределения ключей, обеспечивающее получение общих ключей для совместного использования. Алгоритмы СОК более трудоемки, чем традиционные криптосистемы. Поэтому часто на практике рационально с помощью СОК распределять ключи, объем которых как информации незначителен. А потом с помощью обычных алгоритмов осуществлять обмен большими информационными потоками.

3. Средства аутентификации пользователей.

Чтобы лучше понять, как достигается конфиденциальность данных и проводится аутентификация отправителя, пройдем по всему процессу шаг за шагом. Сначала и Алиса, и Боб должны создать свои пары общих/частных ключей. После создания таких пар Алиса и Боб должны обменяться своими общими ключами. На Рис. 8 показано, как шифрование с помощью общих ключей обеспечивает конфиденциальность информации. Если Алиса хочет отправить Бобу конфиденциальные данные, она шифрует данные с помощью общего ключа Боба и отправляет Бобу данные, зашифрованные этим способом. Получив сообщение от Алисы, Боб расшифровывает его с помощью своего частного ключа. Так как никто, кроме Боба, не имеет этого частного ключа, данные, отправленные Алисой, может расшифровать только Боб. Таким образом, поддерживается конфиденциальность данных.

Рис. 8. Конфиденциальность данных, зашифрованных с помощью открытого ключа

На Рис. 9 показано, как шифрование с помощью общего ключа помогает проводить аутентификацию отправителя. Боб хочет быть уверен, что сообщение отправлено именно Алисой, а не человеком, который выдает себя за нее. Поскольку общий ключ не является секретным, доступ к нему может получить кто угодно. Но если Алиса зашифрует сообщение своим частным ключом, Боб должен расшифровать его с помощью общего ключа Алисы. Аутентификация происходит потому, что доступ к частному ключу Алисы имеет только она одна, и поэтому данные могли быть зашифрованы только ею.

Рис. 9. Аутентификация отправителя с помощью шифрования общим ключом

Важным аспектом асимметричного шифрования является то, что частный ключ должен храниться в тайне. Если частный ключ будет раскрыт, то человек, знающий этот ключ, сможет выступать от вашего имени, получать ваши сообщения и отправлять сообщения так, будто это делаете вы.

Механизмы генерирования пар общих/частных ключей являются достаточно сложными, но в результате получаются пары очень больших случайных чисел, одно из которых становится общим ключом, а другое – частным. Генерирование таких чисел требует больших процессорных мощностей, поскольку эти числа, а также их произведения должны отвечать строгим математическим критериям. Однако этот процесс генерирования абсолютно необходим для обеспечения уникальности каждой пары общих/частных ключей. Алгоритмы шифрования с помощью общих ключей редко используются для поддержки конфиденциальности данных из-за ограничений производительности. Вместо этого их часто используют в приложениях, где аутентификация проводится с помощью цифровой подписи и управления ключами.

Среди наиболее известных алгоритмов общих ключей можно назвать RSA (разработан в 1977 году и получил название в честь его создателей: Рона Ривеста, Ади Шамира и Леонарда Эйдельмана) и ElGamal.

Алгоритм RSA стал мировым стандартом де-факто для открытых систем и рекомендован МККТТ.

Разработчики алгоритма воспользовались тем фактом, что нахождение больших простых чисел в вычислительном отношении осуществляется легко, но разложение на множители произведения двух таких чисел практически невыполнимо. Доказано (теорема Рабина), что раскрытие шифра RSA эквивалентно такому разложению. Поэтому для любой длины ключа можно дать

нижнюю оценку числа операций для раскрытия шифра, а с учетом производительности современных компьютеров оценить и необходимое на это время.

Возможность гарантированно оценить защищенность алгоритма RSA стала одной из причин популярности этой СОК на фоне десятков других схем. Поэтому алгоритм RSA используется в банковских компьютерных сетях, особенно для работы с удаленными клиентами (обслуживание кредитных карточек).

3. Требования к криптосистемам

Процесс криптографического закрытия данных может осуществляться как программно, так и аппаратно. Аппаратная реализация отличается существенно большей стоимостью, однако ей присущи и преимущества: высокая производительность, простота, защищенность и т.д. Программная реализация более практична, допускает известную гибкость в использовании.

Для современных криптографических систем защиты информации сформулированы следующие общепринятые требования:

- зашифрованное сообщение должно поддаваться чтению только при наличии ключа;

- число операций, необходимых для определения использованного ключа шифрования по фрагменту шифрованного сообщения и соответствующего ему открытого текста, должно быть не меньше общего числа возможных ключей;

- число операций, необходимых для расшифровывания информации путем перебора всевозможных ключей должно иметь строгую нижнюю оценку и выходить за пределы возможностей современных компьютеров (с учетом возможности использования сетевых вычислений);

- знание алгоритма шифрования не должно влиять на надежность защиты;

- незначительное изменение ключа должно приводить к существенному изменению вида зашифрованного сообщения даже при использовании одного и того же ключа;

- структурные элементы алгоритма шифрования должны быть неизменными;

- дополнительные биты, вводимые в сообщение в процессе шифрования, должен быть полностью и надежно скрыты в шифрованном тексте;

- длина шифрованного текста должна быть равной длине исходного текста;

- не должно быть простых и легко устанавливаемых зависимостью между ключами, последовательно используемыми в процессе шифрования;

- любой ключ из множества возможных должен обеспечивать надежную защиту информации;

- алгоритм должен допускать как программную, так и аппаратную реализацию, при этом изменение длины ключа не должно вести к качественному ухудшению алгоритма шифрования.

Контрольные вопросы:

1. Что понимается под термином управление криптографическими ключами? Какова основная цель и основные задачи управления ключами?
2. В чем, на Ваш взгляд, отличие жизненного цикла секретных и открытых криптографических ключей?
3. Каковы перспективы практического применения концепции инфраструктуры открытых ключей?
4. Изложите в общих чертах существо сертификации открытых ключей.
5. Каким образом распространяются открытых ключей в криптосистемах?
6. Укажите преимущества симметричных криптосистем, определившие их как национальные стандарты государств.
7. Что такое удостоверяющий центр?
8. Для чего применяются хэш-функции?
9. Какие классы преобразования распространены в симметричных системах?
10. Для чего необходима электронная цифровая подпись?