Глава 2
Основные понятия

Целью настоящего раздела является определение основных понятий и задач криптографии.

§ 2.1. Криптография

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

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

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

Можно воспользоваться одним из известных методов сокрытия информации:

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

— замаскировать канал передачи закрытой информации в открытом канале связи, например спрятав информацию в безобидном "контейнере" с использованием тех или других стеганографических 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.

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

— проверку и подтверждение подлинности содержания и источника сообщения,

а также

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

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

Поэтому можно сказать, что 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 безопасности информационного взаимодействия и составляет основные цели криптографии. Они определяются следующим образом.

Обеспечение *конфиденциальности* — решение проблемы защиты информации от ознакомления с ее содержанием со стороны лиц, не имеющих права доступа к ней. В зависимости от контекста вместо термина "конфиденциальная" информация могут выступать термины "секретная", "частная", "ограниченного доступа" информация.

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

Обеспечение *аутентификации* — разработка методов подтверждения подлинности сторон (*идентификация*) и самой информации в процессе информационного взаимодействия. Информация, передаваемая по каналу связи, должна быть аутентифицирована по источнику, времени создания, содержанию данных, времени пересылки и т. д.

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

Конфиденциальность

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

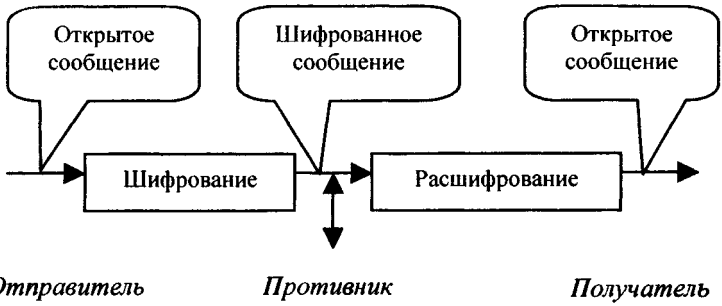

Рис. 7. Передача шифрованной информации

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

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

Под *шифром* обычно понимается семейство обратимых преобразований, каждое из которых определяется некоторым параметром, называемым ключом, а также порядком применения данного преобразования, называемым *режимом шифрования* [1].

[1] Формальное определение шифра будет дано ниже.

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

Каждое преобразование однозначно определяется ключом и описывается некоторым *криптографическим алгоритмом*. Один и тот же криптографический алгоритм может применяться для шифрования в различных режимах. Тем самым реализуются различные способы шифрования (простая замена, гаммирование [2] и т. п.). Каждый режим шифрования имеет как свои преимущества, так и недостатки. Поэтому выбор режима зависит от конкретной ситуации. При расшифровании используется криптографический алгоритм, который в общем случае может отличаться от алгоритма, применяемого для зашифрования сообщения. Соответственно могут различаться ключи зашифрования и расшифрования. Пару алгоритмов зашифрования и расшифрования обычно называют *криптосистемой (шифрсистемой)*, а реализующие их устройства — *шифртехникой*.

Если обозначить через M открытое, а через C шифрованное сообщения, то процессы зашифрования и расшифрования можно записать в виде равенств

$$E_{k_1}(M) = C,$$

$$D_{k_2}(C) = M,$$

в которых алгоритмы зашифрования E и расшифрования D должны удовлетворять равенству

$$D_{k_2}(E_{k_1}(M)) = M.$$

[2] Эти способы шифрования будут рассмотрены ниже.

Различают *симметричные* и *асимметричные* криптосистемы. В симметричных системах знание ключа зашифрования k_1 позволяет легко найти ключ расшифрования k_2 (в большинстве случаев эти ключи просто совпадают). В асимметричных криптосистемах знание ключа k_1 не позволяет определить ключ k_2. Поэтому для симметричных криптосистем оба ключа должны сохраняться в секрете, а для асимметричных — только один — ключ расшифрования k_2, а ключ k_1 можно сделать открытым (общедоступным). В связи с этим их называют еще *шифрами с открытым ключом.*

Симметричные криптосистемы принято подразделять на *поточные* и *блочные* системы. Поточные системы осуществляют зашифрование отдельных символов открытого сообщения. Блочные же системы производят зашифрование блоков фиксированной длины, составленных из подряд идущих символов сообщения.

Асимметричные криптосистемы, как правило, являются блочными. При их использовании можно легко организовать передачу конфиденциальной информации в сети с большим числом пользователей. В самом деле, для того чтобы послать сообщение, отправитель открыто связывается с получателем, который либо передает свой ключ отправителю, либо помещает его на общедоступный сервер. Отправитель зашифровывает сообщение на открытом ключе получателя и отправляет его получателю. При этом никто, кроме получателя, обладающего ключом расшифрования, не сможет ознакомиться с содержанием передаваемой информации. В результате такая система шифрования с общедоступным ключом позволяет существенно сократить объем хранимой каждым абонентом секретной ключевой информации.

Возможна и другая симметричная ситуация, когда открытый и секретный ключи меняются местами. Предположим, например, что для проведения контроля соблюдения выполнения каждой стороной договора об ограничении испытаний ядерного оружия создаются пункты контроля, которые ведут

запись и конфиденциальную передачу сторонам, участвующим в договоре, сейсмологической информации. Поскольку на каждом таком пункте контролируемая сторона одна, а участников договора может быть очень много, то необходимо обеспечить такое шифрование информации, при котором зашифровать сообщение мог бы только один отправитель, а расшифровать мог бы каждый.

Не существует единого шифра, подходящего для всех случаев жизни. Выбор способа шифрования (то есть криптографического алгоритма и режима его использования) зависит от особенностей передаваемой *информации* (ее ценности, объема, способа представления, необходимой скорости передачи и т. д.), а также возможностей владельцев по защите своей информации (стоимость применяемых технических устройств, удобство использования, надежность функционирования и т. п.). Имеется большое разнообразие *видов* защищаемой информации: текстовая, телефонная, телевизионная, компьютерная и т. д., причем у каждого вида информации имеются свои существенные особенности, которые надо учитывать при выборе способа шифрования. Большое значение имеют объемы и требуемая скорость передачи шифрованной информации, а также помехозащищенность используемого канала связи. Все это существенным образом влияет на выбор криптографического алгоритма и организацию защищенной связи.

Наличие надежного криптографического алгоритма и правильный выбор режима еще не гарантируют владельцу защищенность передаваемой информации. Немаловажную роль играет правильность их использования. Поскольку даже самые стойкие шифры при неправильном использовании существенно теряют свои качества, то конфиденциальность передаваемой информации во многом зависит от того, какие *ошибки* допускает ее владелец при использовании криптографической защиты. А то, что все пользователи допускают ошибки, — неизбежно и является непреложным и важным

(для криптоаналитика) фактом, поскольку любые криптографические средства, какими бы они ни были удобными и прозрачными, всегда мешают пользователям в работе, а различные тонкости известны только криптоаналитикам и, как правило, непонятны пользователям этих средств. Более того, в качестве субъектов взаимодействия могут выступать не только люди, но и различные процессы, осуществляющие обработку информации в автоматизированной системе без участия человека. Поэтому защищенность информации в системе существенно зависит от того, насколько правильно там реализована криптографическая подсистема, отвечающая за выполнение криптографических функций. Одно наличие такой подсистемы еще ничего не гарантирует.

Подчеркнем разницу между терминами "*расшифрование*" и "*дешифрование*". При расшифровании действующий ключ считается известным, в то время как при дешифровании ключ неизвестен. Тем самым расшифрование должно осуществляться столь же просто, как и зашифрование; дешифрование представляет собой значительно более сложную задачу. Именно в этом и состоит смысл шифрования.

Для разных шифров задача дешифрования имеет различную сложность. Уровень сложности этой задачи и определяет главное свойство шифра — способность противостоять попыткам противника завладеть защищаемой информацией. В связи с этим говорят о *криптографической стойкости* шифра (или просто *стойкости*), различая более стойкие и менее стойкие шифры. Методы вскрытия шифров разрабатывает наука, носящая название *криптоанализ*. Согласно [Kah67], термин криптоанализ ввел У. Фридман в 1920 г.

В иностранной литературе часто используется термин *криптология* в качестве области знаний, объединяющей *криптографию* и *криптоанализ*, при этом криптография понимается как наука о создании шифров. Если следовать такому толкованию, то можно прийти к тезису о том, что задачи создания криптографической защиты и ее преодоления прин-

ципиально различаются. На самом деле было бы нелогично считать защиту надежной без проведения детального криптоанализа. В связи с этим, применительно к задаче обеспечения конфиденциальности, мы будем считать термины криптография и криптология синонимами, понимая их как название науки о синтезе шифров и "взломе" шифров.

Целостность

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

Итак, для проверки целостности к сообщению M добавляется проверочная комбинация S, называемая *кодом аутентификации сообщения* (сокращенно — КАС) или *имитовставкой*. В этом случае по каналу связи передается пара $C=(M,S)$. При получении сообщения M пользователь вычисляет значение проверочной комбинации и сравнивает его

с полученным контрольным значением S. Несовпадение говорит о том, что данные были изменены.

Как правило, код аутентификации является значением некоторой (зависящей от секретного ключа) криптографической *хэш-функции*[3] от данного сообщения: $h_k(M) = S$. К кодам аутентификации предъявляются определенные требования. К ним относятся:

— невозможность вычисления значения $h_k(M) = S$ для заданного сообщения M без знания ключа k;

— невозможность подбора для заданного сообщения M с известным значением $h_k(M) = S$ другого сообщения M_1 с известным значением $h_k(M_1) = S_1$ без знания ключа k.

Первое требование направлено против создания поддельных (сфабрикованных) сообщений при атаках типа *имитация*; второе — против модификации передаваемых сообщений при атаках типа *подмена*.

Аутентификация

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

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

---

[3] Так обычно называется функция, принимающая значения некоторой фиксированной размерности.

Рассмотрим эти вопросы более подробно.

Применительно к сеансу связи (транзакции) аутентификация означает проверку: целостности соединения, невозможности повторной передачи данных противником и своевременности передачи данных. Для этого, как правило, используют дополнительные параметры, позволяющие "сцепить" передаваемые данные в легко проверяемую последовательность. Это достигается, например, путем вставки в сообщения некоторых специальных чисел или *меток времени*. Они позволяют предотвратить попытки повторной передачи, изменения порядка следования или обратной отсылки части переданных сообщений. При этом такие вставки в передаваемом сообщении необходимо защищать (например, с помощью шифрования) от возможных подделок и искажений.

Применительно к сторонам взаимодействия аутентификация означает проверку одной из сторон того, что взаимодействующая с ней сторона — именно та, за которую она себя выдает. Часто аутентификацию сторон называют также *идентификацией* [4].

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

Протокол — это распределенный алгоритм, определяющий последовательность действий каждой из сторон. В процессе выполнения протокола идентификации каждая из сто-

[4] Формально это некорректно, так как под идентификацией понимают процедуру установления присвоенного данной стороне уникального системного имени-идентификатора, которое позволяет отличать ее от других сторон; обычно идентификация заключается в предъявлении этого имени и предшествует процедуре аутентификации, то есть подтверждению правильности идентификации.

рон не передает никакой информации о своем секретном ключе, а хранит его у себя и использует для формирования ответных сообщений на запросы, поступающие при выполнении протокола.

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

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

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

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

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

Цифровая подпись

В некоторых ситуациях, например в силу изменившихся обстоятельств, отдельные лица могут отказаться от ранее

принятых обязательств. В связи с этим необходим некоторый механизм, препятствующий подобным попыткам.

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

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

Хотя цифровая подпись и имеет существенные отличия, связанные с возможностью отделения от документа и независимой передачей, а также возможностью подписывания одной подписью всех копий документа, она во многом аналогична обычной "ручной" подписи.

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 сообще-

ний с ключа одного из абонентов на ключ другого. Естественно, эта схема является крайне неудобной.

При использовании шифрсистем с открытым ключом возможны два подхода к построению системы цифровой подписи.

Первый подход состоит в преобразовании сообщения в форму, по которой можно восстановить само сообщение и тем самым проверить правильность "подписи". В данном случае подписанное сообщение имеет, как правило, 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.

При втором подходе 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, как правило, этот алгоритм зависит от открытого ключа пользователя. В данном случае длина подписи не зависит от длины подписываемого сообщения.

Одновременно с проблемой цифровой подписи возникла проблема построения бесключевых криптографических *хэш-функций*. Дело в том, что при вычислении цифровой подписи оказывается более удобным осуществить сначала хэширование, то есть свертку текста в некоторую комбинацию фиксированной длины, а затем уже подписывать полученную комбинацию с помощью секретного ключа. При этом функция хэширования, хотя и не зависит от ключа и является откры-

той, должна быть "криптографической". Имеется в виду свойство *односторонности* этой функции: по значению комбинации-свертки никто не должен иметь возможность подобрать соответствующее сообщение.

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

§ 2.2. Управление секретными ключами

Порядок использования криптографической системы определяется системами установки и управления ключами.

Система установки ключей определяет алгоритмы и процедуры генерации, распределения, передачи и проверки ключей.

Система управления ключами определяет порядок использования, смены, хранения и архивирования, резервного копирования и восстановления, замены или изъятия из обращения скомпрометированных, а также уничтожения старых ключей.

Предварительное распределение ключей

Для надежной защиты информации, передаваемой по открытому каналу связи, применяют криптографические средства. Чтобы воспользоваться ими, необходимо осуществить первоначальный выбор и установку ключей. Для генерации ключей могут применяться различные алгоритмы. Выбранные ключи необходимо как-либо передать взаимодействующим сторонам. Поэтому для первоначального распределения ключей необходим защищенный канал связи.

Самый надежный способ первоначального распределения ключей — это личная встреча всех взаимодействующих сторон. Можно использовать также специальных курьеров, которые будут развозить ключи. Однако при большом числе

взаимодействующих сторон требуется предварительная рассылка значительного объема ключевой информации и последующее ее хранение. Поэтому на практике применяют специальные *системы предварительного распределения ключей*, предусматривающие распределение и хранение не самих ключей, а некоторой меньшей по объему исходной информации, на основе которой в дальнейшем каждая сторона может вычислить ключ для взаимодействия с другой стороной. Система предварительного распределения ключей включает два алгоритма. С помощью первого алгоритма осуществляется генерация исходной информации. Эта информация включает открытую часть, которая будет передана всем сторонам или помещена на общедоступном сервере, а также секретные части каждой стороны. Второй алгоритм предназначен для вычисления действующего значения ключа для взаимодействия между абонентами по имеющейся у них секретной и общей открытой части исходной ключевой информации.

Система предварительного распределения ключей должна быть *устойчивой*, то есть учитывать возможность раскрытия части ключей при компрометации, обмане или сговоре абонентов, и *гибкой* — допускать возможность быстрого восстановления путем исключения скомпрометированных и подключения новых абонентов.

Пересылка ключей

После того как предварительное распределение ключей произведено, может потребоваться передача ключей для каждого конкретного сеанса взаимодействия. Передача этих ключей может осуществляться с помощью шифрования с использованием ранее полученных ключей.

Для передачи зашифрованных ключей по открытому каналу связи между не доверяющими друг другу абонентами требуется решение всего комплекса задач по установлению подлинности различных аспектов взаимодействия, начиная от подлинности субъектов взаимодействия, подлинности пере-

даваемых сообщений, подлинности самого сеанса связи и кончая подтверждением правильности (идентичности) полученных абонентами ключей.

Для централизованного управления пересылкой ключей создаются специальные доверенные центры, выполняющие функции центров распределения или перешифрования ключей. Различие между этими центрами заключается в том, что в первом случае генерация ключей осуществляется в центре распределения, а во втором случае — самими абонентами.

Открытое распределение ключей

Наиболее просто распределение ключей осуществляется в *системах открытого распределения (секретных) ключей.* Для сетей связи с большим числом абонентов традиционные подходы к построению системы распределения ключей оказываются очень неудобными. Диффи и Хеллман впервые показали, как можно решить эту задачу, используя незащищенный канал связи.

В предложенной ими системе открытого распределения ключей [Диф79] каждая из сторон изначально имеет свой секретный параметр. Стороны реализуют определенный протокол взаимодействия по открытому каналу связи. При этом они обмениваются некоторыми сообщениями (образованными с помощью своих секретных параметров) и по результатам этого обмена вычисляют общий секретный связной ключ. В более поздних работах такие протоколы стали называть *протоколами выработки общего ключа*, поскольку изначально ни одна из сторон не имеет ключа и как такового распределения или пересылки ключей в нем не происходит.

В исходном виде система Диффи и Хеллмана имела существенные недостатки, связанные с возможностью для третьей стороны по осуществлению активного вхождения в канал связи и проведению полного контроля передаваемой информации. Однако после небольших модификаций и дополнений их протокол уже позволяет осуществлять не только

выработку общего ключа, но и одновременно проверять и подтверждать правильность вычислений, а также проводить взаимную аутентификацию взаимодействующих сторон.

Схема разделения секрета

Еще одной задачей современной криптографии, тесно связанной с проблемой распределения ключей и активно развивающейся в последние годы, является задача построения *схем разделения секрета*. Для многих практически важных приложений, связанных с запуском или активизацией критических процессов или определяющих порядок получения доступа к значимым данным, ответственное лицо должно ввести секретный ключ. Чтобы обезопасить процедуру принятия решения и не отдавать все на волю одного человека, являющегося обладателем ключа, используют метод разделения секрета. Он состоит в назначении определенной группы лиц, которая имеет право принимать решение. Каждый член группы владеет определенной долей секрета (точнее, специально выбранным набором данных), полная совокупность которых позволяет восстановить секретный ключ. При этом схема разделения секрета выбирается с таким условием, что для восстановления секретного ключа требуется обязательное присутствие всех членов группы, так как в случае отсутствия хотя бы одного из участников объединение долей оставшихся членов группы гарантированно не позволяет получить никакой информации о секретном ключе. Таким образом, *схема разделения секрета* определяется двумя алгоритмами, удовлетворяющими сформулированному выше условию: первый алгоритм определяет порядок вычисления значений долей по заданному значению секретного ключа, а второй предназначен для восстановления значения секрета по известным долям.

Задачу построения схемы разделения секрета можно обобщить

— либо путем введения так называемой *структуры доступа,* когда решение может приниматься не одной, а несколькими различными группами, причем часть из участников может наделяться правом "вето",

— либо путем добавления механизмов, позволяющих обнаружить обман или сговор участников,

— либо введением специального протокола распределения долей между участниками с подтверждением правильности полученной информации и аутентификацией сторон.

§ 2.3. Инфраструктура открытых ключей

Сертификаты

Создание цифровой подписи позволило решить проблему *сертификации открытых ключей.* Она заключается в том, что перед тем как использовать открытый ключ некоторого абонента для отправки ему конфиденциального сообщения, отправитель должен быть уверен, что открытый ключ действительно принадлежит этому абоненту. Открытые ключи необходимо очень тщательно обезопасить, в том смысле, что если сервер, на котором они хранятся, не обеспечивает их целостность и аутентичность, то злоумышленник имеет возможность, подменив открытый ключ одного из абонентов, выступать от его имени. Поэтому для защиты открытых ключей создаются специальные *центры сертификации,* которые играют роль доверенной третьей стороны и заверяют открытые ключи каждого из абонентов своими цифровыми подписями.

Сертификат представляет собой набор данных, заверенный цифровой подписью центра и включающий открытый ключ и список дополнительных атрибутов, принадлежащих абоненту. К таким атрибутам относятся: имена пользователя и центра сертификации, номер сертификата, время действия сертификата, предназначение открытого ключа (цифровая подпись, шифрование) и т. д.

Международный стандарт ISO X.509 определяет общую структуру сертификатов открытых ключей и протоколы их использования для аутентификации в распределенных системах.

Центры сертификации

Центр сертификации предназначен для регистрации абонентов, изготовления сертификатов открытых ключей, хранения изготовленных сертификатов, поддержания в актуальном состоянии справочника действующих сертификатов и выпуска списка досрочно отозванных сертификатов.

Для сетей с большим числом абонентов создается несколько центров сертификации. Центры сертификации объединяются в древовидную структуру, в корне которой находится главный центр сертификации, который выдает сертификаты подчиненным ему отраслевым центрам, тем самым обеспечивая доверие к открытым ключам этих центров. Каждый центр вышестоящего уровня аналогичным образом делегирует право выпуска сертификатов подчиненным ему центрам. В результате доверие сертификату открытого ключа каждого центра основано на заверении его сертификата ключом вышестоящего центра. Сертификаты главного центра подписывает сам главный центр.

Зная иерархию и подчиненность друг другу центров сертификации, можно всегда точно установить, является ли абонент владельцем данного открытого ключа.

Основная трудность при создании центров сертификации заключается в их юридическом статусе и потенциальных финансовых возможностях по выплате компенсаций за ущерб, понесенный в результате невыполнения подписанных цифровыми подписями с использованием сертификатов, выданных этим центром, договоров и контрактов, сорванных по причине отказов от цифровых подписей или их подделки.