16. Обобщенная модель электронной цифровой подписи

Схему, изложенную в разделе 5 для асимметричных систем с открытым ключом, можно также использовать для цифровой подписи сообщений, которую невозможно подделать за полиномиальное время.

Пусть пользователю А необходимо подписать сообщение x. Он, зная секрет K, находит такое y, что F_K (y) = x, и вместе с сообщением x посылает y пользователю в качестве своей цифровой подписи. Пользователь В хранит y в качестве доказательства того, что А подписал сообщение x.

Сообщение, подписанное цифровой подписью, можно представлять себе, как пару (x, y), где x —сообщение, y — решение уравнения F_K (y) = x, F_K: X $\rightarrow$ Y — функция с секретом, известная всем взаимодействующим абонентам.

Из определения функции F_K очевидны следующие достоинства цифровой подписи:

1. подписать сообщение x, т.е. решить уравнение F_K (y) = =x, может только абонент — обладатель данного секрета K; другими словами, подделать подпись невозможно;
2. проверить подлинность подписи может любой абонент, знающий открытый ключ, т.е. саму функцию F_K;
3. при возникновении споров отказаться от подписи невозможно в силу ее неподделываемости;
4. подписанные сообщения (x, y) можно, не опасаясь ущерба, пересылать по любым каналам связи.

Важным преимуществом асимметричных методов является возможность идентификации отправителя путем использования его электронной подписи. Идея технологии электронной подписи состоит в следующем. Отправитель передает два экземпляра одного сообщения: открытое и расшифрованное его закрытым ключом (т.е. обратно шифрованное). Получатель шифрует с помощью открытого ключа отправителя расшифрованный экземпляр. Если он совпадет с открытым вариантом, то личность и подпись отправителя считается установленной.

Формально выражаясь, асимметричный метод обеспечивает реализацию электронной подписи при выполнении следующего тождества:

E(D(T)) = D(E(T)) = T.

При практической реализации электронной подписи также шифруется не все сообщение, а лишь специальная контрольная сумма — хэш (hash total), защищающая послание от нелегального изменения. Важно, что электронная подпись здесь как гарантирует целостность сообщения, так и удостоверяет личность отправителя.

Вопросы реализации электронной подписи и вычисления ее хэша определены в отечественных стандартах "Информационная технология. Криптографическая защита информации", а именно: ГОСТ 34.10-94 "Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма" и ГОСТ 34.11-94 "Функция хэширования".

Контроль целостности

Криптографические методы позволяют надежно контролировать целостность как отдельных порций данных, так и их наборов (таких, как поток сообщений); определять подлинность источника данных; гарантировать невозможность отказаться от совершенных действий ("неотказуемость").

В основе криптографического контроля целостности лежат два понятия:

- хэш-функция;
- электронная цифровая подпись (ЭЦП).

Хэш-функция — это труднообратимое преобразование данных (односторонняя функция), реализуемое, как правило, средствами симметричного шифрования со связыванием блоков. Результат шифрования последнего блока (зависящий от всех предыдущих) и служит результатом хэш-функции.

Пусть имеются данные, целостность которых нужно проверить, хэш-функция и ранее вычисленный результат ее применения к исходным данным (так называемый дайджест). Обозначим хэш-функцию через h, исходные данные — через T, проверяемые данные — через T. Контроль целостности данных сводится к проверке равенства h(T') = h(T).

Если оно выполнено, считается, что T' = T. Совпадение дайджестов для различных данных называется коллизией. В принципе, коллизии, конечно, возможны, поскольку мощность множества дайджестов меньше, чем мощность множества хэшируемых данных, однако то, что h есть функция односторонняя, означает, что за приемлемое время специально организовать коллизию невозможно.

Рассмотрим теперь применение асимметричного шифрования для выработки и проверки электронной цифровой подписи. Пусть E(T) обозначает результат зашифрования текста T с помощью открытого ключа, а D(T) — результат расшифрования текста T (как правило, шифрованного) с помощью секретного ключа.

Чтобы асимметричный метод мог применяться для реализации ЭЦП, необходимо выполнение тождества «(/ ; » : E(D(T)) = D(E(T))=T \„ T .

На рис. 11.1 показана процедура выработки электронной цифровой подписи, состоящая в шифровании преобразованием D дайджеста h(T).

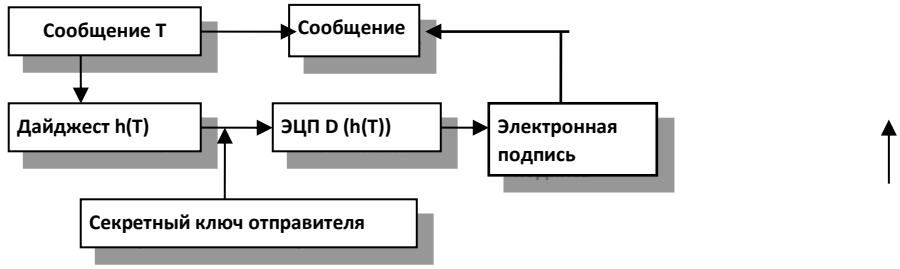

Рис.11.1. Схема процедуры выработки электронной цифровой подписи

Проверка ЭЦП может быть реализована так, как показано на рис.11.2.

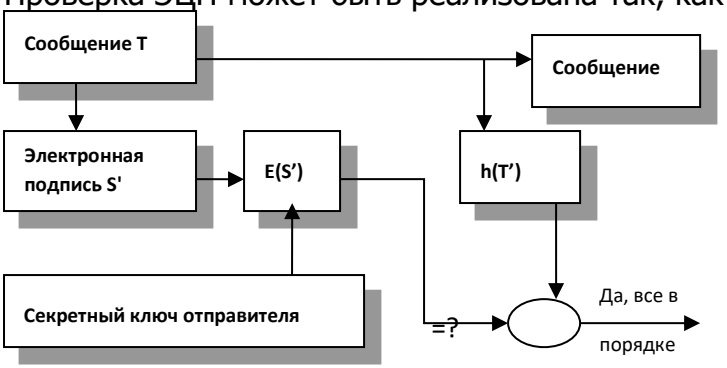

Рис. 11.2. Схема процедуры проверки электронной цифровой подписи

Из равенства E(S') = h(T') I следует, что S' = D(h(T) (для доказательства достаточно применить к обеим частям преобразование D и вычеркнуть в левой части тождественное преобразование D(E())). Таким образом, электронная цифровая подпись защищает целостность сообщения и удостоверяет личность отправителя, то есть защищает целостность источника данных и служит основой неотказуемости.

Два российских стандарта: ГОСТ Р 34.10-94 "Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма" и ГОСТ.Р 34.11-94 "Функция хэширования", объединенные общим заголовком "Информационная технология.

Криптографическая защита информации", регламентируют вычисление дайджеста и реализацию ЭЦП. В сентябре 2001 года был утвержден, а 1 июля 2002 года вступил в силу новый стандарт ЭЦП — ГОСТ Р 34.10-2001, разработанный специалистами ФАПСИ.

Для контроля целостности последовательности сообщений (то есть для защиты от кражи, дублирования и переупорядочения сообщений) применяют временные штампы и

нумерацию элементов последовательности, при этом штампы и номера включают в подписываемый текст.

Цифровые сертификаты

При использовании асимметричных методов шифрования (и, в частности, электронной цифровой подписи) необходимо иметь гарантию подлинности пары (имя пользователя, открытый ключ пользователя). Для решения этой задачи в спецификациях X.509 вводятся понятия цифрового сертификата и удостоверяющего центра.

Удостоверяющий центр — это компонент глобальной службы каталогов, отвечающий за управление криптографическими ключами пользователей. Открытые ключи и другая информация о пользователях хранятся удостоверяющими центрами в виде цифровых сертификатов, **имеющих следующую структуру:**

- порядковый номер сертификата;
- идентификатор алгоритма электронной подписи;
- имя удостоверяющего центра;
- срок годности;
- имя владельца сертификата (имя пользователя, которому принадлежит сертификат);
- открытые ключи владельца сертификата (ключей может быть несколько);
- идентификаторы алгоритмов, ассоциированных с открытыми ключами владельца сертификата;
- электронную подпись, сгенерированную с использованием секретного ключа удостоверяющего центра (подписывается результат хэширования всей информации, хранящейся в сертификате).

Цифровые сертификаты обладают следующими свойствами:

- любой пользователь, знающий открытый ключ удостоверяющего центра, может узнать открытые ключи других клиентов центра и проверить целостность сертификата;
- никто, кроме удостоверяющего центра, не может модифицировать информацию о пользователе без нарушения целостности сертификата.

В спецификациях X.509 не описывается конкретная процедура генерации криптографических ключей и управления ими, однако даются некоторые общие рекомендации. **В частности, оговаривается, что пары ключей могут порождаться любым из следующих способов:**

- ключи может генерировать сам пользователь; в таком случае секретный ключ не попадает в руки третьих лиц, однако нужно решать задачу безопасной связи с удостоверяющим центром;
- ключи генерирует доверенное лицо; здесь приходится решать задачи безопасной доставки секретного ключа владельцу и предоставления доверенных данных для создания сертификата;
- ключи генерируются удостоверяющим центром, в данном случае остается только задача безопасной передачи ключей владельцу.

Цифровые сертификаты в формате X.509 версии 3 стали не только формальным, но и фактическим стандартом, поддерживаемым многочисленными удостоверяющими центрами.

Следует отметить, что криптографические методы используются также для контроля целостности информации и программ. Для этого применяется шифрованная контрольная сумма исходного текста (имитоприставка), вычисленная с применением секретного ключа.

В отличие от традиционной контрольной суммы (используемой для защиты от программно-аппаратных сбоев и ошибок) имитоприставка обеспечивает практически абсолютную защиту как от непреднамеренной, так и преднамеренной модификации данных или программы.

Основные типы криптоаналитических атак

> Нет невзламываемых шифров. Все системы шифрования просто делают взламывание шифровок или заведомо дороже содержащейся в сообщении информации, или затягивают время расшифрования на неприемлемо большой срок.
>
> **В.Жельников**

Фундаментальное правило криптоанализа, впервые сформулированное голландцем А.Керкхоффом еще в XIX в., заключается в том, что стойкость шифра (криптосистемы) должна определяться только секретностью ключа. Иными словами, правило Керкхоффа состоит в том, что весь алгоритм шифрования, кроме значения секретного ключа, известен криптоаналитику противника.

Это обусловлено тем, что криптосистема, реализующая семейство криптографических преобразований, обычно рассматривается как открытая система. Такой подход отражает очень важный принцип технологии защиты информации: защищенность системы не должна зависеть от секретности чего-либо такого, что невозможно быстро изменить в случае утечки секретной информации.

Обычно криптосистема представляет собой совокупность аппаратных и программных средств, которую можно изменить только при значительных затратах времени и средств, тогда как ключ является легко изменяемым объектом. Именно поэтому стойкость криптосистемы определяется только секретностью ключа.

Другое почти общепринятое допущение состоит в том, что криптоаналитик имеет в своем распоряжении шифр тексты сообщений.

Существует четыре основных типа криптоаналитических атак. Конечно, все они формулируются в предположении, что криптоаналитику известен применяемый алгоритм шифрования и шифртексты сообщений:

1. **Криптоаналитическая атака при наличии только известного шифртекста**

   Криптоаналитик имеет только шифр тексты C_1, C_2, …, C_i нескольких сообщений, причем все они зашифрованы с использованием одного и того же алгоритма шифрования E_k.

   Работа криптоаналитика заключается в том, чтобы раскрыть исходные тексты M_1, M_2, …, M_i по возможности большинства сообщений или, еще лучше, вычислить ключ K, использованный для шифрования этих сообщений, с тем чтобы расшифровать и другие сообщения, зашифрованные этим шифром.

   Этот вариант соответствует модели внешнего нарушителя, который имеет физический доступ к линии связи, но не имеет доступа к аппаратуре шифрования и дешифрования.

2. **Криптоаналитическая атака при наличии известного открытого текста**

   Криптоаналитик имеет доступ не только к шифртекстам C_1, C_2, …, C_i и нескольких сообщений, но также к открытым текстам M_1, M_2, …, M_i этих сообщений.

   Его работа заключается в нахождении ключа K, используемого при шифровании этих сообщений, или алгоритма расшифрования D_k любых новых сообщений, зашифрованных тем же ключом, причем все они зашифрованы с использованием одного и того же алгоритма шифрования.

   Возможность проведения такой атаки складывается при шифровании стандартных документов, подготавливаемых по стандартным формам, когда определенные болки данных повторяются и известны.

   Он также применим при использовании режима глобального шифрования, когда вся информация на встроенном магнитном носителе записывается в виде шифртекста, включая главную корневую запись, загрузочный сектор, системные программы и пр.

   При хищении этого носителя (или компьютера) легко установить, какая часть криптограммы соответствует системной информации, и получить большой объем известного исходного текста для выполнения криптоанализа.

3. **Криптоаналитическая атака при возможности выбора открытого текста**

Криптоаналитик не только имеет доступ к шифртекстам C_1, C_2, …, C_i и связанным с ними открытым текстам M_1, M_2, …, M_i этих сообщений, но и может по желанию выбирать открытые тексты, которые затем получает в зашифрованном виде.

Такой криптоанализ получается более мощным по сравнению с криптоанализом с известным открытым текстом, потому что криптоаналитик может выбрать для шифрования такие блоки открытого текста, которые дадут больше информации о ключе. Работа криптоаналитика состоит в поиске ключа K, использованного для шифрования сообщений, или алгоритма рашифрования D_k новых сообщений, зашифрованных тем же ключом.

Этот вариант атаки соответствует модели внутреннего нарушителя. На практике такая ситуация может возникнуть при вовлечении в криптоатаку лиц, которые не знают секретного ключа, но в силу своих служебных полномочий имеют возможность использовать шифрование для передачи своих сообщений.

4. **Криптоаналитическая атака с адаптивным выбором открытого текста**

Это особый вариант атаки с выбором открытого текста. Криптоаналитик может не только выбирать открытый текст, который затем шифруется, но и изменять свой выбор в зависимости от результатов предыдущего шифрования.

При криптоанализе с простым выбором открытого текста криптоаналитик обычно может выбирать несколько крупных блоков открытого текста для их шифрования; при криптоанализе с адаптивным выбором открытого текста он имеет возможность выбрать сначала более мелкий пробный блок открытого текста, затем выбрать следующий блок в зависимости от результатов первого выбора и т.д.

Эта атака предоставляет криптоаналитику еще больше возможностей, чем предыдущие типы атак.

5. **Криптоаналитическая атака с использованием выбранного шифртекста**

Криптоаналитик может выбирать для расшифрования различные шифртексты и имеет доступ к расшифрованным открытым текстам. Например, криптоаналитик получил доступ к защищенному от несанкционированного вскрытия блоку, который выполняет автоматическое расшифрование.

Работа криптоаналитика заключается в нахождении ключа. Этот тип криптоанализа представляет особый интерес для раскрытия алгоритмов с открытым ключом.

6. **Криптоаналитическая атака методом полного перебора всех возможных ключей**

Эта атака предполагает использование криптоаналитиком известного шифр текста и осуществляется посредством полного перебора всех возможных ключей с проверкой, является ли осмысленным получающийся открытый текст. Такой подход требует привлечения предельных вычислительных ресурсов и иногда называется силовой атакой.

Существуют и другие, менее распространенные виды криптоаналитических атак.

Итак, разумеется, отразить в нескольких лекциях все вопросы и проблемы современной криптологии задача невыполнимая. Объем знаний в этой области чрезвычайно велик и продолжает интенсивно увеличиваться.

Кроме того, для полноценного освоения всех вопросов криптологии требуется весьма солидная университетская математическая подготовка.

Важно подчеркнуть, что шифрование информации, с одной стороны, требует определенных затрат на его выполнение, а с другой — не гарантирует 100—процентной надежности защиты от злоумышленника.

Поэтому всегда надо четко оценивать необходимость применения это способа защиты информации в конкретных ситуациях.