**Глава 2**

ПРЕДИСЛОВИЕ

Разные люди понимают под **КРИПТОГРАФИЕЙ** разные вещи. Дети играют в игрушечные шифры и секретные языки. Это, однако, не имеет ничего общего с настоящей криптографией. Настоящая криптография (*strong cryptography*) должна обеспечивать такой уровень секретности, чтобы можно было надежно защитить критическую информацию от расшифровки крупными организациями, такими как мафия, транснациональные корпорации и крупные государства. Настоящая криптография в прошлом использовалась лишь в военных целях. Сейчас, с становлением информационного общества, она становится центральным инструментом для обеспечения конфиденциальности.

По мере образования информационного общества, крупным государствам становятся доступны технологические средства тотального надзора за миллионами людей. Поэтому криптография становится одним из основных инструментов обеспечивающих конфиденциальность, доверие, авторизацию, электронные платежи, корпоративную безопасность и бесчисленное множество других важных вещей.

БАЗОВАЯ ТЕРМИНОЛОГИЯ

Представьте, что вам надо отправить сообщение адресату. Вы хотите, чтобы никто кроме адресата не смог прочитать отправленную информацию. Однако всегда есть вероятность, что кто-либо вскроет конверт или перехватит электронное послание.

В криптографической терминологии исходное послание именуют открытым текстом (**plaintext или cleartext**). Изменение исходного текста так, чтобы скрыть от прочих его содержание, называют шифрованием (**encryption**). Зашифрованное сообщение называют шифротекстом (**ciphertext**). Процесс, при котором из шифротекста извлекается открытый текст, называют дешифровкой (**decryption**). Обычно в процессе шифровки и дешифровки используется некий ключ (**key**) и алгоритм обеспечивает, что дешифрование можно сделать лишь зная этот ключ.

*Криптография* - это наука о том, как обеспечить секретность сообщения. *Криптоанализ* - это наука о том, как вскрыть шифрованное сообщение, то есть, как извлечь открытый текст не зная ключа. Криптографией занимаются криптографы, а криптоанализом занимаются криптоаналитики.

Метод шифровки/дешифровки называют шифром (**cipher**). Все современные алгоритмы используют ключ для управления шифровкой и дешифровкой.

ОСНОВНЫЕ АЛГОРИТМЫ ШИФРОВАНИЯ

Алгоритмы с использованием ключа делятся на два класса: *симметричные* (или алгоритмы секретным ключом) и *ассиметричные* (или алгоритмы с открытым ключом). Разница в том, что симметричные алгоритмы используют один и тот же ключ для шифрования и для дешифрования (или же ключ для дешифровки просто вычисляется по ключу шифровки). В то время как асимметричные алгоритмы используют разные ключи, и ключ для дешифровки не может быть вычислен по ключу шифровки.

*Симметричные* алгоритмы подразделяют на потоковые шифры и блочные шифры. Потоковые позволяют шифровать информацию побитово, в то время как блочные работают с некоторым набором бит данных (обычно размер блока составляет 64 бита) и шифруют этот набор как единое целое.

*Ассиметричные* шифры (также именуемые алгоритмами с открытым ключом) допускают, чтобы открытый ключ был доступен всем (скажем, опубликован в газете). Это позволяет любому зашифровать сообщение. Однако расшифровать это сообщение сможет только нужный человек (тот, кто владеет ключом дешифровки). Ключ для шифрования называют открытым ключом, а ключ для дешифрования называют закрытым ключом или секретным ключом. Таким образом, мы с вами можем понять, что симметричные алгоритмы работают быстрее, чем ассиметричные.

Многие качественные криптографические алгоритмы доступны в книжном магазине, библиотеке или в Интернете. К широко известным симметричным алгоритмам относятся DES и IDEA. Самым лучшим асимметричным алгоритмом является RSA.

ЦИФРОВЫЕ ПОДПИСИ

Некоторые из асимметричных алгоритмов могут использоваться для генерирования **цифровой подписи**. Цифровой подписью называют блок данных, сгенерированный с использованием некоторого секретного ключа. При этом с помощью открытого ключа можно проверить, что данные были действительно сгенерированы с помощью этого секретного ключа. Алгоритм генерации цифровой подписи должен обеспечивать, чтобы было невозможно без секретного ключа создать подпись, которая при проверке окажется правильной.

Цифровые подписи используются для того, чтобы подтвердить, что сообщение пришло действительно от данного пользователя. Цифровые подписи также можно использовать для удостоверения (сертификации) того, что документ принадлежит определенному лицу. Это делается так: открытый ключ и информация о том, кому он принадлежит, подписываются стороной, которой доверяем. При этом доверять подписывающей стороне мы можем на основании того, что ее ключ был подписан третьей стороной. Таким образом, возникает иерархия доверия. Очевидно, что некоторый ключ должен быть корнем иерархии (то есть ему мы доверяем не потому, что он кем-то подписан, а потому, что мы верим, что ему можно доверять). В централизованной инфраструктуре ключей имеется очень небольшое количество корневых ключей сети (например, облеченные полномочиями государственные агентства, их также называют сертификационными агентствами - certification authorities). В распределенной инфраструктуре нет необходимости иметь универсальные для всех корневые ключи, и каждая из сторон может доверять своему набору корневых ключей (скажем своему собственному ключу и ключам, ею подписанным). Эта концепция носит название сети доверия (web of trust) и реализована, например, в PGP.

Цифровая подпись документа обычно создается так: из документа генерируется так называемый дайджест (message digest) и к нему добавляется информация о том, кто подписывает документ, штамп времени и прочее. Получившаяся строка далее зашифровывается секретным ключом подписывающего с использованием того или иного алгоритма. Получившийся зашифрованный набор бит и представляет собой подпись. К подписи обычно прикладывается открытый ключ подписывающего. Получатель сначала решает для себя доверяет ли он тому, что открытый ключ принадлежит именно тому, кому должен принадлежать (с помощью сети доверия или априорного знания), и затем дешифрует подпись с помощью открытого ключа. Если подпись нормально дешифровалась, и ее содержимое соответствует документу (дайджест и др.), то сообщение считается подтвержденным.

Свободно доступны несколько методов создания и проверки цифровых подписей. Наиболее известным является алгоритм RSA.

ОБЕСПЕЧИВАЕМАЯ ШИФРОМ СТЕПЕНЬ ЗАЩИТЫ

Хорошие криптографические системы создаются таким образом, чтобы сделать их вскрытие как можно более трудным делом. Можно построить системы, которые на практике невозможно вскрыть. При этом не требуется очень больших усилий для реализации. Единственное, что требуется - это аккуратность и базовые знания. Нет прощения разработчику, если он оставил возможность для вскрытия системы.

Теоретически, любой шифровальный алгоритм с использованием ключа может быть вскрыт методом перебора всех значений ключа. Если ключ подбирается методом грубой силы (brute force), требуемая мощность компьютера растет экспоненциально с увеличением длины ключа. Ключ длиной в 32 бита требует 232 (около 109) шагов. Такая задача под силу любому дилетанту и решается на домашнем компьютере. Системы с 40-битным ключом требуют 240 шагов - такие компьютерные мощности имеются в большинстве университетов и даже в небольших компаниях. Системы с 56-битными ключами (DES) требуют для вскрытия заметных усилий, однако могут быть легко вскрыты с помощью специальной аппаратуры. Стоимость такой аппаратуры значительна, но доступна для мафии, крупных компаний и правительств. Ключи длиной 64 бита в настоящий момент, возможно, могут быть вскрыты крупными государствами и уже в ближайшие несколько лет будут доступны для вскрытия преступными организациями, крупными компаниями и небольшими государствами. Ключи длиной 80 бит могут в будущем стать уязвимыми. Ключи длиной 128 бит, вероятно, останутся недоступными для вскрытия методом грубой силы в обозримом будущем. Можно использовать и более длинные ключи. В пределе нетрудно добиться того, чтобы энергия, требуемая для вскрытия, превзойдет массу солнца.

Однако, длина ключа - это еще не все. Многие шифры можно вскрыть, не перебирая всех возможных комбинаций. Вообще говоря, очень трудно придумать шифр, который нельзя было бы вскрыть другим более эффективным способом. Разработка собственных шифров может стать приятным занятием, но для реальных приложений использовать самодельные шифры не рекомендуется, если вы не являетесь экспертом и не уверены на 100 процентов в том, что делаете.

В общем, следует держаться в стороне от неопубликованных или секретных алгоритмов. Часто разработчик такого алгоритма не уверен в его надежности, или же надежность зависит от секретности самого алгоритма. Вообще говоря, ни один алгоритм, секретность которого зависит от секретности самого алгоритма, не является надежным. В частности, имея шифрующую программу, можно нанять программиста, который восстановит алгоритм методом обратной инженерии. Опыт показывает, что большинство секретных алгоритмов, ставших впоследствии достоянием общественности, оказались ненадежными.

Длины ключей, используемых в криптографии с открытым ключом обычно значительно больше, чем в симметричных алгоритмах. Здесь проблема заключается не в подборе ключа, а в воссоздании секретного ключа по открытому. В случае RSA проблема эквивалентна разложению на множители большого целого числа, которое является произведением пары неизвестных простых чисел. В случае некоторых других криптосистем, проблема эквивалентна вычислению дискретного логарифма по модулю большого целого числа (такая задача считается примерно аналогичной по трудности задаче разложения на множители). Имеются криптосистемы, которые используют другие проблемы.

Важно подчеркнуть, что *степень надежности криптографической системы определяется ее слабейшим звеном*. Нельзя упускать из вида ни одного аспекта разработки системы - от выбора алгоритма до политики использования и распространения ключей.