Криптография с открытым ключом: от теории к стандарту

А.Н.Терехов, А.В.Тискин
"Программирование РАН", N 5 (сентябрь-октябрь), 1994, стр. 17--22

Введение

На протяжении многих веков человечество использовало криптографические методы для защиты информации при ее передаче и хранении. Приблизительно к концу XIX в. эти методы стали объектом математического изучения. Отрасль математики, изучающая защиту информации, традиционно называется криптологией [cryptology] и подразделяется на криптографию [cryptography], занимающуюся разработкой новых методов и обоснованием их корректности, и криптоанализ [cryptanalysis], задача которого - интенсивное изучение существующих методов, часто с целью реального раскрытия секретов другой стороны. Криптография и криптоанализ находятся в тесном взаимодействии друг с другом и с практическими нуждами и развиваются параллельно закрытыми правительственными организациями многих государств и международным научным сообществом.

В настоящее время существуют тысячи криптографических систем, реализованных как программно, так и аппаратно. Среди них можно выделить системы, сам криптографический принцип работы которых держится в секрете, как, например, микросхема Clipper, предлагаемая правительством США в качестве криптографического стандарта для телекоммуникаций, и системы, алгоритм которых открыт, а секретной является только определенная, как правило небольшая, порция информации, называемая (секретным) ключом [(secret) key] - к ним относится большинство систем, реализуемых программно и предназначенных для широкого использования. В дальнейшем мы будем рассматривать только системы второго типа.

В системе рассматриваемого типа задача вскрытия системы, то есть нарушения защиты информации без предварительного знания ключа, как правило, теоретически разрешима при наличии у вскрывающей стороны неограниченных вычислительных ресурсов. С математической точки зрения надежность криптографической системы определяется сложностью решения этой задачи с учетом реальных вычислительных ресурсов потенциальной вскрывающей стороны. С организационной точки зрения имеет значение соотношение стоимости потенциального вскрытия и ценности защищаемой информации.

Математическое исследование надежности криптографических систем затруднено отсутствием универсального математического понятия сложности. По этой причине надежность большинства криптографических систем в настоящее время невозможно не только доказать, но даже адекватно сформулировать. Как правило, применение той или иной криптографической системы основано на результатах многолетнего практического криптоанализа систем данного типа, в той или иной степени подкрепленных математическим обоснованием. Это обоснование может сводить задачу раскрытия данной криптосистемы к какой-либо задаче теории чисел или комбинаторики, решение которой считается реально не осуществимым, или, что предпочтительнее, к классу NP-полных задач, сводимость к которому является “эталоном” практической неразрешимости. В то же время, понятие практической неразрешимости для конкретных практических задач не является четко определенным или стабильным, благодаря развитию вычислительной техники и методов криптоанализа.

Криптография с симметричным ключом

Долгое время традиционной криптографической схемой была схема с симметричным ключом [symmetric key, dual key]. В этой схеме имеется один ключ, который участвует в шифровании и дешифровании информации. Шифрующая процедура при помощи ключа производит ряд действий над исходными данными, дешифрующая процедура при помощи того же ключа производит обратные действия над кодом. Дешифрование кода без ключа предполагается практически неосуществимым. Если зашифрованная таким образом информация передается по обычному, т.е. незащищенному, каналу связи, один и тот же ключ должен иметься у отправителя и получателя, вследствие чего возникает необходимость в дополнительном защищенном канале для передачи ключа, повышается уязвимость системы и увеличиваются организационные трудности.

К классу алгоритмов с симметричным ключом относится метод “одноразового блокнота” [one-time pad], заключающийся в побитовом сложении (“гаммировании”) шифруемого текста со случайной последовательностью битов - ключом (см. [S94]). Длина ключа должна совпадать с длиной шифруемого текста и каждый отрезок ключа должен использоваться однократно; в противном случае текст легко поддается несанкционированной расшифровке. При выполнении же этих условий данный метод является единственным методом, теоретически устойчивым против криптоанализа противника с неограниченными вычислительными ресурсами. Несмотря на это, в настоящее время метод “одноразового блокнота” практически не применяется из-за организационных сложностей, связанных с генерацией, передачей и хранением используемых в нем сверхдлинных ключей.

Другим примером схемы с симметричным ключом может служить алгоритм DES (Data Encryption Standard), принятый 23 ноября 1976 г. в качестве официального криптографического стандарта США для защиты некритичной [unclassified] информации (см. [S94], с.219-243). В стандарт было включено положение об обязательной ресертификации (пересмотре) алгоритма каждые пять лет; последняя такая ресертификация состоялась в 1992 г. По мнению экспертов, в связи с определенными успехами в криптоанализе DES и появлением новых методов шифрования с симметричным ключом, алгоритм может не быть ресертифицирован на следующий пятилетний срок. Тем не менее, DES по-прежнему считается криптографически стойким алгоритмом и остается самой распространенной схемой шифрования с симметричным ключом.

Российский стандарт на криптографию с симметричным ключом определен ГОСТ 28147-89 “Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования”, который был введен в действие 1 июля 1990 г. В отличие от DES, стандарт содержит указание на то, что он “по своим возможностям не накладывает ограничений на степень секретности защищаемой информации”. В общих чертах алгоритм ГОСТ 28147 аналогичен DES, но имеется ряд существенных отличий, как, например, длина ключа и трактовка содержимого узлов замены [в схеме DES называемых “S-boxes”]. В то время, как заполнение узлов замены DES оптимизировано с точки зрения криптографической стойкости и явно указано в стандарте, заполнение узлов замены ГОСТ 28147 “является секретным элементом и поставляется в установленном порядке”. Учитывая, что оно в то же время “является долговременным ключевым элементом, общим для сети ЭВМ”, и что “установленный порядок” поставки может не предусматривать криптографическую оптимизацию, этот пункт стандарта представляется одним из его слабых мест, затрудняющим реализацию и не способствующим криптографической стойкости. Однако при задании оптимизированных значений для узлов замены криптографическая стойкость алгоритма сравнима со стойкостью DES.

Криптография с открытым ключом

В 1976 г. У.Диффи и М.Хеллманом [DH76] был предложен новый тип криптографической системы - система с открытым ключом [public key cryptosystem]. В схеме с открытым ключом имеется два ключа, открытый [public] и секретный [private, secret], выбранные таким образом, что их последовательное применение к массиву данных оставляет этот массив без изменений. Шифрующая процедура использует открытый ключ, дешифрующая - секретный. Дешифрование кода без знания секретного ключа практически неосуществимо; в частности, практически неразрешима задача вычисления секретного ключа по известному открытому ключу. Основное преимущество криптографии с открытым ключом - упрощенный механизм обмена ключами. При осуществлении коммуникации по каналу связи передается только открытый ключ, что делает возможным использование для этой цели обычного канала и устраняет потребность в специальном защищенном канале для передачи ключа.

С появлением систем с открытым ключом понятие о защите информации, а вместе с ним функции криптографии значительно расширились. Если раньше основной задачей криптографических систем считалось надежное шифрование информации, в настоящее время область применения криптографии включает также цифровую подпись (аутентификацию), лицензирование, нотаризацию (свидетельствование), распределенное управление, схемы голосования, электронные деньги и многое другое (см. [BFS91], ч.7, [S94], ч.1). Наиболее распространенные функции криптографических систем с открытым ключом - шифрование и цифровая подпись, причем роль цифровой подписи в последнее время возросла по сравнению с традиционным шифрованием: некоторые из систем с открытым ключом поддерживают цифровую подпись, но не поддерживают шифрование.

Цифровая подпись используется для аутентификации текстов, передаваемых по телекоммуникационным каналам. Она аналогична обычной рукописной подписи и обладает ее основными свойствами: удостоверяет, что подписанный текст исходит именно от лица, поставившего подпись, и не дает самому этому лицу возможности отказаться от обязательств, связанных с подписанным текстом. Цифровая подпись представляет собой небольшое количество дополнительной информации, передаваемой вместе с подписываемым текстом. В отличие от шифрования, при формировании подписи используется секретный ключ, а при проверке - открытый.

Из-за особенностей алгоритмов, лежащих в основе систем с открытым ключом, их быстродействие при обработке единичного блока информации обычно в десятки раз меньше, чем быстродействие систем с симметричным ключом на блоке той же длины. Для повышения эффективности систем с открытым ключом часто применяются смешанные методы, реализующие криптографические алгоритмы обоих типов. При шифровании информации выбирается случайный симметричный ключ, вызывается алгоритм с симметричным ключом для шифрования исходного текста. а затем алгоритм с открытым ключом для шифрования симметричного ключа. По коммуникационному каналу передается текст, зашифрованный симметричным ключом, и симметричный ключ, зашифрованный открытым ключом. Для расшифровки действия производятся в обратном порядке: сначала при помощи секретного ключа получателя расшифровывается симметричный ключ, а затем при помощи симметричного ключа - полученный по каналу зашифрованный текст. Для формирования электронной подписи по подписываемому тексту вычисляется его однонаправленная хэш-функция (дайджест) [one-way hash function, digest], представляющая собой один короткий блок информации, характеризующий весь текст в целом; задача восстановления текста по его хэш-функции или подбора другого текста, имеющего ту же хэш-функцию, практически неразрешима. При непосредственном формировании подписи, вместо шифрования секретным ключом каждого блока текста секретный ключ применяется только к хэш-функции; по каналу передается сам текст и сформированная подпись хэш-функции. Для проверки подписи снова вычисляется хэш-функция от полученного по каналу текста, после чего при помощи открытого ключа проверяется, что подпись соответствует именно данному значению хэш-функции. Алгоритмы вычисления однонаправленных хэш-функций, как правило, логически тесно связаны с алгоритмами шифрования с симметричным ключом.

Описанные гибридные методы шифрования и цифровой подписи сочетают в себе эффективность алгоритмов с симметричным ключом и свойство независимости от дополнительных секретных каналов для передачи ключей, присущее алгоритмам с открытым ключом. Криптографическая стойкость конкретного гибридного метода определяется стойкостью слабейшего звена в цепи, состоящей из алгоритмов с симметричным и с открытым ключом, выбранных для его реализации.

Система RSA

В 1978 г. Р.Ривест, А.Шамир и Л.Адлеман [RSA78] создали первую криптосистему с открытым ключом для шифрования и цифровой подписи, получившую название RSA (по первым буквам фамилий авторов). Система описывается в терминах элементарной теории чисел. Ее надежность обуславливается практической неразрешимостью задачи разложения большого натурального числа на простые множители. Современное состояние алгоритмов факторизации (разложения на множители) позволяет решать эту задачу для чисел длиной до 430 бит; исходя из этого, ключ длиной в 512 бит считается надежным для защиты данных на срок до 10 лет, а в 1024 бита - безусловно надежным. Длина подписи в системе RSA совпадает с длиной ключа.

Несмотря на то, что отсутствует математически доказанное сведение задачи раскрытия RSA к задаче разложения на множители, а также задачи разложения на множители к классу NP-полных задач, система выдержала испытание практикой и является признанным стандартом de-facto в промышленной криптографии, а также официальным стандартом ряда международных организаций. С другой стороны, свободное распространение программного обеспечения, основанного на RSA, ограничено тем, что алгоритм RSA защищен в США рядом патентов.

Проект DSS

В 1991 г. в США был опубликован проект федерального стандарта цифровой подписи - DSS (Digital Signature Standard, [DSS91], см. также [S94], с.304-314), описывающий систему цифровой подписи DSA

(Digital Signature Algorithm). Одним из основных критериев при создании проекта была его патентная чистота.

Предлагаемый алгоритм DSA, имеет, как и RSA, теоретико-числовой характер, и основан на криптографической системе Эль-Гамаля [E85] в варианте Шнорра [S89]. Его надежность основана на практической неразрешимости определенного частного случая задачи вычисления дискретного логарифма. Современные методы решения этой задачи имеют приблизительно ту же эффективность, что и методы решения задачи факторизации; в связи с этим предлагается использовать ключи длиной от 512 до 1024 бит с теми же характеристиками надежности, что и в системе RSA. Длина подписи в системе DSA меньше, чем в RSA, и составляет 320 бит.

С момента опубликования проект получил много критических отзывов (см., напр., [R92]), многие из которых были учтены при его доработке. Одним из главных аргументов против DSA является то, что, в отличие от общей задачи вычисления дискретного логарифма, ее частный случай, использованный в данной схеме, мало изучен и, возможно, имеет существенно меньшую сложность вскрытия. Кроме того, стандарт не специфицирует способ получения псевдослучайных чисел, используемых при формировании цифровой подписи, и не указывает на то, что этот элемент алгоритма является одним из самых критичных по криптографической стойкости.

Функции DSA ограничены только цифровой подписью, система принципиально не предназначена для шифрования данных. По быстродействию система DSA сравнима с RSA при формировании подписи, но существенно (в 10-40 раз) уступает ей при проверке подписи.

Вместе с проектом DSS опубликован проект стандарта SHS (Secure Hash Standard), описывающий однонаправленную хэш-функцию SHA (Secure Hash Algorithm), рекомендованную для использования вместе с DSA (см. [S94], с.333-336). Хэш-функция SHA является модификацией алгоритма MD4, хорошо известного в криптографической литературе.

Российский стандарт цифровой подписи

В 1993 г. в России были изданы два государственных стандарта “Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма” и “Функция хэширования”, под общим заголовком “Информационная технология. Криптографическая защита информации”.

Стандарт “Процедуры выработки и проверки электронной цифровой подписи...” во многом схож со своим американским аналогом DSS. Для формирования и проверки цифровой подписи в нем используется тот же алгоритм Эль-Гамаля и Шнорра, что и в DSS, с незначительными модификациями. Имеется две альтернативных длины ключа, 512 и 1024 бит; длина подписи составляет 512 бит.

Для генерации ключей предложен ряд новых алгоритмов. Ключи, получаемые при помощи этих алгоритмов, имеют специальный вид, что потенциально может упростить задачу вскрытия системы по сравнению с DSS. Критика DSS, связанная с недостаточно разработанным теоретическим обоснованием алгоритма, в случае росийского стандарта несколько смягчается тем, что элемент ключа q выбирается более длинным, чем в DSA. Критика. связанная с отсутствием спецификации на способ получения псевдослучайных чисел, остается в силе.

Как и DSS, российский стандарт определяет только алгоритм цифровой подписи, но не шифрования. Быстродействие обоих алгоритмов приблизительно совпадает.

Стандарт “Функция хэширования” предназначен для использования вместе со стандартом “Процедуры выработки и проверки цифровой подписи” и представляет собой оригинальный алгоритм, основанный на методе шифрования с симметричным ключом ГОСТ 28147. Стандарт не содержит криптографического обоснования выбранного алгоритма и не корректирует ГОСТ 28147 в части заполнения узлов замены.

Несмотря на указанные недостатки, система, описанная в российском стандарте, применима во многих областях, особенно для коммерческих приложений.

Программная криптографическая система ТерКрипт

Санкт-петербургским МГП “ТЕРКОМ” разработана криптографическая система ТерКрипт, представляющая собой комплекс программ на языке С стандарта ANSI. Система реализует в полном объеме алгоритмы DES, ГОСТ 28147, RSA, DSS/SHS и российских криптографических стандартов. Алгоритмы реализованы на основе общих процедур теории чисел, использующих современные теоретико-числовые методы для достижения максимальной эффективности. Имеется специальная версия системы, оптимизированная для работы на персональных компьютерах IBM AT 286, 386, 486.

Литература

[BFS91] Th.Beth, M.Frisch, G.J. Simmons (eds.) Public-Key Cryptography: State of the Art and Future Directions. E.I.S.S. Workshop - Oberwolfach, Germany, July 1991 - Final Report. Lecture Notes in Computer Science, V.578.

[DH76] W.Diffie, M.Hellman. New Directions in Cryptography. IEEE Trans. Inform. Theory, IT-22, No.6 (1976), pp.644-654.

[DSS92] The Digital Signature Standard Proposed by NIST. CACM, V.35 (1992), No.7, pp.36-40.

[E85] T.ElGamal. A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. IEEE Trans. Inform. Theory, IT-31 (1985), pp.469-472.

[R92] Responses to NIST’s Proposal. CACM, V.35 (1992), No.7, pp 41-54.

[RSA78] R.L.Rivest, A.Shamir, L.Adleman. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. CACM, V.21 (1978), No.2, pp.120-126.

[S94] B.Schneier. Applied Cryptography: Protocols, Algorithms and Source Code in C. John Wiley & Sons, Inc., 1994.

[S89] C.P.Schnorr. Efficient Identification and Signatures for Smart Cards. Advances in Cryptology: Proceedings of Crypto’89, G.Brassard (ed). Lecture Notes in Computer Science, V.435, pp.239-251.