ОЦЕНКИ АЛГОРИТМОВ ЦИФРОВОЙ ПОДПИСИ

А.М. Суходольский., Д.П. Урбанович
(БГУИР, г. Минск)

Введение

Большинство методов аутентификации электронных сообщений базируются на тех или иных криптографических алгоритмах. Такие методы аутентификации электронных сообщений существуют давно, но только с появлением нового направления в криптографии [1] они стали выполнять все требования, которые предъявляются к цифровой подписи.

Новое направление в криптографии связано с введение понятия *системы с открытыми ключами*. Одна из таких систем появилась в 1978 году, как результат работы трёх её авторов R. Rivest, A. Shamir, L. Adleman, и сейчас носит название RSA [2].

Такие криптосистемы с самого начала были ориентированны на обеспечение возможности выполнения с помощью них *цифровой подписи* электронных документов. Для полноты картины здесь необходимо упомянуть ещё одну систему с открытыми ключами, автором которой является T. El Gamal [3] и которая стала основой для создания государственных стандартов на цифровую подпись США (Digital Signature Standard - DSS).

В статье анализируются сравнительные оценки некоторых алгоритмов формирования и использования электронной подписи.

Особенности использования цифровой подписи

Приведём сравнительную оценку обычной подписи (под обычной подписью мы здесь понимаем подпись и печать) с цифровой подписью с точки зрения выполняемых ими защитных функций.

Защита целостности документа. В случае применения обычной подписи и печати после подписания документ может быть изменён (например, допечатано пару нулей). Изменить же электронный документ, подписанный цифровой подписью, невозможно, поскольку содержание документа через его дайджест "включается" в саму подпись.

Подделка подписи. Чтобы подделать обычную подпись достаточно иметь компьютер, цветные сканер и принтер, а также образец подписи и печати. Стоимость перечисленного оборудования в настоящее время не превышает $2000. Далее дело техники. Для подделки цифровой подписи, при рекомендуемой специалистами на настоящее время длине ключей, необходимо

иметь специальный суперкомпьютер стоимостью несколько сот миллионов долларов и запас по времени приблизительно в 300 – 500 лет. Если длину ключей увеличить в два раза, то стоимость оборудования и время вычисления подписи резко возрастают.

Конфиденциальность. Документ, подписанный обычной подписью, может быть прочитан любым лицом, к которому он попал в руки. В случае цифровой подписи предусматривается режим, когда документ может быть прочитан только лицом, которому он адресован.

Оценка некоторых алгоритмов цифровой подписи

Проведем теперь сопоставление некоторых конкретных алгоритмов цифровой подписи с целью выявления их преимуществ и недостатков в различных ситуациях. Для удобства оценки основных свойств того или иного алгоритма мы будем сравнивать его основные характеристики: длину ключей, длину цифровой подписи, сложность (время) вычисления и сложность (время) проверки подлинности цифровой подписи при условии, что уровень стойкости подписи по отношению к любым методам фальсификации не ниже, чем 10^{21} (или 30 лет непрерывной работы сети из 1000 суперкомпьютеров). В качестве "базовой" длины ключей и длины самой цифровой подписи мы будем рассматривать длину в 64 байта.

RSA. Первым по времени изобретения конкретным алгоритмом цифровой подписи был разработанный в 1977 году в Массачусетском технологическом институте алгоритм RSA. Алгоритм RSA основывается на том математическом факте, что задача дискретного логарифмирования при выборе целого параметра **n** в виде произведения двух различных простых чисел примерно равных по порядку величины, т.е. **n = p*q** становится не менее сложной, чем разложение **n** на эти простые множители, а последняя задача давно (еще со времен Архимеда и Евклида) известна в математике как сложная.

По современным оценкам сложность задачи разложения на простые множители при целых числах **n** из 64 байт составляет порядка 10^{17} - 10^{18} операций, т. е. находится где-то на грани досягаемости для серьезного "взломщика". Поэтому обычно в системах цифровой подписи на основе алгоритма RSA применяют более длинные целые числа **n** (обычно от 75 до 128 байт).

Это соответственно приводит к увеличению длины самой цифровой подписи относительно 64-байтного варианта примерно на 20% -100% (в данном случае ее длина совпадает с длиной записи числа **n**), а также от 70% до 800% увеличивает время вычислений при подписывании и проверке.

Кроме того, при генерации и вычислении ключей в системе RSA необходимо проверять большое количество довольно сложных дополнительных условий на простые числа **p** и **q** (что сделать достаточно трудно и чего обычно не делают, пренебрегая вероятностью неблагоприятного исхода - возможной подделки цифровых подписей)., а невыполнение любого из них может сделать возможным фальсификацию подписи со стороны того, кто обнаружит невыполнение хотя бы одного из этих условий (при подписывании важных документов допускать, даже теоретически, такую возможность нежелательно).

DSA.. Национальным институтом стандартов и технологий США в 1991 году на основе алгоритма Эль-Гамаля [3] был разработан и представлен на рассмотрение Конгресса США новый алгоритм цифровой подписи, получивший название DSA (сокращение от Digital Signature Algorithm). Алгоритм DSA, ставший в дальнейшем основой национального стандарта США на цифровую подпись, имеет по сравнению с алгоритмом RSA целый ряд преимуществ: во-первых, при заданном уровне стойкости цифровой подписи целые числа, с которыми приходится проводить вычисления, имеют запись как минимум на 20% короче, что соответственно уменьшает сложность вычислений не менее чем на 70% и позволяет заметно сократить объем используемой памяти; во-вторых, при выборе параметров достаточно проверить всего три достаточно легко проверяемых условия; в-третьих, процедура подписывания по этому методу не позволяет вычислять (как это возможно в RSA) цифровые подписи под новыми сообщениями без знания секретного ключа.

Эти преимущества, а также соображения, связанные с возможностью его реализовывать любым разработчиком свободно без коммерческих лицензионных соглашений с держателями патента, компанией RSA Data Security, и возможностью свободного безлицензионного экспорта такой технологии из США послужили главным мотивом для принятия в 1994 году национального стандарта цифровой подписи (DSS) на его основе.

Кроме того, в практике в последние годы нередко встречаются алгоритмы цифровой подписи, основанные на вычислениях с алгебраическими кривыми. Эти алгоритмы позволяют значительно сократить длину цифровой подписи при сохранении надежности защиты от подделки, но научная основа оценок их надежности настолько сложна математически, что говорить о широко известной сложной задаче, лежащей в основе надежности цифровой подписи, уже не приходится. В этом случае пользователю приходится полностью доверять мнению

очень узкой группы экспертов. И даже поверхностное представление о современных оценках надежности этих алгоритмов получить не просто.

Литература

1. W. Diffie and M.E. Hellman. New directions in cryptography//IEEE Trans. on Info. Theory, vol. IT-22, pp. 644-654, Nov. 1976.

2. R. Rivest, A. Shamir, and L. Adleman. A Method for Obtaining Digital Signatures and Public Key Cryptosystems//Commun. of the Assoc. of Comp. Math., Vol. 21, pp. 120-126, Feb. 1978.

3. T. El Gamal. A Public – Key Cryptosystem and a Signature Scheme Based on Discrete Logarithm// IEEE Trans. on Info. Theory, vol. IT-31, pp. 469-472, July 1985.

НЕКОТОРЫЕ АСПЕКТЫ ПРОБЛЕМЫ ИСПОЛЬЗОВАНИЯ ЭЛЕКТРОННОЙ ПОДПИСИ

Д.П. Урбанович

(БГУИР, г. Минск)

Введение

Тенденции развития вычислительной техники и математики стимулируют развитие новых, принципиально отличающихся технологий решения информационных задач в различных сферах. Одним из таких направлений является *электронная коммерция*. Проблемы, возникающие и решаемые в указанной области, активно обсуждаются на конференциях и в печати (см., например, [1]). Ниже проанализируем особенность одной из проблем: *электронную подпись*.

О подписи вообще

Все современные информационные технологии, связанные с обменом электронных документов, в своей основе содержат "кирпичик", который получил название *цифровая подпись*. К системам, использующим такие технологии, относятся автоматизированные банковские системы типа "Клиент – Банк", системы для обеспечения электронных платежей в Интернет, платёжные системы на основе *smart–карт*, другие коммерческие и секретные системы связи.

Любая подпись, будь-то обычная или цифровая, всегда выполняет, по крайней мере, три функции: первая – это удостоверение того, что подписавшийся является тем, за которого мы его принимаем (функция авторизации); вторая - это то, что подписавшийся не может отказаться от документа, который он подписал; и третья – подтверждение того, что отправитель подписал именно тот документ, который отправил, а не какой-либо иной. Другими словами, ему нельзя навязать другой или похожий документ, поскольку у него есть подпи-