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-

санная копия оригинала. Заметим, что две первые функции обеспечивают защиту интересов лица, для которого предназначен документ (приемника), а третья - защищает интересы подписывающего (передатчика). Во всех этих случаях "работает" свойство подписи, называемое *аутентичность*, т.е. подлинность. Это свойство переносится на документ, под которым стоит подпись.

Аутентификация сообщений является жизненно важным фактором для всех абонентов как коммерческих, так и секретных систем связи. Например, лица, принимающие чек, обычно настаивают на подтверждении личности выписывающего чек – аутентификации источника информации, или передатчика, а лицо, выписывающее чек, проставляет сумму не только цифрами, но и прописью. Таковы простейшие способы аутентификации передаваемой информации или сообщений.

Говоря в доступных терминах, аутентификация – это не более и не менее, как установление приёмником и, возможно, арбитром того факта, что при существующем протоколе (правилах) аутентификации данное сообщение послано санкционированным (законным) передатчиком и что оно при этом не заменено и не искажено. 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 [3] 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 [3].

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 и которая стала основой для создания государственных стандартов на цифровую подпись США (Digital Signature Standard - DSS).

Цифровая подпись

Предположим, что некоторый абонент **A** хочет подписать какое-либо сообщение и отправить его абоненту **B**. Для этого он, с помощью специальной математической функции, так называемой *хеш-функции*, создаёт *дайджест* (слепок) этого сообщения. Односторонняя хеш-функция не использует ключ.

Это обычная формула для преобразования послания любой длины в одну строку символов (дайджест послания). При использовании 16-байтной хеш-функции обработанный ей текст будет иметь на выходе длину 16 байт — например, послание может быть представлено цепочкой символов CBBV235ndsAG3D67. Каждое послание образует свой случайный дайджест. Затем зашифровывает его своим секретным ключом **Е.** Свойства хеш-функции таковы, что полученный с помощью её дайджест "жестко" связан с сообщением. Зашифрованный дайджест "прикрепляется" к сообщению, теперь он является цифровой подписью сообщения.

Абонент **В** использует открытый ключ абонента **А** для расшифровки цифровой подписи и получает копию дайджеста послания от **А**. Поскольку он сумел расшифровать цифровую подпись открытым ключом **А**, то значит, **А** является ее автором. Затем **В** использует ту же самую хеш-функцию (о которой оба договорились заранее) для подсчета собственного дайджеста для открытого текста послания **А**. Если полученная им строка совпадает с той, что прислал **А**, то он может быть уверена в аутентичности цифровой подписи. А это означает не только то, что отправитель послания **А**, но также и то, что послание не было изменено. На рис. 1 показана упрощенная схема процессов выполнения подписи документа и проверки подписи получателем в таких системах.

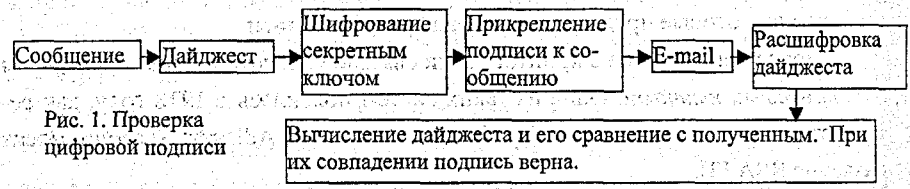

Рис. 1. Проверка цифровой подписи

Для шифрования открытого текста послания следует дополнительно использовать симметричный алгоритм с секретным ключом. Но это приведет к дальнейшему усложнению процесса. Таким образом, цифровая подпись на основе систем с открытыми ключами полностью выполняет три функции подписи, которые были перечислены выше.

Литература.

1. Урбанович Д.П. Принципы организации и использования возможностей электронной коммерции и бизнеса// II International Symposium NEET'2001. New Electrical & Electronic technologies & their industrial implementation.Symposium Proceedings. Poland. 14-17.02.2001.

2. Kosiur D. Understanding electronic Commerce, Microsoft Press, 1998. – 288 p.

3. 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.