АНАЛИЗ ОСОБЕННОСТЕЙ ИСПОЛЬЗОВАНИЯ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ ОСНОВАННОЙ НА АССИМЕТРИЧНЫХ АЛГОРИТМАХ ШИФРОВАНИЯ

Розумный А.Ю.
Лицей «Интеллект», г. Донецк

Введение

Благодаря бурному развитию информационной сферы, в нашу жизнь вошли и стали уже привычными технологии, без которых современный мир уже и трудно себе представить. Одной из таких технологий, которая, между прочим, стоит на страже безопасности совершаемых в сети операций, является электронная цифровая подпись (ЭЦП). Её применение в качестве средства для идентификации и подтверждения юридической значимости документов становится стандартом цифрового мира. ЭЦП используется в качестве аналога собственноручной подписи.

В прошлом для того, чтобы подписать документ или установить подлинность какой-либо бумаги, необходимо было личное присутствие всех заинтересованных сторон. Сейчас, благодаря ЭЦП, появилась возможность решать такие вопросы удаленно.

Что же такое электронная цифровая подпись?

Электронная цифровая подпись – это реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий установить отсутствие искажения информации в электронном документе. Из этого определения видно, что ЭЦП формируется при помощи специальных математических алгоритмов на основе собственно документа и некого «закрытого ключа», позволяющего однозначно идентифицировать отправителя сообщения.

Общая схема реализации ЭЦП

Существует несколько методов построения ЭЦП. Например, шифрование электронного документа (ЭД) на основе симметричных алгоритмов. Данная схема предусматривает наличие в системе третьего лица – арбитра, пользующегося доверием обеих сторон. Авторизацией документа в данной схеме является сам факт шифрования ЭД секретным ключом и передача его арбитру.

Также используют ассиметричные алгоритмы шифрования. Фактом подписания документа является шифрование его на основе секретного ключа отправителя. Развитием предыдущей идеи стала наиболее распространенная схема ЭЦП – шифрование окончательного результата обработки ЭД хеш-функцией при помощи ассиметричного алгоритма.

Кроме перечисленных, существуют и другие методы построения схем ЭЦП: групповая подпись, неоспариваемая подпись, доверенная подпись и др. Появление этих разновидностей обусловлено разнообразием задач, решаемых с помощью электронных технологий передачи и обработки электронных документов.

Схема электронной подписи основанной на ассиметричных алгоритмах шифрования включает в себя:

- алгоритм генерации ключевых пар пользователя;
- функцию вычисления подписи;
- функцию проверки подписи.

Каждому пользователю ЭЦП, участвующему в обмене электронными документами, генерируются уникальные открытый и закрытый (секретный) криптографические ключи. Секретный ключ (код) есть у каждого субъекта, имеющего право подписи, и может храниться на дискете или смарт-карте. Открытый ключ используется получателями документа для проверки подлинности ЭЦП.

На рис. 1 показано, каким образом происходит функционирование ЭЦП. Во-первых, информация обрабатывается с помощью хеш-функции (происходит так называемый процесс хеширования). Хеширование – это процесс преобразования входного массива данных произвольной длины в выходную битовую строку фиксированной длины.

Хеш-функция создает контрольную сумму данных. Эта контрольная сумма затем шифруется с использованием секретного ключа пользователя. Информация и зашифрованная контрольная сумма передаются получателю информации.

Когда информация принимается получателем, он обрабатывает её той же самой хэш-функцией. Далее получатель проверяет присланную контрольную сумму соответствующим открытым ключом и сравнивает две контрольные суммы. Если они совпадают, это означает, что информация не была изменена.

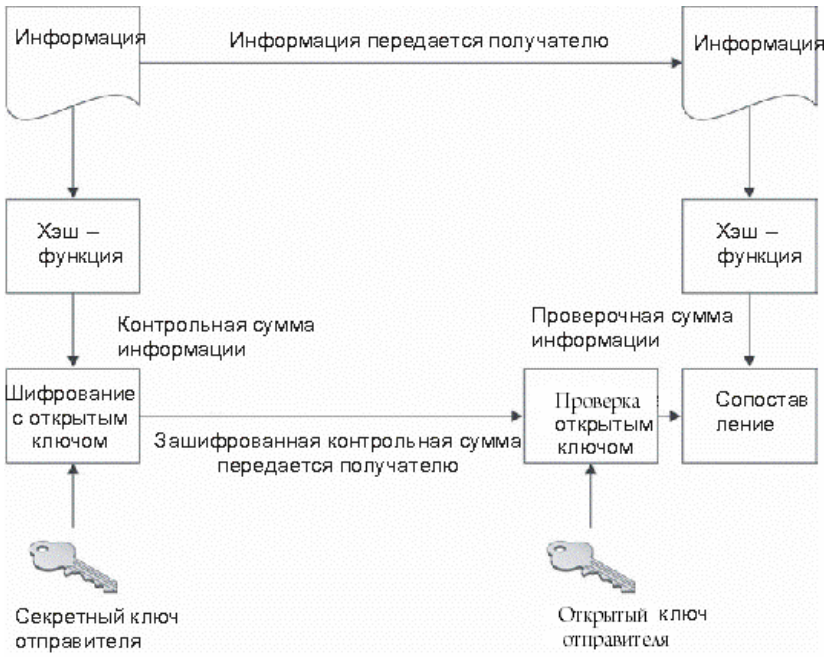

Рисунок 1 – Функционирование цифровых подписей основанных на ассиметричных алгоритмах

Управление ключами от ЭЦП

Важной проблемой всей криптографии с открытым ключом, в том числе и систем ЭЦП, является управление открытыми ключами. Необходимо обеспечить доступ любого пользователя к подлинному открытому ключу любого другого пользователя, защитить эти ключи от подмены злоумышленником, а также организовать отзыв ключа в случае его компрометации.

Задача защиты ключей от подмены решается с помощью сертификатов. Сертификат позволяет удостоверить заключенные в нём данные о владельце и его

открытый ключ подписью какого-либо доверенного лица. В централизованных системах сертификатов используются центры сертификации. В децентрализованных системах путём перекрёстного подписания сертификатов знакомых и доверенных людей каждым пользователем строится сеть доверия.

Управлением ключами занимаются центры распространения сертификатов. Обратившись к такому центру, пользователь может получить сертификат какого-либо пользователя, а также проверить, не отозван ли ещё тот или иной открытый ключ.

Защищённость ЭЦП

Очевидно, что ЭЦП не совершенна. Возможны следующие угрозы цифровой подписи. Злоумышленник может:

- попытаться подделать подпись для выбранного им документа;
- попытаться подобрать документ к данной подписи, чтобы подпись к нему подходила;
- попытаться подделать подпись для хоть какого-нибудь документа;
- в случае кражи закрытого ключа подписать любой документ от имени владельца ключа;
- обманом заставить владельца подписать какой-либо документ, например, используя протокол слепой подписи;

При использовании надежной хэш-функции, вычислительно сложно создать поддельный документ с таким же хэшем, как и у подлинного. Однако эти угрозы могут реализоваться из-за слабостей конкретных алгоритмов хэширования, подписи или ошибок в их реализациях.

Несмотря на стремительное развитие высоких технологий «взломать» ЭЦП достаточно сложно. Это требует огромного количества вычислений, которые (при современном уровне математики и вычислительной техники) не могут быть проведены за приемлемое время, то есть пока информация, содержащаяся в подписанном документе, сохраняет актуальность. Дополнительная защита от подделки обеспечивается сертификацией удостоверяющим центром открытого ключа подписи.

Преимущества использования ЭЦП

- подпись аутентична, то есть с ее помощью получателю документа можно доказать, что она принадлежит подписывающему лицу;
- подпись защищает подписанный документ от подделки, а также от изменения или искажения содержащейся в нем информации
- подпись непереносима, то есть является частью документа и поэтому перенести ее на другой документ невозможно;
- подпись неоспорима;

Средства работы с ЭЦП

В настоящее время существует большое количество комплексов для работы с электронной подписью, или использующие ее. Наиболее известный - это пакет PGP (Pretty Good Privacy), без сомнений являющийся на сегодня самым распространенным программным продуктом, позволяющим использовать современные надежные криптографические алгоритмы для защиты информации в персональных компьютерах. К основным преимуществам данного пакета, выделяющим его среди других аналогичных продуктов следует отнести следующие:

1. ***Открытость***. Исходный код всех версий программ PGP доступен в открытом виде.

2. ***Стойкость***. Для реализации основных функций использованы надёжные алгоритмы, при этом допускается возможность использования достаточно большой длины ключа для надежной защиты данных.
3. ***Бесплатность***. Готовые базовые продукты PGP (равно как и исходные тексты программ) доступны в Интернете в частности на официальном сайте PGP Inc.
4. ***Поддержка*** как централизованной (через серверы ключей) так и децентрализованной (через "сеть доверия") модели распределения открытых ключей.
5. ***Удобство программного интерфейса***. PGP изначально создавалась как продукт для широкого круга пользователей, поэтому освоение основных приемов работы отнимает всего несколько часов.

Вывод

Таким образом, электронная цифровая подпись - это эффективное решение для всех, кто хочет идти в ногу с новыми требованиями времени. ЭЦП является надёжным методом аутентификации электронной информации посредством шифрования. ЭЦП является наиболее перспективным и широко используемым в мире способом защиты электронных документов от подделки и обеспечивает высокую достоверность сообщения.

Сфера применения электронной цифровой подписи очень широка. Это – осуществление разнообразных регистрационных процедур, оформление документов для предоставления государственным учреждениям, участие в тендерах на закупку товаров, работ и услуг за государственные средства, электронные платежи и коммерция.

Документы, подписанные электронной цифровой подписью, могут быть переданы к месту назначения в течение нескольких секунд. Все участники электронного обмена документами получают равные возможности независимо от их удаленности друг от друга.

Литература

[1] Баричев С.Г., Гончаров В.В., Серов Р.Е. Основы современной криптографии.–М.: Горячая линия – Телеком, 2001.–152с.

[2] Петров А.А. Компьютерная безопасность. Криптографические методы защиты.–М.: ДМК, 2000. – 448с.: ил.

[3] Терехов А.Н., Тискин А.В. Криптография с открытым ключом: от теории к стандарту//Программирование РАН.–1994.– № 5.– С. 17-22.