УДК [004.78:655.3]:347.189

И.И. Белоусов, студент,
Харьковский национальный экономический университет
г. Харьков, Украина
Griffin-89@mail.ru
Научный руководитель Климнюк В. Е.

ФАКТОРЫ, ПРЕПЯТСТВУЮШИЕ РАСПРОСТРАНЕНИЮ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ В ПОЛИГРАФИИ И ПУТИ ИХ УСТРАНЕНИЯ

Распространение интернет технологий, способствует интенсификации общения между автором и издательством по средствам глобальной сети. Однако наряду с преимуществами существует опасность перехвата высылаемых файлов для нейтрализации, которой внедряются программные средства зашиты. Одним из таких средств основанным на криптографическом преобразовании информации является электронная цифровая подпись, которая имеет юридически силу как аналоговая. Основной из причин таких распространения является совместимость ЭЦП созданных с помощью разных программ. Указанное обстоятельство обусловливает цель данного исследования, которая состоит в исследовании совместимости ЭЦП разных программных средств, и путей устранения этой проблемы.

Электронная цифровая подпись (ЭЦП) (Digital signature) - вид электронной подписи, полученного по результату криптографического превращения набора электронных данных, который добавляется к этому набору или логично с ним совмещается и дает возможность подтвердить его целостность и идентифицировать подписывателя. Электронная цифровая подпись налагается с помощью закрытого ключа и проверяется с помощью открытого ключа. [1]

Закрытый ключ - параметр криптографического алгоритма формирования электронной цифровой подписи, доступный только подписывателю.

В настоящее время существуют следующие устройства хранения закрытого ключа:

- Дискеты
- Смарт-карты
- USB-брелоки
- Таблетки Touch-Memory [2]

Открытый ключ - параметр криптографического алгоритма проверки электронной цифровой подписи, доступный субъектам отношений, в сфере использования электронной цифровой подписи.[1]

Важной проблемой всей криптографии с открытым ключом, в том числе и систем ЭЦП, является управление открытыми ключами. Так как открытый ключ доступен любому пользователю, то необходим механизм проверки того, что этот ключ принадлежит именно своему владельцу. 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.[2]

Обзор алгоритмов ЭЦП

Для генерации пары ключей (секретного и открытого) в алгоритмах ЭЦП, используются разные математические схемы, основанные на применении однонаправленных функций. Эти схемы разделяются на две группы. В основе такого разделения лежат известные сложные вычислительные задачи:

- задача факторизации (разложения на множители) больших целых чисел;
- задача дискретного логарифмирования.

Первой и наиболее известной во всем мире конкретной системой ЭЦП стала система RSA, математическая схема которой была разработана в 1977 г. в Массачуссетском технологическом институте США. Алгоритм получил свое название по первым буквам фамилий его авторов: Rivest, Shamir и Adleman. Надежность алгоритма основывается на трудности факторизации больших чисел.

Более надежный и удобный для реализации на персональных компьютерах ЭЦП алгоритм был разработан в 1984 г. американцем арабского происхождения Тахером Эль Гамалем и получил название El Gamal Signature Algorithm (EGSA).

Идея EGSA основана на том, что для обоснования практической невозможности фальсификации ЭЦП может быть использована более сложная вычислительная задача, чем разложение на множители большого целого числа – задача дискретного логарифмирования. Кроме того Эль Гамалю удалось избежать явной слабости алгоритма ЭЦП RSA, связанной с возможностью подделки ЭЦП под некоторыми сообщениями без определения секретного ключа.

Алгоритм цифровой подписи Digital Signature Algorithm (DSA) предложен в 1991г. в США для использования в стандарте цифровой подписи DSS (Digital Signature Standard). Алгоритм DSA является развитием алгоритма ЭЦП EGSA. По сравнению с алгоритмом ЭЦП EGSA алгоритм DSA имеет ряд преимуществ: сокращен объем памяти и время вычисления подписи. Недостатком же является необходимость при подписывании и проверке подписи выполнять сложные операции деления по модулю большого числа.[3]

Предлагаемые сейчас варианты реализации цифровой подписи имеют один общий недостаток: все они являются *программно-зависимыми*. Снабжение документа такой подписью происходит таким образом, что подпись встраивается в файл, содержащий документ. При этом файл преобразуется в специфический формат. Он воспринимается только той системой документооборота, в которую встроены средства, поддерживающие именно такую подпись. Более того, чтобы нормально воспроизвести такой документ в его исходном формате, в некоторых случаях эту подпись нужно после проверки отсечь, а это может сделать только программа, корректно распознающая ее. Другими словами, такая подпись действует лишь *внутри системы* - с ее помощью нельзя проверить подлинность документа, поступившего извне. Министерство статистики не сможет полноценно обработать в своей системе электронный документ, поступивший, например, из Национального банка, и наоборот. Нетрудно представить, какие проблемы возникнут, когда все ведомства захотят обмениваться электронными документами, а затем и передавать их в государственный.

Очевидно, что при внедрении цифровой подписи непосредственно в файл все средства ЭЦП, внедряемые в разных организациях, должны быть или единообразными (подобно тому, как в любой организации есть текстовый редактор Word), или, по крайней мере, поддерживать единый формат обмена данными (так текст из того же Word'a можно перенести в электронную таблицу Excel или базу данных Access с помощью буфера обмена, при этом он временно преобразуется в формат rtf, понимаемый всеми этими программами). Но более удачным подходом представляется такой, при котором значение хэш-функции рассчитывается разными программами по стандартному алгоритму, а выработанная на ее основе цифровая подпись хранится в отдельном файле-приложении стандартизированного формата. Этот формат должен распознаваться любыми средствами ЭЦП. При этом исходные файлы, содержащие общую часть документа, остаются доступными. Подлинность их содержания обеспечивается за счет того, что при любом исправлении изменится и значение хэш-функции, которое всегда можно проверить и сопоставить с особенной частью, хранящейся в защищенном файле-приложении. [4]

Если производители программного обеспечения для ЭЦП будут работать по одним алгоритмам и создавать совместимые продукты, или встраивать свой продукт конвертер способный распознавать файлы других программных обеспечений то ЭЦП будет более востребовано в полиграфических предприятиях Украины.

Литература:

1. Закон України "Про електронний цифровий підпис". [Электронный ресурс] // Державне підприємство Український державний центр радіочастот. – Режим доступа: http://www.ucrf.gov.ua/uk/doc/laws/1149760377/

2. Электронная цифровая подпись. [Электронный ресурс] // Википедия, свободная энциклопедия. – Режим доступа: http://ru.wikipedia.org/wiki

3. Анализ алгоритмов электронной цифровой подписи. [Электронный ресурс] // Лаборатория Информационной Безопасности. – Режим доступа: http://www.security.ase.md/publ/ru/pubru86/

4. Цифровая подпись в современном делопроизводстве. [Электронный ресурс] // Персональный сайт белорусского историка Вячеслава Носевича. – Режим доступа: http://vn.belinter.net/digit/8.html