УДК 004.052.2

Е.В. Ромашка, А.В. Гапонов, А.Е. Алпатова
Восточноукраинский национальный университет
имени В.Даля, г. Луганск
Кафедра компьютерных наук

ИНФОРМАЦИОННАЯ МОДЕЛЬ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ С ИСПОЛЬЗОВАНИЕМ ХЕШ-ФУНКЦИИ

Аннотация

Ромашка Е.В., Гапонов А.В., Алпатова А.Е. Информационная модель электронной цифровой подписи с использованием хеш-функции. *Рассмотрена защита информации в компьютерных системах с помощью применения технологии электронной цифровой подписи. Указаны основные принципы работы электронной цифровой подписи. Представлена схема формирования и проверки электронной цифровой подписи. Проанализирована надежность использования технологии электронной цифровой подписи.*

Ключевые слова: *защита информации, электронная цифровая подпись, надежность, хеш-функция.*

Постановка проблемы. В современных условиях при обработке документов в электронной форме совершенно непригодны традиционные способы установления подлинности по рукописной подписи и оттиску печати на бумажном документе. Таким образом, возникает необходимость внедрения современных технологий в этой области, таких как электронная цифровая подпись. Однако с использованием цифровой подписи возникает вопрос ее надежности. В связи с этим необходимо провести анализ информационной модели цифровой подписи и выявление ее достоинств и недостатков.

Защита информации. Электронная цифровая подпись используется для аутентификации текстов, передаваемых по телекоммуникационным каналам. Функционально она аналогична обычной рукописной подписи и обладает ее основными достоинствами:

- удостоверяет, что подписанный текст исходит от лица, поставившего подпись;
- не дает самому этому лицу возможности отказаться от обязательств, связанных с подписанным текстом;
- гарантирует целостность подписанного текста. [1]

Технология применения системы электронной цифровой подписи предполагает наличие сети абонентов, посылающих друг другу подписанные электронные документы. Для каждого абонента генерируется пара ключей: секретный и открытый. Секретный ключ хранится абонентом в тайне и

используется им для формирования электронной цифровой подписи. Открытый ключ известен всем другим пользователям и предназначен для проверки цифровой подписи получателем подписанного электронного документа. Открытый ключ не позволяет вычислить секретный ключ.

Для генерации пары ключей (секретного и открытого) в алгоритмах электронной цифровой подписи, как и в асимметричных системах шифрования, 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.

Принципиальным моментом в системе электронной цифровой подписи является невозможность ее подделки пользователя без знания его секретного ключа подписывания. [2]

В качестве подписываемого документа может быть использован любой файл. Подписанный файл создается из неподписанного путем добавления в него одной или более электронных подписей.

Каждая подпись содержит следующую информацию:

- дату подписи,
- срок окончания действия ключа данной подписи,
- информацию о лице, подписавшем файл (Ф.И.О., должность, краткое наименование фирмы),
- идентификатор подписавшего (имя открытого ключа),
- собственно цифровую подпись.

Хеш-функция предназначена для сжатия подписываемого документа до нескольких десятков или сотен бит. Хеш-функция h() принимает в качестве аргумента сообщение (документ) M произвольной длины и возвращает хеш-значение h(M)=H фиксированной длины.

Следует отметить, что значение хеш-функции h(M) сложным образом зависит от документа M и не позволяет восстановить сам документ M.

Хеш-функция должна удовлетворять следующим условиям:

1. хеш-функция должна быть чувствительна к всевозможным изменениям в тексте M, таким как вставки, выбросы, перестановки и т.п.;
2. хеш-функция должна обладать свойством необратимости, то есть задача подбора документа M', который обладал бы требуемым значением хеш-функции, должна быть вычислительно неразрешима;
3. вероятность того, что значения хеш-функций двух различных документов (вне зависимости от их длин) совпадут, должна быть ничтожно мала.

Большинство хеш-функций строится на основе однонаправленной функции f(), которая образует выходное значение длиной n при задании двух входных значений длиной n. Этими входами являются блок исходного текста M, и хеш-значение H_{i-1} предыдущего блока текста (рисунок 1).

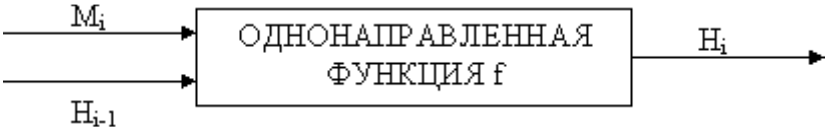

Рисунок 1 - Построение однонаправленной хеш-функции

$$H_i = f(M_i, H_{i-1}) \quad (1)$$

Хеш-значение, вычисляемое при вводе последнего блока текста, становится хеш-значением всего сообщения M.

В результате однонаправленная хеш-функция всегда формирует выход фиксированной длины n (независимо от длины входного текста). [3]

Основы построения хеш-функций. Общепринятым принципом построения хеш-функций является итеративная последовательная схема. По этой методике ядром алгоритма является преобразование k бит в n бит. Величина n - разрядность результата хеш-функции, а k - произвольное число, большее n. Базовое преобразование должно обладать всеми свойствами хеш-функции, т.е. необратимостью и невозможностью инвариантного изменения входных данных.

Хеширование производится с помощью промежуточной вспомогательной переменной разрядностью в n бит. В качестве ее начального значения выбирается произвольное известное всем сторонам значение, например, 0.

Входные данные разбиваются на блоки по (k-n) бит. На каждой итерации хеширования со значением промежуточной величины, полученной на предыдущей итерации, объединяется очередная (k-n)-битная порция входных данных, и над получившимся k-битным блоком производится базовое преобразование. В результате весь входной текст оказывается "перемешанным" с начальным значением вспомогательной величины. Из-за характера преобразования базовую функцию часто называют сжимающей. Значение вспомогательной величины после финальной итерации поступает на выход хеш-функции (рисунок 2). Иногда над получившимся значением производят дополнительные преобразования. Но в том случае, если сжимающая функция спроектирована с достаточной степенью стойкости, эти преобразования излишни.

При проектировании хеш-функции по итеративной схеме возникают два взаимосвязанных вопроса: как поступать с данными, не кратными числу (k-n), и как добавлять в хеш-сумму длину документа, если это требуется. Есть два варианта решения этих вопросов. В первом варианте в начало документа перед хешированием добавляется поле фиксированной длины (например, 32 бита), в котором в двоичном виде записывается исходная длина текста. Затем объединенный блок данных дополняется нулями до ближайшего кратного (k-n) бит размера. Во втором варианте документ дополняется справа одним битом

"1", а затем до кратного (k-n) бит размера битами "0". В этом варианте необходимость в поле длины отпадает - никакие два разных документа после выравнивания по границе порций не станут одинаковыми.

Кроме более популярных однопроходных алгоритмов хеширования существуют и многопроходные алгоритмы. В этом случае входной блок данных на этапе расширения неоднократно повторяется, а уже затем дополняется до ближайшей границы порции.

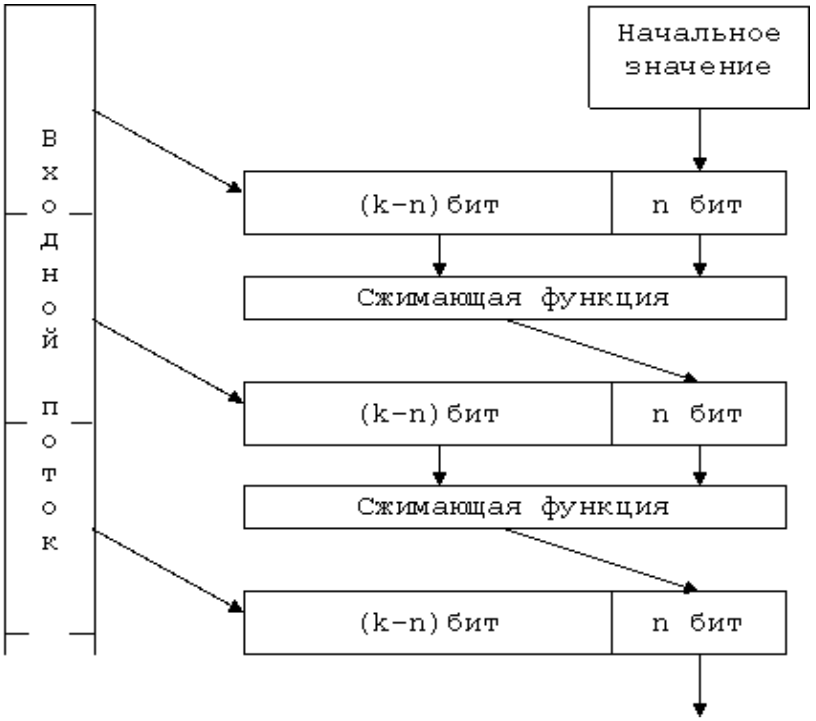

Рисунок 2 - Итерактивная хеш-функция

Обобщенная схема формирования и проверки цифровой подписи показана на рисунке 3

Допустим, что отправитель хочет подписать сообщение M перед его отправкой. Сначала сообщение M (блок информации, файл, таблица) сжимают с помощью хеш-функции h() в целое число m:

$$m = h(M) \quad (2)$$

Затем вычисляют цифровую подпись S под электронным документом M, используя хеш-значение m и секретный ключ D:

$$S = m^D (mod\ N) \quad (3)$$

Пара (M,S) передается партнеру-получателю как электронный документ M, подписанный цифровой подписью S, причем подпись S сформирована обладателем секретного ключа D.

После приема пары (M,S) получатель вычисляет хеш-значение сообщения M двумя разными способами. Прежде всего он восстанавливает хеш-значение m', применяя криптографическое преобразование подписи S с использованием открытого ключа E:

$$m = S^E (mod\ N) \quad (4)$$

Кроме того, он находит результат хеширования принятого сообщения M с помощью такой же хеш-функции h():

$$m = h(M) \quad (5)$$

Если соблюдается равенство вычисленных значений, т.е.

$$S^E (mod\ N) = h(M), \quad (6)$$

то получатель признает пару (M,S) подлинной. Доказано, что только обладатель секретного ключа D может сформировать цифровую подпись S по документу M, а определить секретное число D по открытому числу E не легче, чем разложить модуль N на множители.

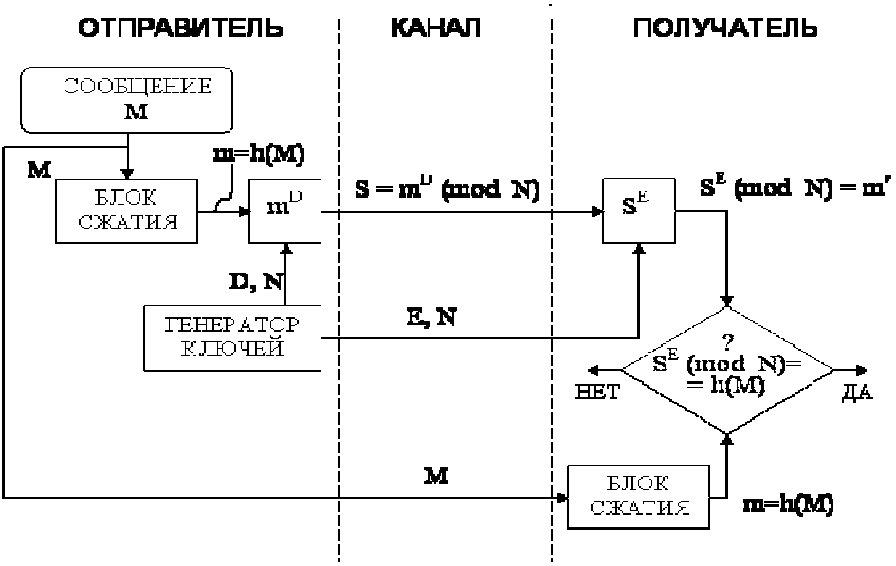

Рисунок 3 - Обобщённая схема цифровой подписи

Кроме того, можно строго математически доказать, что результат проверки цифровой подписи S будет положительным только в том случае, если при вычислении S был использован секретный ключ D, соответствующий открытому ключу E. Поэтому открытый ключ E иногда называют "идентификатором" подписавшего. [4]

Недостатки алгоритма цифровой подписи:

1. При вычислении модуля N, ключей E и D для системы цифровой подписи необходимо проверять большое количество дополнительных условий, что сделать практически трудно. Невыполнение любого из этих условий делает возможным фальсификацию цифровой подписи со стороны того, кто обнаружит такое невыполнение. При подписании важных документов нельзя допускать такую возможность даже теоретически.
2. Для обеспечения криптостойкости цифровой подписи по отношению к попыткам фальсификации на уровне, например, национального стандарта США на шифрование информации, т.е. 10^{18}, необходимо использовать при вычислениях N, D и E целые числа не менее 2512 (или около 10154) каждое, что требует больших вычислительных затрат, превышающих на 20...30% вычислительные затраты других алгоритмов цифровой подписи при сохранении того же уровня криптостойкости.
3. Цифровая подпись уязвима к так называемой мультипликативной атаке. Иначе говоря, алгоритм цифровой подписи позволяет злоумышленнику без знания секретного ключа D сформировать подписи под теми документами, у которых результат хеширования можно вычислить как произведение результатов хеширования уже подписанных документов.

Выводы. Рост информации показывает, что без электронной цифровой подписи в новом тысячелетии не обойтись. Применение ее необходимо, а со временем она может вытеснить из документооборота подпись при помощи шариковой ручки, посредством почтовой, телеграфной, телефонной и (или) телетайпной связи. Нескончаемый поток информации, стремление совершить сделку либо заключить то или иное правительственное соглашение в наиболее сжатые сроки заставит правоприменителя воспользоваться средствами электронной цифровой подписи.

Однако, не смотря на множество преимуществ, существует еще ряд недостатков, которые необходимо устранить для обеспечения неуязвимости технологии электронной цифровой подписи.

Список литературы

1. Закон України про електронний цифровий підпис (http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=852-15)
2. Саломаа А.: Криптография с открытым ключом. - М: Мир, 2008. - 318с.
3. Конеев И.Р., Беляев А.В. Информационная безопасность предприятия. - СПб.: БХВ-Петербург, 2003.-324с.
4. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. Под ред. В.Ф. Шаньгина. - 2-е изд., перераб. и доп. - М.: Радио и связь, 2001. - 376 с.: ил.