Лабораторная работа №6

Алгоритмы генерации и верификации электронной цифровой подписи

Цели работы

Изучение алгоритмов генерации и верификации электронной цифровой подписи и приобретение практических навыков их реализации.

Продолжительность: 4 часа

Теоретические сведения

Электронная цифровая подпись (ЭЦП) — важный элемент современных информационных систем, использующих криптографические методы. Понятие ЭЦП было введено в 1976 году У. Диффи и М. Хеллманом. После создания RSA появились алгоритмы цифровой подписи И. Рабина и Р. Меркле. В 1984 году Ш. Гольдвассер, С. Микалии и Р. Ривест сформулировали требования безопасности к этим алгоритмам и описали возможные атаки на ЭЦП.

Электронная цифровая подпись – контрольная характеристика сообщения, которая вырабатывается с использованием личного ключа, проверяется с использованием открытого ключа, служит для контроля целостности и подлинности сообщения и обеспечивает невозможность отказа от авторства.

Таким образом, ЭЦП выполняет те же функции, что и собственноручная (поставленная «от руки») подпись:

- аутентифицирование лица, подписавшего сообщение;
- контроль целостности подписанного сообщения;
- защита сообщения от подделок;
- доказательство авторства лица, подписавшего сообщение, если это лицо отрицает свое авторство.

Важнейшие отличительные особенности ЭЦП:

- ЭЦП представляет собой бинарную последовательность (в отличие от графического образа, каковым является подпись от руки);
- указанная бинарная последовательность зависит от содержания подписываемого сообщения.

Как следует из определения, основным компонентом в технологии ЭЦП является ключ. Принадлежность ключа, в предположении, что он известен только законным пользователям, позволяет решать все «возложенные на ЭЦП», сформированную на основе этого ключа, задачи. В соответствии с этим обстоятельством перечисленные выше функции ЭЦП могут быть реализованы на основе классических методов зашифрования/расшифрования:

- на основе симметричных систем (с тайным ключом);
- на основе симметричных систем и посредника;
- на основе асимметричных систем (с открытым ключом).

Первый из перечисленных методом ничем не отличается, например, от DES.

Во втором случае создаются две симметричные системы: между отправителем и посредником и между посредником и получателем. Причем посредник выдает двум сторонам различный тайный (для иных субъектов системы) ключ.

В последнем случае сообщение, отправляемое получателю, шифруется тайным ключом отправителя. Отправитель же верифицирует подпись (в данном случае – устанавливает авторство, используя для расшифрования публичный ключ отправителя, и получает гарантию в защищенности переданного сообщения от подделок, если после расшифрования формат и содержание документа имеют логическую стройность) с помощью открытого ключа отправителя.

Таким образом, в этом случае, как и в первых двух случаях, ЭЦП, как отдельный, самостоятельный, присоединенный к исходному документу элемент получаемого сообщения, отсутствует. Кроме того, в отличие от классической асимметричной криптографии, где используется ключевая информация получателя, в нашем случае используется ключевая информация отправителя: открытый ключ – для зашифрования, тайный – для расшифрования.

С учетом изложенного можем сформулировать определение ЭЦП в несколько ином виде.

Электронная цифровая подпись – бинарная (или в ином виде) последовательность символов, являющаяся реквизитом электронного документа, зависящая от содержания этого документа и предназначенная для подтверждения целостности и подлинности электронного документа.

ЭЦП на основе хешей подписываемых сообщений

Классическая технология использования ЭЦП предусматривает подписание не самого сообщения (обозначим его здесь $M_о$), а его хеша, $H(M_о)$. Это сокращает время генерации/верификации подписи и снижает вероятность появления случайных ошибок в итоговом документе.

Основу рассматриваемых протоколов составляют методы асимметричной криптографии и эллиптических кривых.

Общая структура подписанного электронного документа – $M_о - M'$ – представляет собой, как правило, конкатенацию этого документа и ЭЦП S. Кроме этих двух элементов, интегральный документ может содержать некоторую служебную информацию (дата, время отправки или различные данные об отправителе), как это схематично показано на рис. 1.

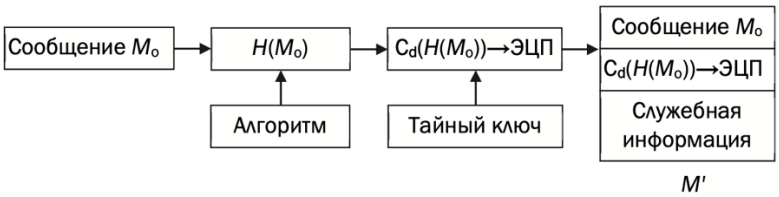

Рис. 1. Пояснение к процедуре формирования ЭЦП и структуре подписанного документа

Важное свойство цифровой подписи заключается в том, что ее может проверить (верифицировать) каждый, кто имеет доступ к открытому ключу ее автора. На рис. 2 показан в общем виде порядок процесса верификации (без учета использования служебной информации). Заметим, что в общем случае версии исходного документа ($M_о$) и полученного ($M_п$) могут отличаться.

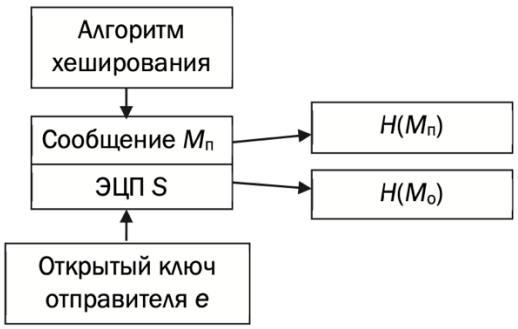

Рис. 2. Пояснение к процедуре верификации ЭЦП

Если в результате устанавливается равенство хешей: $H(M_п) = H(M_о)$, то принимается решение о подлинности подписи и целостности документа $M_п$, т. е. это также означает, что $M_п = M_о$.

Из приведенных на рис. 1 и рис. 2 последовательных преобразований можно сделать следующие общие выводы:

- при генерации ЭЦП (по классической схеме) для сообщения M отправитель последовательно выполняет следующие действия:
  - вычисляет хеш (хеш-образ) сообщения M: $H(M)$;
  - вычисляет содержание ЭЦП (собственно ЭЦП S) по хешу $H(M)$ с использованием своего закрытого ключа d: $S = C_d(H(M))$;
  - присоединяет (конкатенирует) ЭЦП к сообщению M и некоторой служебной информации, создавая таким образом итоговое сообщение M';
  - посылает сообщение M' получателю.
- получив сообщение M', другая сторона последовательно выполняет следующие действия:
  - отделяет цифровую подпись S от сообщения M (для общего случая применим одинаковые символьные обозначения);
  - применяет к сообщению M операцию хеширования, используя ту же функцию, что и отправитель, и получает хеш-образ полученного сообщения;

- используя открытый ключ отправителя, расшифровывает S, т. е. извлекает из ЭЦП хеш-образ отправленного сообщения;
- проверяет соответствие (равенство) обоих хеш-образов, и если они совпадают, то отправитель действительно является тем, за кого себя выдает, а сообщение при передаче не подверглось искажению.

При этом стойкость ЭЦП к подделыванию (криптостойкость) определяется теми же факторами, что и криптостойкость алгоритмов зашифрования/расшифрования сообщений: чтобы применение ЭЦП имело смысл, необходимо, чтобы вычисление легитимной подписи без знания закрытого ключа было вычислительно сложным процессом. Решение такой задачи в асимметричных алгоритмах реализации ЭЦП опирается на известные нам вычислительные задачи:

- факторизации, т. е. разложения числа на простые множители;
- дискретного логарифмирования.

Алгоритм RSA основывается на первой задаче, а алгоритмы Эль-Гамаля, DSA и Шнорра — на второй. Рассмотрим кратко математические основы этих алгоритмов.

ЭЦП на основе RSA

Здесь можно рассматривать две ситуации:

- сообщение M_o подписывается и передается в открытом (незашифрованном) виде;
- сообщение M_o подписывается и передается в зашифрованном виде.

Первый случай соответствует схеме и операциям, представленным на рис. 1 и рис. 2. При этом подпись S вычисляется на основе известного из лабораторной работы № 5 соотношения:

$$S \equiv \left(H(M_o)\right)_{d_o} \bmod n_o,$$

при указанном выше реверсе в отношении ключевой информации; в d_o и n_o – элементы тайного ключа отправителя. Передаваемое сообщение $M' = M_o||S$.

Соответственно, операция расшифрования на приемной стороне (получатель анализирует $M_п||S$) будет производиться с известной модификацией ключей:

$$H(M_o) \equiv (S)_{e_o} \bmod n_o.$$

Далее вычисляется $H(M_п)$. Если $H(M_o) = H(M_п)$, подпись верифицирована.

Если подписываемое сообщение $M(M')$ также должно передаваться в зашифрованном виде, то обычно M' шифруется на стороне отправителя стандартным образом: с помощью открытого ключа получателя ($e_п$ и $n_п$), который перед основным процессом верификации подписи расшифровывает послание своим тайным ключом: $d_п$ и $n_п$. Далее осуществляются вычисления и анализ, как и в первом случае.

ЭЦП на основе DSA

Алгоритм DSA (Digital Signature Algorithm – алгоритм цифровой подписи), или DSS (Digital Signature Standard – стандарт цифровой подписи), является одним из известных, нередко и сейчас применяемых. В алгоритме используются следующие параметры: p – простое число длиной от 64 до 1024 битов (число должно быть кратно 64); q – 160-битный простой множитель $(p - 1)$. Далее вычисляется число g:

$$g = v^{(p-1)/g} mod\ p,$$

где v – любое число, меньшее $(p - 1)$, для которого выполняется условие:

$$v^{(p-1)/g} mod\ p > 1.$$

Числа p, q, v могут использоваться группой лиц. Еще один элемент открытого ключа y вычисляется в соответствии с выражением

$$y \equiv g^x mod\ p,$$

где $x < q$; x – закрытый ключ.

Общая схема генерации и верификации ЭЦП приведена на рис. 3. Здесь $H(m)$ – хеш подписываемого сообщения. ЭЦП состоит из двух чисел: r и s. Число k здесь играет такую же роль, что и одноименный параметр в шифре Эль-Гамаля.

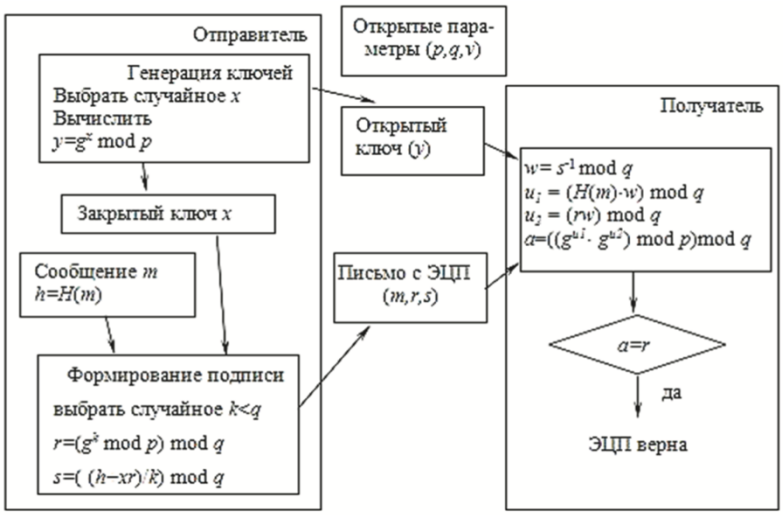

Рис. 3. Общая схема генерации и верификации ЭЦП DSA

ЭЦП Эль-Гамаля

Ключевая информация отправителя для ЭЦП создается аналогично другим криптографическим алгоритмам. Она состоит из тех же элементов, что и ключи в DSA. Основное отличие в применении расчетов состоит в том, что результатом зашифрования является только одна пара чисел, а не пара для каждого блока исходного сообщения. В данном случае таким сообщением является хеш подписываемого документа: $H(M_o)$.

Итак, ключевая информация отправителя: открытый ключ: y, g и p; тайный ключ: x. Чтобы подписать сообщение M_o, обладатель используемых для ЭЦП ключей должен выбрать, как и в предыдущей схеме, случайное число k, взаимно простое с $(p-1)$. Затем вычисляется числа a и b, являющиеся цифровой подписью ($S = \{a, b\}$):

$$a \equiv g_k \, mod \, p;$$

для вычисления b с помощью расширенного алгоритма Евклида решается уравнение

$$H(M_o) \equiv (xa + kb) \, mod \, (p-1).$$

Получателю отправляется сообщение $M' = M_o||S$.

Для верификации подписи вычисляется хеш полученного сообщения $H(M_п) = h$. Далее нужно убедиться, что выполняется равенство

$$y_a a_b \equiv g_h \, mod \, p.$$

Если равенство выполняется, подпись верифицируется.

ЭЦП Шнорра

Алгоритм ЭЦП К. Шнорра (К. Schnorr) является вариантом алгоритма ЭЦП Эль-Гамаля. В алгоритме ЭЦП Эль-Гамаля число p должно быть достаточно большим для усложнения задачи дискретного логарифма. Рекомендуемая длина p составляет минимум 1024 бита. Для уменьшения размера подписи Шнорр предложил новую схему с уменьшенным размером подписи.

Ключевая информация: p – простое число в диапазоне от 512 до 1024 битов; q –160-битное простое число, делитель $(p-1)$; любое число g $(g \neq 1)$ такое, что

$$g_q \equiv 1 \, mod \, p.$$

Числа p, g, q являются открытыми и могут применяться группой пользователей.

Выбирается число x $< q$ (x является тайным ключом) и вычисляется последний элемент открытого ключа:

$$y \equiv g^{-x} mod \, p.$$

Секретный ключ имеет длину не менее 160 бит.

Для подписи сообщения M_o выбирается случайное число k $(1 < k < q)$ и вычисляет параметр a:

$$a \equiv g_k mod \, p.$$

Далее вычисляется хеш от конкатенации сообщения M_o и числа a: $h = H(M_o||a)$. Обратим внимание, что хэш-функция непосредственно не применяется к сообщению. Создается хеш-образ подписываемого сообщения, спереди присоединенного к числу a. Далее вычисляется значение b:

$$b \equiv (k + xh) \, mod \, q.$$

Получателю отправляются $M' = M_o||S$; $S = \{h, b\}$.

Для проверки подписи получатель вычисляет

$$X \equiv g^{b} y^{h} (mod\ p).$$

Затем он проверяет выполнение равенства: $h = H(M_{п}||X)$. Подпись достоверна, если равенство выполняется.

Основные вычисления для генерации подписи могут производиться предварительно. Порядок величин x и h – около 140 двоичных разрядов, порядок числа k – около 70–72 разрядов. С учетом этого сложность операций умножения можно считать ничтожно малой по сравнению с модульным умножением в схеме RSA.

Лабораторное задание

Разработать реализацию одного из следующих алгоритмов генерации и верификации ЭЦП на выбор:

- DSA
- ЭЦП на основе Эль-Гамаля
- ЭЦП Шнорра