

Лабораторная работа № 10

Исследование алгоритмов генерации и верификации электронной цифровой подписи

Цель: изучение алгоритмов генерации и верификации электронной цифровой подписи и приобретение практических навыков их реализации

Задачи:

1. Закрепить теоретические знания по алгебраическому описанию и алгоритмам реализации операций генерации и верификации электронной цифровой подписи (ЭЦП).
2. Получить навыки практической реализации методов генерации и верификации ЭЦП на основе хеширования подписываемых сообщений и алгоритмов RSA, Эль-Гамала и Шнора, а также DSA.
3. Разработать приложение для реализации заданных алгоритмов генерации и верификации ЭЦП.
4. Оценить скорость генерации и верификации ЭЦП.
5. Результаты выполнения лабораторной работы оформить в виде описания разработанного приложения, методики выполнения экспериментов с использованием приложения и результатов эксперимента.

10.1 ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ

10.1.1 Определение, назначение, основные функции и типы ЭЦП

Электронная цифровая подпись (ЭЦП) является важным элементом современных информационных систем, использующих методы и технологии криптографического преобразования информации.

Остановимся на важнейших свойствах и иных информационных и фактологических характеристиках ЭЦП. Более подробные сведения из предметной области можно найти, например, в [2, 4, 29, 50].

Понятие «*электронная цифровая подпись*» было введено в 1976 году У. Диффи и М. Хеллманом.

После создания RSA разработаны алгоритмы цифровой подписи И. Рабина и Р. Меркле. В 1984 году Ш. Гольдвассер, С. Микали и Р. Ривест сформулировали требования безопасности к алгоритмам ЭЦП, описали атаки на ЭЦП.

Государственный стандарт РБ [50] определяет понятие ЭЦП в следующем виде.

Определение 1. 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:

- *аутентифицировать* лицо, подписавшее сообщение;
- *контролировать целостность* подписанного сообщения;
- *защищать* сообщение от подделок;
- *доказать авторство* лица, подписавшего сообщение, если это лицо отрицает свое авторство.

Важнейшими отличительными особенностям ЭЦП являются:

- 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 1, 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 (см. гл. 10 в [2]):

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

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

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

Во 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.

Определение 2. 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.

10.1.2 ЭЦП на основе хешей подписываемых сообщений

Классическая технология использования ЭЦП предусматривает подписание не самого сообщения (обозначим его здесь M_o), а его хеша, $H(M_o)$. 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 $M_o - M'$ – 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. 10.1.

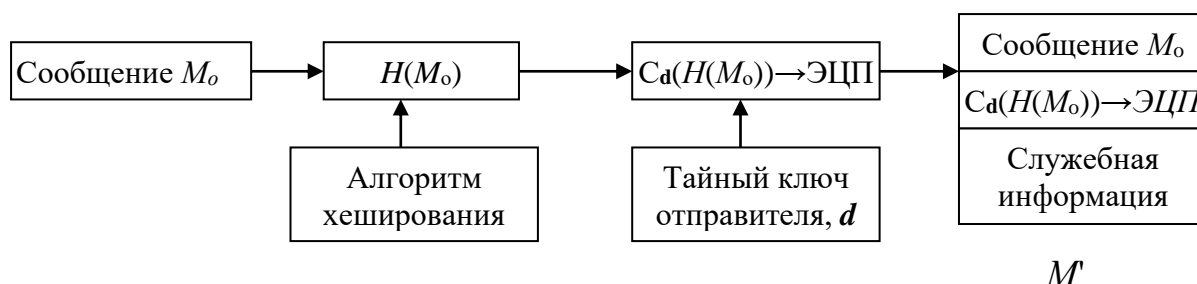


Рисунок 10.1. Пояснение к процедуре формирования ЭЦП и структуре подписанного документа

Важное свойство цифровой подписи заключается в том, что ее может проверить (верифицировать) каждый, кто имеет доступ к *открытому ключу* ее автора. На рис. 10.2 показан в общем виде порядок процесса верификации (без учета использования служебной информации). Заметим, что в общем случае версии исходного документа (M_o) и полученного (M_n) могут отличаться.

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

Из приведенных на рис. 10.1 и рис. 10.2 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 : $S = C_d(H(M))$;

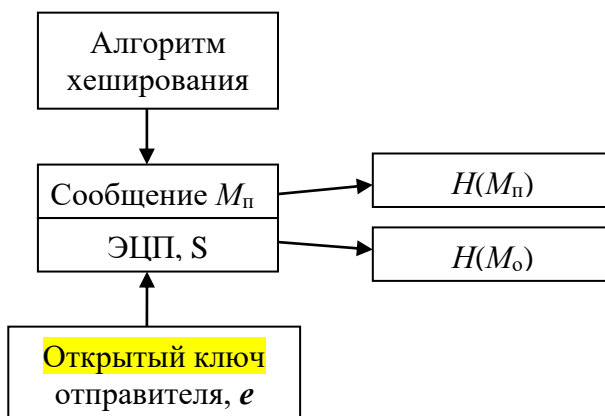


Рисунок 10.2 Пояснение к процедуре верификации ЭЦП

- 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, то есть разложения числа на простые множители,
- дискретного логарифмирования.

На основе первой задачи строится алгоритм RSA, на основе второй – алгоритмы, например, Эль-Гамала, DSA, Шнорра. Эти алгоритмы достаточно подробно рассмотрены в [2], глава 11. Здесь остановимся на кратком описании математических основ алгоритмов.

10.1.2.1 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.

Первый случай соответствует схеме и операциям, представленным на рис. 10.1 и рис. 10.2. При этом подпись S вычисляется на основе известного из лабораторной работы №8 соотношения (8.5):

$$S = (H(M_o))^{d_o} \bmod n_o \quad (10.1)$$

при указанном выше реверсе в отношении ключевой информации; в (10.1) d_o и n_o – элементы тайного ключа отправителя. Передаваемое сообщение $M' = M_o || S$.

Соответственно, операция расшифрования на приемной стороне (получатель анализирует $M_{||}S$) будет производиться в соответствии с формулой (8.6) с известной модификацией ключей:

$$H(M_o) = (S)^{e_o} \bmod n_o. \quad (10.2)$$

Далее вычисляется $H(M_{||})$. Если $H(M_o) = H(M_{||})$, 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 ($e_{||}$ и $n_{||}$), который перед основным процессом верификации подписи расшифровывает послание своим тайным ключом: $d_{||}$ и $n_{||}$. Далее осуществляются вычисления и анализ, как и в первом случае.

10.1.2.2 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 бит (число должно быть кратно 64); q – 160-битный простой множитель $p-1$. Далее вычисляется число g :

$$g = v^{(p-1)/q} \bmod p, \quad (10.3)$$

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

$$v^{(p-1)/q} \bmod p > 1.$$

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

$$y = g^x \bmod p. \quad (10.4)$$

где $x < q$; x – закрытый ключ.

Общая схема генерации и верификации ЭЦП приведена на рис. 10.3. Здесь $H(m)$ – хеш подписываемого сообщения. ЭЦП состоит из двух чисел: r и s . Число k здесь играет такую же роль, как и одноименный параметр в шифре Эль-Гамала.

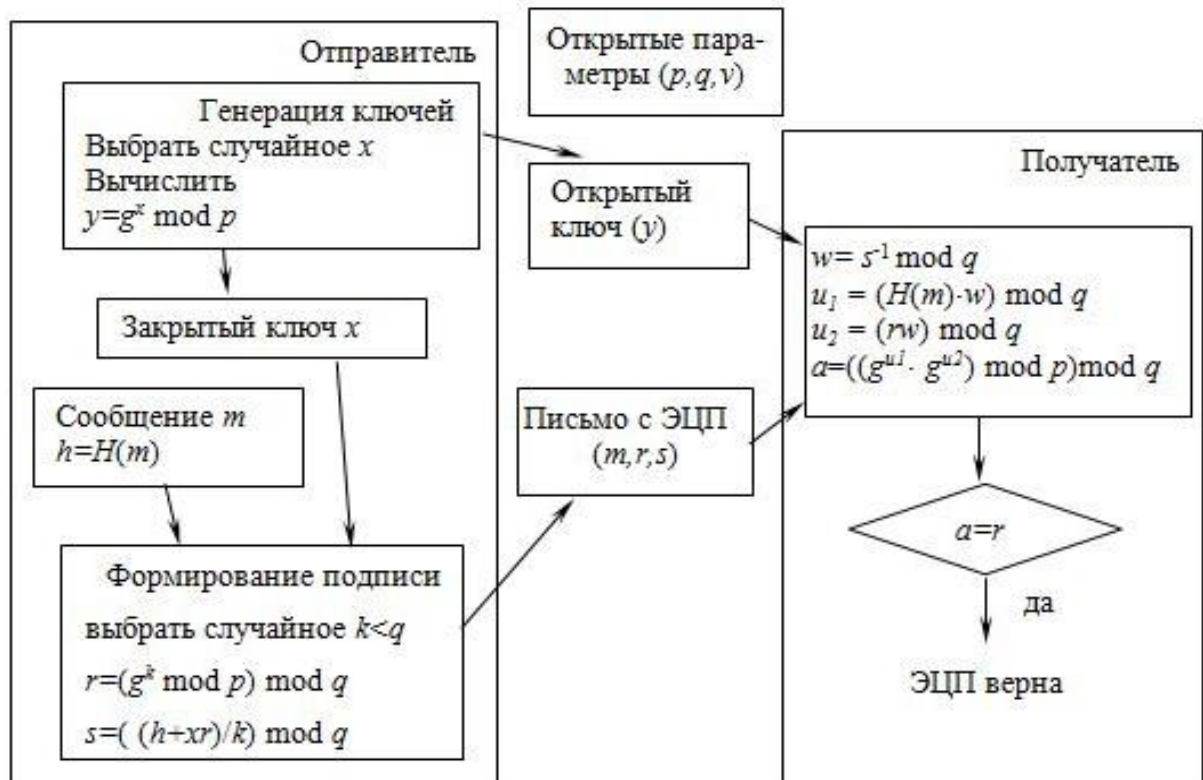


Рисунок 10.3 Общая схема генерации и верификации ЭЦП DSA

10.1.2.3 ЭЦП Эль-Гамала

Ключевая информация отправителя для ЭЦП создается точно так же, как это описано в материалах к ЛР №8. 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. Причем в рассматриваемом случае таким сообщением является хеш подписываемого документа: $H(M_0)$.

Итак, ключевая информация отправителя: открытый ключ: y , g и p ; тайный ключ: x . Чтобы подписать сообщение M_0 , 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 ($S = \{a, b\}$):

$$a = g^k \mod p; \quad (10.5)$$

для вычисления b с помощью расширенного алгоритма Евклида решается уравнение

$$H(M_0) = (xa + kb) \mod (p-1). \quad (10.6)$$

Получателю отправляется сообщение $M' = M_0 || S$.

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

$$y^a * a^b = g^h \pmod{p}. \quad (10.7)$$

Если равенство выполняется, подпись верифицируется.

10.1.2.4 ЭЦП Шнорра

Рассматриваемая схема является основой стандарта ЭЦП в Беларуси. Алгоритм ЭЦП К. Шнорра (K. Schnorr) является вариантом алгоритма ЭЦП Эль-Гамала.

Одной из особенностей ЭЦП Эль-Гамала является то, что число p должно быть очень большим, чтобы сделать действительно трудной проблему дискретного логарифма. Рекомендуется длина p , по крайней мере, должна составлять 1024 бита. Чтобы уменьшить размер подписи, Шнорр предложил новую схему, но с уменьшенным размером подписи.

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

$$g^q = 1 \pmod{p}. \quad (10.8)$$

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:

$$y = g^{-x} \pmod{p}. \quad (10.9)$$

Секретный ключ имеет длину не менее 160 бит.

Для подписи сообщения M_0 выбирается случайное число k ($1 < k < q$) и вычисляет параметр a :

$$a = g^k \pmod{p}. \quad (10.10)$$

Далее вычисляется хеш от канкатенации сообщения M_0 и числа a : $h = H(M_0 || a)$. Обратим внимание, что хэш-функция непосредственно не применяется к сообщению. Создается хеш-образ подписываемого сообщения, спереди присоединенного к числу a . Далее вычисляется значение b :

$$b = (k + xh) \pmod{q}. \quad (10.11)$$

Получателю отправляются $M' = M_0 || S$; $S = \{h, b\}$.

Для проверки подписи получатель вычисляет

$$X = g^b y^h \pmod{p}. \quad (10.12)$$

Затем он проверяет выполнение равенства: $h = H(M_{\text{п}}/X)$. 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.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ

1. Разработать авторское оконное приложение в соответствии с целью лабораторной работы. При этом можно воспользоваться результатами выполнения предыдущих лабораторных работ, а также доступными библиотеками либо программными кодами.

Приложение должно реализовывать следующие операции:

- генерацию и верификацию ЭЦП на основе алгоритмов RSA, Эль-Гамала и Шнорра;
- оценку времени выполнения указанных процедур при реальных (требуемых) ключевых параметрах.

Для вычисления хешей можно также воспользоваться доступными on-line-средствами, например, *katvin* (<https://katvin.com/tools/hash-generator.html>).

2. Для выполнения необходимых операций передачи (по сети)/верификации информации обменивайтесь открытой ключевой информацией с получателем подписанного сообщения для каждого исследуемого алгоритма (по согласованию с преподавателем).

3. Результаты оформить в виде отчета по установленным правилам.

ВОПРОСЫ ДЛЯ КОНТРОЛЯ И САМОКОНТРОЛЯ

1. Дать определение ЭЦП.
2. Охарактеризовать основные функции ЭЦП.
3. В чем заключаются сходства и различия между собственноручной и электронной подписью.
4. Охарактеризовать основные способы реализации ЭЦП.
5. Имеется ли различие в использовании ключевой информации при передаче зашифрованных сообщений и при передаче подписанных (ЭЦП) сообщений?
6. Охарактеризовать криптостойкость ЭЦП на основе RSA, схемы Эль-Гамала, схемы Шнорра, а также на основе DSA.
7. Какие элементы составляют ключевую информацию алгоритмов реализации ЭЦП, перечисленных в п.6?
8. Дать сравнительные характеристики схемам ЭЦП, перечисленным в п.6.

9. Охарактеризовать особенности государственного стандарта ЭЦП в Республике Беларусь.

К списку источников

50. СТБ 34.101.45-2013. Информационные технологии и безопасность. Алгоритмы электронной цифровой подписи и транспорта ключа на основе эллиптических кривых. – Минск: Госстандарт, 2013.
<http://apmi.bsu.by/assets/files/std/bign-spec29.pdf>