ЛАБОРАТОРНАЯ РАБОТА № 6

ЭЛЕКТРОННАЯ ЦИФРОВАЯ ПОДПИСЬ

Цель работы: ознакомление с принципами защищенного электронного документооборота в телекоммуникационных сетях и алгоритмами постановки электронной подписи.

Описание лабораторной работы. Обмен электронными документами по телекоммуникационным сетям существенно снижает затраты на обработку и хранение документов, ускоряется их поиск, однако при этом возникает проблема аутентификации, т.е. установления подлинности автора и отсутствия изменений в полученном документе.

При обработке документов в электронной форме непригодны традиционные способы установления подлинности по рукописной подписи и оттиску печати на бумажном документе, здесь принципиально новым решением является электронная подпись.

Электронная подпись — информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию[1].

Первая схема электронной цифровой подписи (ЭЦП)[2] — RSA была разработана еще в конце 1970-х годов, однако проблема подтверждения авторства стала актуальной настолько, что в 1990-х потребовалось установление стандарта. Причиной послужило повсеместное расширение глобальной сети Интернет и массовое распространение электронной торговли и оказания услуг. Именно по указанной причине стандарты ЭЦП в России и США были приняты практически одновременно, в 1994 г.

Из предложенных криптологами схем ЭЦП наиболее удачными оказались RSA и схема Эль-Гамаля. Первая из них была запатентована в США и в ряде других стран (патент на RSA прекратил свое действие совсем недавно). У второй схемы существует большое количество возможных модификаций, и все их запатентовать весьма затруднительно. Именно по этой причине схема ЭЦП Эль-Гамаля осталась по большей части свободной от патентов. Кроме того, эта схема имеет и определенные практические преимущества: размер блоков, которыми оперируют алгоритмы, и соответственно размер ЭЦП в ней

---

[1] Федеральный закон «Об электронной подписи» от 06.04.2011 № 63-ФЗ, принятый взамен ранее действовавшего ФЗ от 10.01.2002 «Об электронной цифровой подписи».

[2] Согласно упомянутому ФЗ № 63, понятия «электронная подпись» и «электронная цифровая подпись» считаются синонимами.

оказались значительно меньше, чем в RSA, при той же самой стойкости. Именно поэтому стандарты ЭЦП России и США базируются на схеме Эль-Гамаля.

Принцип построения ЭЦП. Асимметрия ролей отправителя и получателя в схемах ЭЦП требует наличия двух тесно связанных ключей: *секретного*, или ключа подписи, и *открытого*, или ключа проверки подписи.

Любая схема ЭЦП обязана определить три следующих алгоритма:

1) генерации ключевой пары для подписи и ее проверки;
2) постановки подписи;
3) проверки подписи.

Стандарты России и США очень похожи, они различаются лишь некоторыми числовыми параметрами и отдельными деталями выработки ключевой пары, вычисления и проверки подписи. Действительно, оба стандарта являются вариантами одной и той же схемы ЭЦП Эль-Гамаля.

ЭЦП используется для аутентификации текстов, передаваемых по телекоммуникационным каналам. Функционально она аналогична обычной рукописной подписи и обладает основными ее достоинствами:

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

ЭЦП представляет собой относительно небольшое количество дополнительной цифровой информации, передаваемой вместе с подписываемым текстом, и включает две процедуры:

1) процедуру постановки подписи, в которой используется секретный ключ отправителя сообщения;
2) процедуру проверки подписи, в которой используется открытый ключ отправителя.

Процедура постановки подписи. При формировании ЭЦП отправитель прежде всего вычисляет хэш-функцию $h(M)$ подписываемого текста M. Вычисленное значения хэш-функции $h(M)$ представляет собой один короткий блок информации m, характеризующий весь текст M в целом. Затем значение m шифруется секретным ключом отправителя. Получаемая при этом пара чисел представляет собой ЭЦП для данного текста M.

Процедура проверки подписи. При проверке ЭЦП получатель сообщения снова вычисляет хэш-функцию $m = h(M)$ принятого по каналу текста M, после чего при помощи открытого ключа отправителя проверяет, соответствует ли полученная подпись вычисленному значению m хэш-функции.

Принципиальным моментом в системе ЭЦП является невозможность подделки ЭЦП пользователя без знания его секретного ключа.

Каждая подпись, как правило, содержит следующую информацию:

- дата подписи;
- срок окончания действия ключа данной подписи;
- информация о лице, подписавшем текст;
- идентификатор подписавшего (имя открытого ключа);
- собственно цифровая подпись.

Однонаправленные хэш-функции. Хэш-функция предназначена для сжатия подписываемого документа M до нескольких десятков или сотен бит. Хэш-функция $h(.)$ использует в качестве аргумента сообщение M произвольной длины и возвращает хэш-значение $h(M) = H$ фиксированной длины. Обычно хэшированная информация является сжатым двоичным представлением основного сообщения произвольной длины. Следует отметить, что значение хэш-функции $h(M)$ сложным образом зависит от документа M и не позволяет восстановить сам документ M.

Хэш-функция должна удовлетворять целому ряду условий:

- быть чувствительной к всевозможным изменениям в тексте M;
- обладать свойством необратимости, т.е. задача подбора документа M_1, который обладал бы требуемым значением хэш-функции, должна быть вычислительно неразрешима;
- вероятность того, что значения хэш-функции двух различных документов совпадут, должна быть ничтожно мала.

Большинство хэш-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_i и хэш-значение H_{i-1} предыдущего блока текста (рис. 2.3).

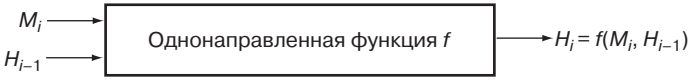

Рис. 2.3. Схема формирования хэш-функции

Алгоритм цифровой подписи DSA. Алгоритм цифровой подписи DSA (Digital Signature Authorization) предложен в 1991 г. в США и является развитием алгоритма цифровой подписи Эль-Гамаля.

Отправитель и получатель электронного документа используют при вычислении большие целые числа:

G, P — простые числа по *L*-бит каждое (*L* = 512 ... 1024 бит)*;*

q — простое число длиной 160 бит делитель числа (*P* – 1).

Числа *G, P, q* являются открытыми и могут быть общими для всех пользователей сети.

Описание алгоритма

1. Отправитель выбирает случайное целое число *X,* $1 < X < q$. Число *X* является *секретным ключом* отправителя для формирования электронной подписи.
2. Отправитель вычисляет значение

$$Y = G^X \bmod P.$$

Число *Y* является *открытым ключом* для проверки подписи отправителя и передается всем получателям документа.

3. Для того чтобы подписать документ *M*, отправитель хэширует его в целое хэш-значение *m:*

$$m = h(M),\ 1 < m < q.$$

Затем генерирует случайное целое число *K,* $1 < K < q$ и вычисляет число *r*:

$$r = (G^K \bmod P) \bmod q.$$

4. При помощи секретного ключа X отправитель вычисляет число *s*:

$$s = ((m + r \cdot X)K^{-1}) \bmod q.$$

Пара чисел *r*, *s* образуют цифровую подпись $S = (r, s)$ под документом *M*.

5. Доставленное получателю сообщение вместе с подписью представляет собой тройку чисел [*M*, *r*, *s*]. Прежде всего получатель проверяет выполнение соотношений:

$$0 < r < q;\ 0 < s < q.$$

6. Далее получатель вычисляет значения:

$$w = s^{-1} \bmod q;$$

$$m = h(M) \text{ — хэш-значение;}$$

$$u_1 = (m \cdot w) \bmod q;$$

$$u_2 = (r \cdot w) \bmod q.$$

Затем при помощи открытого ключа Y вычисляется значение

$$v = ((G^{u1} \cdot Y^{u2}) \bmod P) \bmod q$$

и проверяется выполнение равенства $v = r$. Если оно выполняется, то подпись признается подлинной, так как можно строго математически доказать, что последнее равенство будет выполняться тогда и только тогда, когда подпись $S = (r, s)$ под документом M получена при помощи именно того секретного ключа X, из которого был получен открытый ключ Y.

Алгоритм цифровой подписи RSA. Рассмотрим подробно процедуры постановки и проверки электронной подписи с использованием алгоритма RSA.

Сначала необходимо вычислить пару ключей (секретный ключ и открытый ключ). Для этого отправитель электронных документов вычисляет два больших простых числа P и Q, затем находит их произведение N = P × Q и значение функции Эйлера:

$$\varphi(N) = (P - 1) \times (Q - 1).$$

Далее отправитель вычисляет число E из условий:

$$1 < E \leqslant \varphi(N), \text{ НОД } (E, \varphi(N)) = 1$$

и число D из условий:

$$D < N, E \times D \equiv 1 \pmod{\varphi(N)}.$$

Пара чисел (E, N) является открытым ключом. Эту пару чисел автор передает партнерам по переписке для проверки его цифровых подписей. Число D сохраняется отправителем как секретный ключ для подписывания сообщения. Обобщенная схема формирования и проверки цифровой подписи RSA показана на рис. 2.4.

Допустим, что отправитель хочет подписать сообщение M перед его отправкой. Сначала сообщение M разбивается на блоки и преобразуют в целое число m.

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

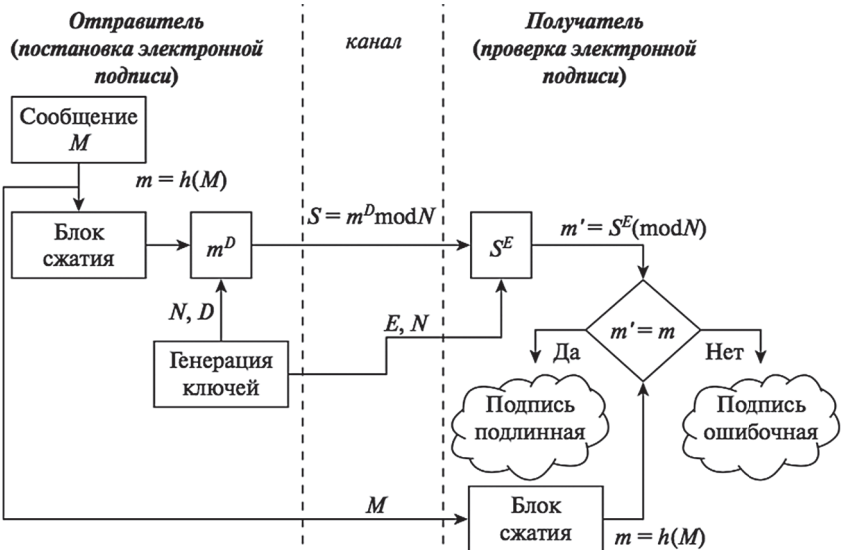

Рис. 2.4. Обобщенная схема формирования и проверки цифровой подписи RSA

$$S = m^D (\mathrm{mod}\ N).$$

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 восстанавливает значение m′, применяя криптографическое преобразование подписи S с использованием открытого ключа E:

$$m' = S^E (\mathrm{mod}\ N).$$

Задание

1. Ознакомиться с основными направлениями работ в рамках федеральной целевой программы «Электронная Россия», а также со сведениями о порядке использования и действующих алгоритмах постановки электронной цифровой, изложенными выше.

Запустить программу **labWork6.exe**, предназначенную для демонстрации порядка постановки и проверки электронной цифровой подписи.

2. Сгенерировать и переслать участникам обмена ключи для шифрования исходного документа и ключи для подписания документа. Исходный текст для шифрования набирается непосредственно в окне программы.
3. Зашифровать исходное сообщение и подписать его на секретном ключе отправителя.
4. Переслать зашифрованное и подписанное сообщение получателю. Выполнить проверку правильности ЭЦП и восстановить исходный текст сообщения.
5. Сохранить в отчете экранные формы, демонстрирующие процесс генерации и распространения ключей; процесс шифрования исходного документа и постановки ЭЦП.
6. Привести в отчете ответы на контрольные вопросы в соответствии с номером варианта (табл. 2.2).

Таблица 2.2

Номер варианта	Контрольные вопросы
1, 5, 7, 3, 9, 18, 28	В чем состоит назначение хэш-функций и какие требования предъявляются к хэш-функциям, используемым для постановки ЭЦП? Перечислите стандарты хэш-функций, действующие в Российской Федерации
2, 4, 6, 8, 20, 22, 24, 26, 30	Опишите процедуры постановки и проверки ЭЦП. Какая информация содержится в ЭЦП?
11, 13, 15, 10, 17, 19, 27	Перечислите стандарты ЭЦП, действующие в Российской Федерации. На каких принципах основана криптостойкость современных алгоритмов ЭЦП?
12, 14, 16 21, 23, 25, 29	Приведите пример реализации алгоритма ЭЦП (RSA, Эль-Гамаль, DSA)