# **ЛР №12 Криптография. Исследование алгоритмов генерации и верификации электронной цифровой подписи**

**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:

• аутентификацию 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.

**Функции ЭЦП** могут быть реализованы **на основе классических методов зашифрования/расшифрования**:

* на основе симметричных систем (с тайным ключом): по факту почти DES;
* на основе симметричных систем и посредника: 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;
* на основе асимметричных систем (с открытым ключом): сообщение, отправляемое получателю, шифруется тайным ключом отправителя. Отправитель же верифицирует подпись с помощью открытого ключа отправителя.

В нашем случае используется ключевая информация отправителя: открытый ключ – для зашифрования, тайный – для расшифрования.

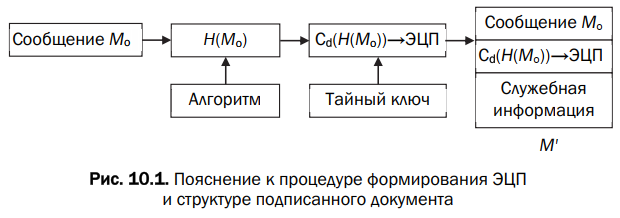
**Определение 2. Электронная цифровая подпись** – бинарная (или в ином виде) последовательность символов, являющаяся реквизитом электронного документа, зависящая от содержания этого документа и предназначенная для подтверждения целостности и подлинности электронного документа.

# **ЭЦП на основе хешей подписываемых сообщений**

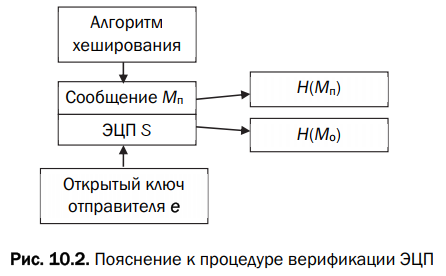
ЭЦП предусматривает подписание не самого сообщения (обозначим его здесь Мо), а его хеша, H(Mо).

**Общая структура подписанного электронного документа**

Мо – М' – представляет собой конкатенацию этого документа и ЭЦП S. Кроме этих двух элементов, документ может содержать некоторую служебную информацию, как это схематично показано на рис. 10.1.



Важное свойство цифровой подписи заключается в том, что ее может проверить (верифицировать) каждый, кто имеет доступ к открытому ключу ее автора.



Если в результате устанавливается равенство хешей: Н(Мп) = Н(Мо), то принимается решение о подлинности подписи и целостности документа Мп, т. е. это также означает, что Мп = Мо.

|  |  |
| --- | --- |
| **Отправитель**   * вычисляет хеш (хеш-образ) сообщения М: Н(М); * вычисляет содержание ЭЦП (собственно ЭЦП S) по хешу Н(М) с использованием своего закрытого ключа d: S =Сd(Н(М)); * присоединяет (конкатенирует) ЭЦП к сообщению М и некоторой служебной информации, создавая таким образом итоговое сообщение М'; * посылает сообщение М' получателю. | **Получатель**   * отделяет цифровую подпись S от сообщения М (для общего случая применим одинаковые символьные обозначения); * применяет к сообщению М 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. |

# **ЭЦП на основе RSA**

Здесь можно рассматривать две ситуации:

* сообщение Мo подписывается и передается **в открытом (незашифрованном) виде;**

Схемы 10.1-10.2. Подпись вычисляется по формуле с элементами тайного ключа отправителя. На стороне получателя анализ и вычисление хэша сообщения. Если H(Mo) = H(Mп), подпись верифицирована.

* сообщение Мo подписывается и передается **в зашифрованном виде**.

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

# **ЭЦП на основе DSA**

В алгоритме используются следующие параметры:  
*p* – простое число длиной от 64 до 1024 битов (число должно быть кратно 64);

*q –* 160-битный простой множитель (*р* – 1).

Далее вычисляется число *g*: *g = v*(*p* – 1)/*g* mod *p*, (10.3)  
где *v –* любое число, меньшее (*р* – 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 *у* вычисляется в соответствии с выражением

|  |  |
| --- | --- |
| *y* ≡ *gx* mod *p*,  где *x* < *q*; *х* – закрытый ключ. | (10.4) |

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, что и одноименный параметр в шифре Эль-Гамаля.



# **ЭЦП Эль-Гамаля**

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: Н(Mо).

Итак, ключевая информация отправителя: открытый ключ: y, g и р; тайный ключ: х.

Чтобы подписать сообщение Мо, обладатель используемых для ЭЦП ключей должен выбрать, как и в предыдущей схеме, случайное число k, взаимно простое с (р – 1).

Затем вычисляется числа а и b, являющиеся цифровой подписью (S = {a, b}):

a ≡ gk mod p; (10.5)

для вычисления b с помощью расширенного алгоритма Евклида решается уравнение

Н(Mо) ≡ (xa + kb) mod (p – 1). (10.6)

Получателю отправляется сообщение М' = Мо || S.

Для верификации подписи вычисляется хеш полученного сообщения Н(Мп) = h. Далее нужно убедиться, что выполняется равенство

yaab ≡ gh mod p. (10.7)

**Если равенство выполняется, подпись верифицируется.**

# **ЭЦП Шнорра**

Одной из особенностей ЭЦП Эль-Гамаля является то, что число p должно быть очень большим, чтобы сделать действительно трудной проблему дискретного логарифма. Рекомендуемая длина p должна составлять по крайней мере 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 битов; q –160-битное простое число, делитель (p – 1); любое число g (g ≠ 1) такое, что **gq ≡ 1 mod p. (10.8)**

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

Выбирается число х < q (х является тайным ключом) и вычисляется последний элемент открытого ключа: **y ≡ g–х mod p. (10.9)**

Секретный ключ имеет длину не менее 160 битов. Для подписи сообщения Мо выбирается случайное число k (1 < k < q) и вычисляет параметр а: **а ≡ gk mod p. (10.10)**

Далее вычисляется хеш от канкатенации сообщения Мо и числа **а: h = H(Mo||a).**

Создается хеш-образ подписываемого сообщения, спереди присоединенного к числу а. Далее вычисляется значение b: **b ≡ (k + xh) mod q. (10.11)**

Получателю отправляются М' = Мо||S; S = {h, b}.

Для проверки подписи получатель вычисляет **Х ≡ gbyh (mod p)**.

Затем он проверяет выполнение равенства: h = Н(Mп||Х). Подпись достоверна, если равенство выполняется.

Основные вычисления для генерации подписи могут производиться предварительно. Порядок величин х 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.