

## 7. Протоколы электронной цифровой подписи

7.1. Общие сведения.

7.2. Протокол на базе RSA.

7.3. Алгоритм цифровой подписи ГОСТ 34.10-94.

7.4. Алгоритм цифровой подписи ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012.

7.5. Разновидности ЭЦП.

7.6. Юридические основания использования ЭЦП.

Вопросы для самопроверки.

### 7.1. Общие сведения

Протоколы ЭЦП с одной стороны относят к протоколам аутентификации, т.к. гарантируют, что сообщение поступило от достоверного отправителя, а с другой стороны к протоколам контроля целостности, т.к. гарантируют, что сообщение пришло в неискаженном виде. Более того, получатель в дальнейшем может использовать ЭЦП как доказательство достоверности сообщения третьим лицам (арбитру) в том случае, если отправитель впоследствии попытается отказаться от него.

Говоря о схеме цифровой подписи, обычно имеют в виду следующую **классическую ситуацию** :

- отправитель знает содержание сообщения, которое он подписывает;
- получатель, зная открытый ключ проверки подписи, может проверить правильность подписи полученного сообщения в любое время без какого-либо разрешения и участия отправителя;
- безопасность схемы подписи гарантируется.

**Электронная цифровая подпись** – реквизит электронного документа, предназначенный для защиты данного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа ЭЦП и позволяющий *идентифицировать владельца* сертификата ключа подписи, а также *установить отсутствие искажения информации* в электронном документе.

**Электронная цифровая 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*.

**[Электронная цифровая] подпись** – строка бит, полученная в результате процесса формирования подписи (ISO/IEC 14888-1:2008 "Информационные технологии. Методы защиты. Цифровые подписи с приложением. Часть 1. Общие положения" и ГОСТ Р 34.10-2012 "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи").

При создании цифровой подписи по классической схеме отправитель:

- применяет к исходному сообщению **T** хеш-функцию **h(T)** и получает хеш-образ **r** сообщения;
- вычисляет цифровую подпись **s** по хеш-образу **r** с использованием своего закрытого ключа;
- посылает сообщение **T** вместе с цифровой подписью **s** получателю.

Получатель, отделив цифровую подпись от сообщения, выполняет следующие действия:

- применяет к полученному сообщению  $T$  хеш-функцию  $h(T)$  и получает хеш-образ  $r$  сообщения;
- расшифровывает хеш-образ  $r'$  из цифровой подписи  $s$  с использованием открытого ключа отправителя;
- проверяет соответствие хеш-образов  $r$  и  $r'$  и если они совпадают, то отправитель действительно является тем, за кого себя выдает, и сообщение при передаче не подверглось искажению.

Как видно из этой схемы, порядок использования ключей обратный тому, который используется при передаче секретных сообщений. Вначале отправитель использует свой закрытый ключ, а затем получатель применяет открытый ключ отправителя.

Существует несколько схем ЭЦП, которые, как правило, применяются совместно с определенными хеш-функциями. Некоторые из них приведены в таблице.

Таблица 7.1. Схемы ЭЦП

| Схема цифровой подписи   | Задача  | Хеш-функция  |
|--|---|--|
| RSA  | Разложение числа на множители                                   | MD4 или MD5 (Message Digest Algorithm - алгоритм краткого изложения сообщения, Р. Ривест)  |
| DSS (NIST <sup>1</sup> . FIPS Publication 186: Digital Signature Standard (DSS). May 1994)<br>DSS – Федеральный стандарт цифровой подписи США  | Дискретное логарифмирование                                     | SHA-1 (NIST. FIPS Publication 180: Secure Hash Standard (SHS). May 1993)<br>SHS – стандарт хэш-функции США<br>SHA - Secure Hash Algorithm – алгоритм хеш-функции |
| ECDSA (Elliptic Curve Digital Signature Algorithm) - алгоритм цифровой подписи на эллиптических кривых<br>Принят в качестве стандарта ISO <sup>2</sup> 14888-3 в 1998 г., ANSI <sup>3</sup> X9.62 – 1999 г., IEEE <sup>4</sup> 1363 – 2000 г. и NIST 186-2 – 2000 г.<br>(последняя редакция – NIST. FIPS Publication 186-3: Digital Signature Standard (DSS). June 2009) | Дискретное логарифмирование в группе точек эллиптической кривой | SHA (NIST. FIPS 180-3: Secure Hash Standard (SHS). October 2008)   |
| ГОСТ 34.10-94 (Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма)  | Дискретное логарифмирование                                     | ГОСТ 34.11-94 (Информационная технология. Криптографическая защита информации. Функция хэширования)  |
| ГОСТ Р 34.10-2001 (Информационная технология. Криптографическая защита информации. Процессы формирования и проверки  | Дискретное логарифмирование в группе точек эллиптической кривой | ГОСТ 34.11-94 (Информационная технология. Криптографическая защита   |

|   |   |   |
|---|---|---|
| электронной цифровой подписи)   |   | информации. Функция хэширования)  |
| ГОСТ Р 34.10-2012 (Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи) | Дискретное логарифмирование в группе точек эллиптической кривой | ГОСТ Р 34.11-2012 (Информационная технология. Криптографическая защита информации. Функция хэширования) |

Примечания.

<sup>1</sup>NIST - Национальный Институт стандартов и технологий, США (The National Institute of Standards and Technology).

<sup>2</sup>ISO - Международная организация по стандартизации (International Organization for Standardization).

<sup>3</sup>ANSI - Американский национальный институт стандартов (American National Standards Institute).

<sup>4</sup>IEEE - Институт инженеров по электротехнике и электронике (Institute of Electrical and Electronics Engineers).

## 7.2. Протокол на базе RSA

Этап 1. Выработка ключей (выполняет отправитель **A**) - см. лекцию "Шифрование с открытым ключом".

Этап 2. Отправка сообщения и электронной подписи (выполняет отправитель **A**).

Таблица 7.2. Отправка сообщения и ЭЦП на базе алгоритма RSA

| № п/п | Описание операции  | Пример                     |
|-------|--|----------------------------|
| 1     | Вычисление хеш-образа $h = h(T)$ , где <b>T</b> – исходное сообщение, <b>h(T)</b> – хеш-функция (для MD5 длина хеш-образа 128 бит).                        | $h = 7$                    |
| 2     | Выработка цифровой подписи $s = h^d \bmod n$ , где <b>d</b> – закрытый ключ отправителя <b>A</b> , <b>n</b> – часть открытого ключа отправителя <b>A</b> . | $s = 7^{29} \bmod 91 = 63$ |
| 3     | Отправка получателю <b>B</b> исходного сообщения <b>T</b> и цифровой подписи <b>s</b> .  |                            |

Этап 3. Получение сообщения и проверка электронной подписи (выполняет получатель **B**).

Таблица 7.3. Получение сообщения и проверка ЭЦП на базе алгоритма RSA

| № п/п | Описание операции  | Пример                  |
|-------|--|-------------------------|
| 1     | Вычисление хеш-образа по полученному сообщению $h' = h(T')$ , где <b>T'</b> – полученное сообщение.<br>Если $T = T'$ , то должно быть $h = h'$ . | $h' = 7$                |
| 2     | Вычисление хеш-образа из цифровой подписи $h = s^e \bmod n$ , где <b>e</b> и <b>n</b> – открытый ключ отправителя <b>A</b> .                     | $h = 63^5 \bmod 91 = 7$ |
| 3     | Т.к. $h' = h$ , то получатель <b>B</b> делает вывод, что полученное сообщение $T' = T$ и оно действительно отправлено <b>A</b> .                 |                         |

### 7.3. Алгоритм цифровой подписи ГОСТ 34.10-94

Алгоритм цифровой подписи ГОСТ 34.10-94 похож на DSS-94, вариация на тему алгоритмов Шнорра и Эль-Гамала.

Этап 1. Выработка ключей (выполняет отправитель **A**).

Таблица 7.4. Выработка ключей для ЭЦП по ГОСТ 34.10-94

| № п/п | Описание операции  | Пример                             |
|-------|--|------------------------------------|
| 1     | Выбор <b>p</b> - простого числа (для ГОСТ $509 < p < 512$ битов, либо $1020 < p < 1024$ битов).  | $p = 79$                           |
| 2     | Выбор <b>q</b> - простого числа - множителя $(p - 1)$ (для ГОСТ $254 < q < 256$ битов).  | $q = 13$                           |
| 3     | Выбор <b>a</b> - любого числа, меньшего $(p - 1)$ , для которого $a^q \bmod p = 1$ .   | $8^{13} \bmod 79 = 1$ ,<br>$a = 8$ |
| 4     | Выбор закрытого ключа <b>x</b> - числа, меньшего $q$ .   | $x = 4$                            |
| 5     | Вычисление открытого ключа $y = a^x \bmod p$ .   | $y = 8^4 \bmod 79 = 67$            |
| 6     | Публикация ключей.<br>Первые три параметра <b>p</b> , <b>q</b> и <b>a</b> - открыты и могут совместно использоваться пользователями сети,<br><b>y</b> – персональный открытый ключ для одного пользователя, <b>x</b> – персональный закрытый ключ отправителя <b>A</b> . |                                    |

Этап 2. Отправка сообщения и электронной подписи (выполняет отправитель **A**).

Таблица 7.5. Отправка сообщения и ЭЦП по ГОСТ 34.10-94

| № п/п | Описание операции   | Пример   |
|-------|---|--|
| 1     | Вычисление хеш-образа <b>h</b> = $h(T)$ (для ГОСТ длина хеш-образа 256 бит).  | $h = 7$  |
| 2     | Выбор <b>k</b> - любого числа, меньшего $q$ .   | $k = 11$   |
| 3     | Вычисление двух значений:<br>$w = a^k \bmod p$ и $w' = w \bmod q$ (для ГОСТ длина $w'$ 256 бит).<br>Если $w' = 0$ , перейти к этапу 2 и выбрать другое значение числа $k$ . | $w = 8^{11} \bmod 79 = 21$<br>$w' = 21 \bmod 13 = 8$ |
| 4     | Вычисление $s = (x w' + k h) \bmod q$ (для ГОСТ длина $s$ 256 бит).<br>Если $s = 0$ , перейти к этапу 2 и выбрать другое значение числа $k$ .                               | $s = (4 \cdot 8 + 11 \cdot 7) \bmod 13 = 5$          |
| 5     | Отправка получателю <b>B</b> исходного сообщения <b>T</b> и цифровой подписи ( <b>w'</b> , <b>s</b> ).  |  |

Этап 3. Получение сообщения и проверка электронной подписи (выполняет получатель **B**).

Таблица 7.6. Получение сообщения и проверка ЭЦП по ГОСТ 34.10-94

| №<br>п/п | Описание операции  | Пример  |
|----------|--|---|
| 1        | Вычисление хеш-образа по полученному сообщению $h' = h(T')$ .<br>Если $T = T'$ , то должно быть $h = h'$ .                       | $h' = 7$  |
| 2        | Вычисление $v = h'^{q-2} \bmod q$ .  | $v = 7^{11} \bmod 13 = 2$   |
| 3        | Вычисление двух значений:<br>$z_1 = (s \cdot v) \bmod q$ и $z_2 = ((q - w') \cdot v) \bmod q$ .                                  | $z_1 = (5 \cdot 2) \bmod 13 = 10$<br>$z_2 = ((13 - 8) \cdot 2) \bmod 13 = 10$ |
| 4        | Вычисление $u = ((a^{z_1} \cdot y^{z_2}) \bmod p) \bmod q$ .   | $u = ((8^{10} \cdot 67^{10}) \bmod 79) \bmod 13 = 8$                          |
| 5        | Т.к. $w' = u$ , то получатель <b>В</b> делает вывод, что полученное сообщение $T' = T$ и оно действительно отправлено <b>А</b> . |   |

#### 7.4. Алгоритм цифровой подписи ГОСТ Р 343.10-2001 и ГОСТ Р 34.10-2012

Алгоритмы цифровой подписи ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012 совпадают и похожи на ECDSA.

Этап 1. Выработка ключей (выполняет отправитель **А**) - см. Лекцию «Шифрование с открытым ключом».

Этап 2. Отправка сообщения и электронной подписи (выполняет отправитель **А**).

Таблица 7.7. Отправка сообщения и ЭЦП по ГОСТ 34.10-2001 (34.10-2012)

| №<br>п/п | Описание операции  | Пример  |
|----------|--|---|
| 1        | Вычисление хеш-образа $h = h(T)$ (для ГОСТ длина хеш-образа 256 бит).  | $h = 7$                                       |
| 2        | Вычисление $e = h \bmod q$ , где $q$ – часть открытого ключа отправителя <b>А</b> .  | $e = 7 \bmod 47 = 7$                          |
| 3        | Выбор $k$ - любого числа, меньшего $q$ .   | $k = 11$                                      |
| 4        | Определение точки эллиптической кривой $C(x_c, y_c) = k P(x_p, y_p)$ , где $P(x_p, y_p)$ – часть открытого ключа отправителя <b>А</b> .  | $C = 11 \cdot P(7, 17) = (16, 16)$            |
| 5        | Вычисление $r = x_c \bmod q$ .<br>Если $r = 0$ , перейти к этапу 2 и выбрать другое значение числа $k$ .   | $r = 16 \bmod 47 = 16$                        |
| 6        | Вычисление $s = (r \cdot d + k \cdot e) \bmod q$ , где $d$ - закрытый ключ отправителя <b>А</b> .<br>Если $s = 0$ , перейти к этапу 2 и выработать другое значение числа $k$ . | $s = (16 \cdot 10 + 11 \cdot 7) \bmod 47 = 2$ |
| 7        | Отправка получателю <b>В</b> исходного сообщения <b>Т</b> и цифровой подписи <b>(r, s)</b> .   |   |

Этап 3. Получение сообщения и проверка электронной подписи (выполняет получатель **В**).

Таблица 7.8. Получение сообщения и проверка ЭЦП по ГОСТ 34.10-2001 (34.10-2012)

| № п/п | Описание операции  | Пример  |
|-------|--|---|
| 1     | Вычисление хеш-образа по полученному сообщению $h' = h(T')$ .<br>Если $T = T'$ , то должно быть $h = h'$ .   | $h' = 7$  |
| 2     | Вычисление $e' = h' \bmod q$ .   | $e' = 7 \bmod 47 = 7$   |
| 3     | Вычисление $v = e'^{-1} \bmod q$ .<br>$(e' * e'^{-1}) \bmod q = 1$ .   | $e'^{-1} = 27$<br>$v = 27 \bmod 47 = 27$                                |
| 4     | Вычисление двух значений:<br>$z_1 = (s v) \bmod q$ и $z_2 = ((q - r) v) \bmod q$ .   | $z_1 = (2 * 27) \bmod 47 = 7$<br>$z_2 = ((47 - 16) * 27) \bmod 47 = 38$ |
| 5     | Определение точки эллиптической кривой $C'(x_c, y_c) = z_1 P(x_p, y_p) + z_2 Q(x_q, y_q)$ , где $Q(x_q, y_q)$ – часть открытого ключа отправителя <b>A</b> . | $C' = 7 P(7, 17) + 38 Q(36, 20) = (22, 26) + (11, 31) = (16, 16)$       |
| 6     | Вычисление $r' = x_c \bmod q$ .  | $r' = 16 \bmod 47 = 16$   |
| 7     | Т.к. $r' = r$ , то получатель <b>B</b> делает вывод, что полученное сообщение $T' = T$ и оно действительно отправлено <b>A</b> .                             |   |

### 7.5. Разновидности ЭЦП

Кроме классической схемы ЭЦП различают еще несколько **специальных** :

- схема "конфиденциальной" (неотвергаемой) подписи – подпись не может быть проверена без участия сгенерировавшего ее лица;
- схема подписи "вслепую" ("затемненной" подписи) - отправитель не знает подписанного им сообщения;
- схема "мультиподписи" - вместо одного отправителя сообщение подписывает группа из нескольких участников;
- схема "групповой" подписи - получатель может проверить, что подписанное сообщение пришло от члена некоторой группы отправителей, но не знает, кем именно из членов группы оно подписано. В тоже время, в случае необходимости, отправитель может быть определен;
- и др.

### 7.6. Юридические основания использования ЭЦП

В системах, где число пользователей исчисляется сотнями и тысячами, для проверки ЭЦП используются так называемые сертификаты ЭЦП (ЭП).

**Сертификат ЭЦП** – открытый ключ с некоторой дополнительной информацией о его владельце (регистрационный номер сертификата, ФИО владельца, срок действия и т.д.), подписанный ключом **Центра сертификации** (ЦС, Certificate Authority, СА, Удостоверяющий центр, УЦ).

**Сертификат ключа проверки электронной подписи** – электронный документ или документ на бумажном носителе, выданные УЦ либо доверенным лицом удостоверяющего центра и подтверждающие принадлежность ключа проверки ЭП владельцу сертификата ключа проверки ЭП.

**Квалифицированный сертификат ключа проверки электронной подписи** – сертификат ключа проверки ЭП, выданный аккредитованным УЦ или доверенным лицом аккредитованного УЦ либо федеральным органом исполнительной власти, уполномоченным в сфере использования ЭП.

При получении документа, подписанного ЭЦП, вначале подается запрос в ЦС, который высылает сертификат ЭЦП, информацию об окончании срока его действия или информацию об отсутствии сертификата. Если ЦС выслал сертификат, то считается, что документ послал именно тот, кто указан в сертификате. Для автоматизации деятельности ЦС применяется системы, называемые **системы поддержки инфраструктуры открытых ключей** (Public Key Infrastructure, PKI).

Впервые ссуда под ЭЦП (на покупку дома) была выдана в США 25 июля 2000г.

### **Вопросы для самопроверки**

1. Дайте определение понятию "электронная цифровая подпись".
2. Опишите последовательность действий участников протокола при отправке и проверке ЭЦП.
3. Какой порядок использования ключей (открытый; закрытый) при отправке и проверке ЭЦП?
4. Опишите схему протокола ЭЦП на основе алгоритма RSA.
5. Перечислите специальные схемы ЭЦП.
6. Назовите цель введения в действие Федерального закона "Об электронной цифровой подписи".

### **Практическая работа №2.3.**

#### **Электронная цифровая подпись (RSA, ГОСТы 34.10-94 и 34.10-2001)**

В практической работе необходимо привести последовательность выполнения процедур генерации и проверки ЭЦП с использованием следующих способов:

- на базе алгоритмы RSA;
- по ГОСТ 34.10-94;
- по ГОСТ 34.10-2001.

При оформлении отчета необходимо привести таблицы генерации ключей, отправки сообщения с ЭЦП и получения сообщения с ЭЦП. В качестве хеш-образа исходного сообщения  $h(T)$  принять коды, соответственно, 1-ой, 2-ой и 3-ей буквы своей фамилии согласно их положению в алфавите.