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 (Федеральный закон "Об электронной цифровой подписи" № 1-ФЗ от 10.01.2002г.).

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* (Федеральный закон "Об электронной подписи" № 63-ФЗ от 06.04.2011г.).

[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 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[1]. FIPS Publication 186: Digital Signature Standard (DSS). May 1994) DSS – Федеральный стандарт цифровой подписи США	Дискретное логарифмирование	SHA-1 (NIST. FIPS Publication 180: Secure Hash Standard (SHS). May 1993) SHS – стандарт хэш-функции США SHA - Secure Hash Algorithm – алгоритм хеш-функции
ECDSA (Elliptic Curve Digital Signature Algorithm) - алгоритм цифровой подписи на эллиптических кривых Принят в качестве стандарта ISO[2] 14888-3 в 1998 г., ANSI[3] X9.62 – 1999 г., IEEE[4] 1363 – 2000 г. и NIST 186-2 – 2000 г. (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	Дискретное логарифмирование	ГОСТ 34.11-94 (Информационная технология. Криптографическая защита

асимметричного криптографического алгоритма)		информации. Функция хэширования)
ГОСТ Р 34.10-2001 (Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи)	Дискретное логарифмирование в группе точек эллиптической кривой	ГОСТ 34.11-94 (Информационная технология. Криптографическая защита 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)

Протокол на базе RSA

Этап 1. Выработка ключей (выполняет отправитель **A**) – [см. лаб. раб. 3]

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

Таблица 2. Отправка сообщения и ЭЦП на базе алгоритма RSA

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

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

Таблица 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 **T'** – полученное сообщение. Если T = T', то должно быть h = h'.	h' = 7
2	Вычисление хеш-образа из цифровой подписи **h** = s^e mod n, где **e** и **n** – открытый ключ отправителя **A**.	h = 63^5 mod 91 = 7

3	Т.к. h' = h, то получатель **B** делает вывод, что полученное сообщение T’ = T и оно действительно отправлено **A**.	

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-Гамаля.

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

Таблица 4. Выработка ключей для ЭПЦ по ГОСТ 34.10-94

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

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

Таблица 5. Отправка сообщения и ЭЦП по ГОСТ 34.10-94

№ п/п	Описание операции	Пример
1	Вычисление хеш-образа **h** = h(T) (для ГОСТ длина хеш-образа 256 бит).	h = 7
2	Выбор **k** - любого числа, меньшего q.	k = 11
3	Вычисление двух значений: **w** = $a^k \bmod p$ и **w’** = w mod q (для ГОСТ длина w’ 256 бит). Если w’ = 0, перейти к этапу 2 и выбрать другое значение числа k.	$w = 8^{11} \bmod 79 = 21$ w’ = 21 mod 13 = 8

4	Вычисление **s** = (x w’ + k h) mod q (для ГОСТ длина s 256 бит). Если s = 0, перейти к этапу 2 и выбрать другое значение числа k.	s = (4*8 + 11*7) mod 13 = 5
5	Отправка получателю **B** исходного сообщения **T** и цифровой подписи (**w’**, **s**).	

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

Таблица 6. Получение сообщения и проверка ЭЦП по ГОСТ 34.10-94

№ п/п	Описание операции	Пример
1	Вычисление хеш-образа по полученному сообщению **h’** = h(T’). Если T = T’, то должно быть h = h’.	h' = 7
2	Вычисление **v** = $h'^{\,q-2}$ mod q.	$v = 7^{11} \bmod 13 = 2$
3	Вычисление двух значений: $\mathbf{z_1}$ = (s v) mod q и $\mathbf{z_2}$ = ((q – w’) v) mod q.	$z_1 = (5 * 2) \bmod 13 = 10$ $z_2 = ((13 – 8) * 2) \bmod 13 = 10$
4	Вычисление **u** = $((a^{z1} * y^{z2}) \bmod p) \bmod q$.	$u = ((8^{10} * 67^{10}) \bmod 79) \bmod 13 = 8$
5	Т.к. w’ = u, то получатель **B** делает вывод, что полученное сообщение T’ = T и оно действительно отправлено **A**.	

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 то же время, в случае необходимости, отправитель может быть определен;

Юридические основания использования ЭЦП

10 января 2002 г. Президент Российской Федерации В.В. Путин подписал Федеральный закон "Об электронной цифровой подписи" № 1-ФЗ. **Цель Федерального закона № 1-ФЗ** - обеспечение правовых условий использования ЭЦП в электронных документах, при соблюдении которых ЭЦП в электронном документе признается равнозначной собственноручной подписи в документе на бумажном носителе.

В настоящий момент действует Федеральный закон "Об электронной подписи" № 63-ФЗ от 06.04.2011 г. **Сфера действия (цель) Федерального закона № 63-ФЗ** - регулирует отношения в области использования электронных подписей при совершении гражданско-правовых сделок, оказании государственных и муниципальных услуг, исполнении государственных и муниципальных функций, при совершении иных юридически значимых действий, в том числе в случаях, установленных другими федеральными законами.

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, CA, Удостоверяющий центр, УЦ).

В Федеральном законе "Об электронной подписи" № 63-ФЗ от 06.04.2011 г. даны следующие определения.

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.

Задание на практическую работу.

Составить отчет о проделанной практической работе**.** В отчете **должны** содержаться **выполненные задания**, указанные ниже.

1) Ответить на контрольные вопросы

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".

2) Привести последовательность выполнения процедур генерации и проверки ЭЦП с использованием следующих способов:

- на базе алгоритма RSA;

- по ГОСТ 34.10-94;

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.