**Практическое занятие №7**

**Тема «Криптографическая защита информации»**

**Цель: изучить и закрепить умение реализации ЭЦП на примере RSA.**

**Теоретические сведения**

Чтобы документ приобрёл юридическую силу, его нужно подписать. Бумажные документы подписывают собственноручно, а для электронных используется **электронная цифровая подпись** (**ЭЦП**) — уникальная цифровая информация в виде комбинации символов. Из этой информации можно узнать, кто именно и когда подписал документ. Таким образом, электронная подпись — это официальный утверждённый законом аналог собственноручной подписи, который применяется для подписания электронных и заверения бумажных документов, преобразованных в электронный формат.

Технически электронная подпись отличается от рукописной, но она точно так же позволяет идентифицировать подписанта. Создаётся такая подпись с помощью специальных программных средств. Она всегда уникальна, её нельзя подделать. Когда электронный документ подписан ЭЦП, изменения или дополнения уже недоступны, поэтому и сам документ, его содержимое, подделать невозможно — только создавать новый.

# **Реализация элементов ЭЦП RSA**

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").

**Реквизит документа** - атрибут, характеризующий **документ** (например, наименование **документа**, автор, дата создания).

При создании цифровой подписи по классической схеме отправитель:

* применяет к исходному сообщению **T** хеш-функцию **h(T)** и получает хеш-образ r сообщения;

Хеш-функция — функция, осуществляющая преобразование массива входных данных произвольной длины в выходную битовую строку установленной длины, выполняемое определённым алгоритмом.

* вычисляет цифровую подпись **s по хеш-образу (результату хеш-функции) 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.

**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.

**Этап 1.** Выработка ключей (выполняет отправитель **А**) - см. практическую работу 6  "Шифрование методом RSA".

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

Отправка сообщения и ЭЦП на базе алгоритма RSA



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

Получение сообщения и проверка ЭЦП на базе алгоритма RSA



**Задание**

В практической работе необходимо объяснить последовательность выполнения процедур генерации и проверки ЭЦП.

Опишите последовательность действий участников протокола при отправке и проверке ЭЦП.

Опишите схему протокола ЭЦП на основе алгоритма RSA.

\*На базе алгоритма RSA получить ЭЦП (в проекте можно использовать существующие криптографические алгоритмы). Удостовериться, что ЭЦП принадлежит именно этому сообщению.

Оформите отчет. Запишите результаты выполнения задания и код полученной программы в отчет. Ответить на контрольные вопросы.

**Контрольные вопросы:**

1. Дайте определение понятию "электронная цифровая подпись".

2. Объясните какой порядок использования ключей (открытый; закрытый) при отправке и проверке ЭЦП.

3. Перечислите специальные схемы ЭЦП.