ТЕМА 7. Цифровая подпись

7.1. Требования к цифровой подписи

Аутентификация защищает двух участников, которые обмениваются сообщениями, от воздействия некоторой третьей стороны. Однако простая аутентификация не защищает участников друг от друга, тогда как и между ними тоже могут возникать определенные формы споров.

Например, предположим, что Джон посылает Мери аутентифицированное сообщение, и аутентификация осуществляется на основе общего секрета. Рассмотрим возможные недоразумения, которые могут при этом возникнуть:

- Мери может подделать сообщение и утверждать, что оно пришло от Джона.
- Джон может отрицать, что он посылал сообщение Мери.

В ситуации, когда обе стороны не доверяют друг другу, необходимо нечто большее, чем аутентификация на основе общего секрета. Возможным решением подобной проблемы является использование *цифровой подписи*. *Цифровая подпись* должна обладать следующими свойствами:

1. Должна быть возможность проверить автора, дату и время создания подписи.
2. Должна быть возможность аутентифицировать содержимое во время создания подписи.
3. Подпись должна быть проверяема третьей стороной для разрешения споров.

Таким образом, функция *цифровой подписи* включает функцию аутентификации.

На основании этих свойств можно сформулировать следующие требования к *цифровой подписи*:

1. Подпись должна быть битовым образцом, который зависит от подписываемого сообщения.
2. Подпись должна использовать некоторую уникальную информацию отправителя для предотвращения подделки или отказа.
3. Создавать *цифровую подпись* должно быть относительно легко.
4. Должно быть вычислительно невозможно подделать *цифровую подпись* как созданием нового сообщения для существующей *цифровой подписи*, так и созданием ложной *цифровой подписи* для некоторого сообщения.
5. *Цифровая подпись* должна быть достаточно компактной и не занимать много памяти.

Сильная хэш-функция, зашифрованная закрытым ключом отправителя, удовлетворяет перечисленным требованиям.

Существует несколько подходов к использованию функции *цифровой подписи*. Все они могут быть разделены на две категории: *прямые* и *арбитражные*.