Подпись

Опр.

Цифровая подпись (электронная подпись) – это математическая схема для аутентификации электронных сообщений или документов. Получается за счет криптографического преобразования информации с использованием закрытого ключа подписи и позволяющая проверить целостность, авторство и неотказуемость (факт подписания документа).

Составляющие:

* Алгоритм генерации ключа, который выбирает закрытий ключ равномерно случайно из множества возможных закрытых ключей. Результат: закрытый ключ и соответствующий открытый ключ.
* Алгоритм подписи, который по подписи и закрытому ключу, генерирует электронную подпись.
* Алгоритм верификации, который по сообщению, открытому ключу и электронной подпись, аутентифицирует сообщение.

Важно:

1. Аутентификация сигнатуры, сгенерированной из фиксированного сообщения и фиксированного закрытого ключа, может быть подтверждена соответствующим открытым ключом.
2. Невозможно вычислить и сгенерировать валидную сигнатуру без известного закрытого ключа.

DIGITAL SIGNATURE ALGORITHM (DSA)

Тройка алгоритмов (G,S,V)

G: key-generator

S: signing

V: verifying

Принципы:

* Можно сгенерировать открытый и закрытый ключи, так, чтобы зная открытый ключ нельзя было вычислить закрытый за разумное время. Механизм генерации является общеизвестным. При этом каждому открытому ключу соответствует определенный закрытый ключ.
* Имеются надежные методы шифрования, позволяющие зашифровать сообщение закрытым ключом так, чтобы расшифровать его можно было только открытым ключом. Механизм шифрования является общеизвестным.
* Если электронный документ поддается расшифровке с помощью открытого ключа и при этом получается валидный набор данных, то можно быть уверенным, что он был зашифрован с помощью соответствующего закрытого ключа.

При этом шифруется хеш документа. Фактически цифровой подписью является шифрованный хеш.

Алгоритм может быть:

* На основе симметричного шифрования.
* На основе асимметричного шифрования.

Симметричное шифрование предусматривает в системе наличие третьего лица – арбитра. Авторизацией документа является сам факт зашифрования его секретным ключом и передача его арбитру.

Замечание: Если хеш функция криптографически стойкая, то при верификации получить исходный текст будет вычислительно сложно.

В отличии от асимметричных алгоритмов шифрования, в которых шифрование производится с помощью открытого ключа, а расшифровка с помощью закрытого, в асимметричных схемах с цифровой подписью подписание производится с применением закрытого ключа, а проверка подписи с применением открытого.

## Ответы:

* Как формируется подпись?

Ответ:

Прогнать документ через хэш-функцию, затем закодировать получившийся хэш приватным ключом RSA. Получившаяся подпись поставляется с документом, вместе с публичным ключом. При этом на публичный ключ имеется сертификат, что он принадлежит автору.

Алгоритмы хеширования знать не нужно, только названия SHA2, SHA3, MD6, мб еще что

* Как проверяется подпись?

Ответ:

Подпись расшифровывается с публичным ключом. Документ прогоняется через такую же хэш-функцию, как при зашифровки. Сравниваем расшифрованную подпись и хэш. Если совпадают - все ок.