现代密码学

第四十四讲 数字签名的基本概念

信息与软件工程学院

第44讲数字签名基本概念

- 数字签名基本概念
- 数字签名的构成
- 数字签名安全需求

数字签名

- 数字签名是一种类似写在纸上的传统的物理签名。它使用公钥加密技术实现，用于鉴别数字信息或者签名者身份的方法。

- 数字签名必须保障：
  - （1）接收者能够核实发送者对文档的签名；
  - （2）发送者事后不能否认对文档的签名；
  - （3）不能伪造对文档的签名

数字签名载体

- 一个签名有消息和载体两个部分，即签名所表示的意义和签名的物理表现形式。

数字签名VS手写签名

- 传统手写签名中签名与文件是一个物理整体
  - 具有共同的物理载体
  - 物理上的不可分割、不可复制的特性
  - 签名与文件的不可分割和不能重复使用
- 数字签名中，签名与文件是电子形式
  - 没有固定的物理载体，即签名及文件的物理形式和消息已经分开
  - 电子载体是可以任意分割、复制的
  - 数字签名有可能与文件分割，被重复使用

- 传统签名的验证是通过与存档手迹对照来确定真伪的，它是主观的、模糊的、容易伪造的，从而也是不安全的。

- 数字签名则是用密码，通过公开算法可以检验的，是客观的、精确的，在计算上是安全的。

传统签名和数字签名的特点

- 传统签名的基本特点：
  - 能与被签的文件在物理上不可分割
  - 签名者不能否认自己的签名
  - 签名能被伪造
  - 容易被验证
- 数字签名是传统签名的数字化，基本要求：
  - 能与所签文件“绑定”
  - 签名者不能否认自己的签名
  - 签名不能被伪造
  - 容易被自动验证

第41讲 数字签名的构成

- 数字签名基本概念
- 数字签名的构成
- 数字签名安全需求

数字签名方案的构成

- 一个数字签名方案包括如下3个算法：
  - 密钥生成：产生用户的公私钥
  - 签名算法：产生消息的签名
  - 验证算法：验收消息的签名是否是合法

第41讲 数字签名的构成

- 数字签名基本概念
- 数字签名的构成
- 数字签名安全需求

数字签名的需求

- 数字签名方案为了实现安全认证，需要满足如下条件：
  - 必须相对容易生成该数字签名
  - 必须相对容易识别和验证该数字签名
  - 伪造该数字签名在计算上不可行，既包括对一个已有的数字签名构造新的消息，也包括对一个消息伪造一个数字签名