> 教材第十三章

- 数字签名具有认证功能
- 数字签名假设通信双方是不信任的；消息认证假设通信双方是信任的
- 给一个例子，要会**计算**（数字签名的生成及如何验证）
- 具体算法不用掌握，要了解不同算法的异同点

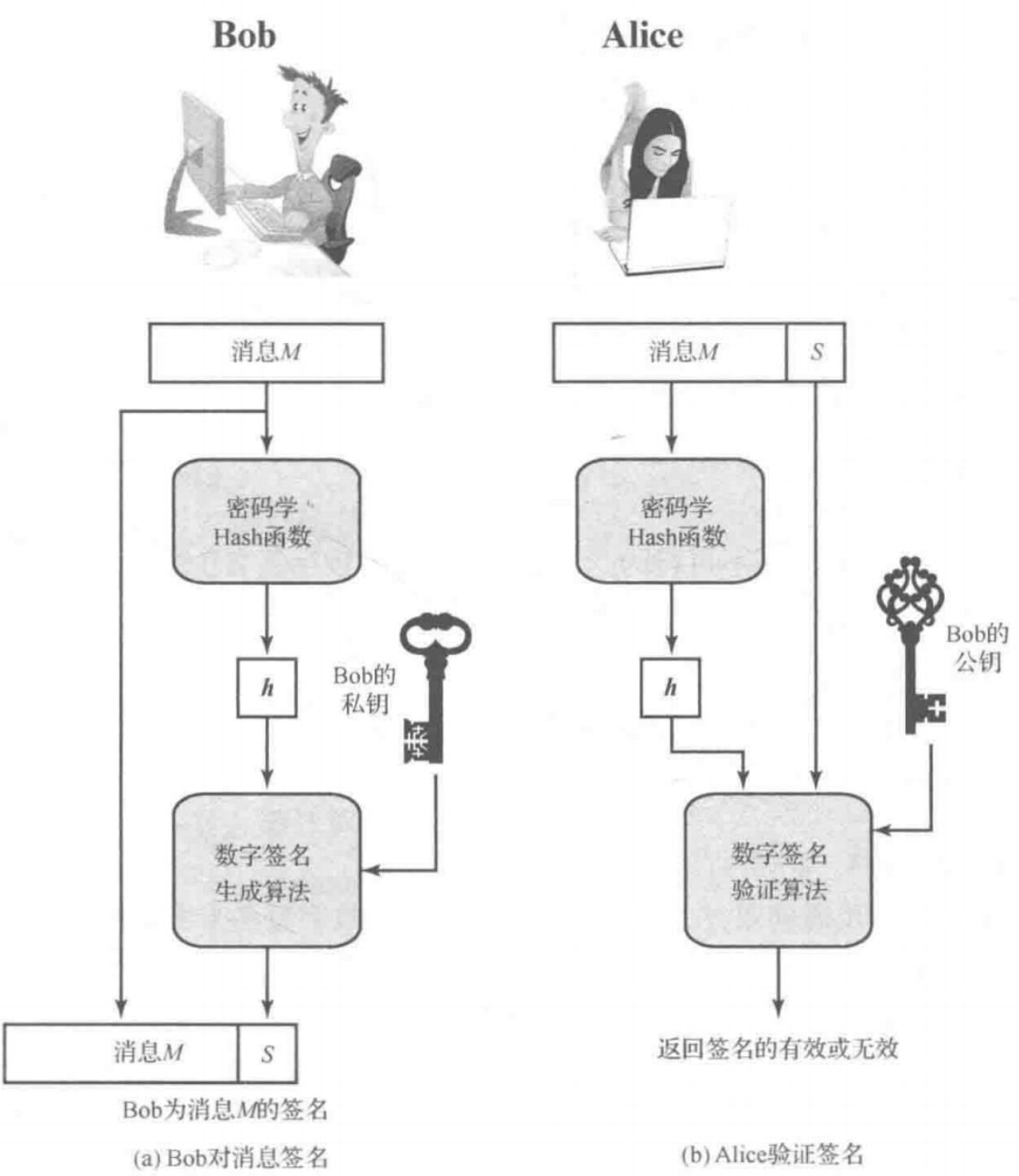

图 13.1　数字签名过程中关键部分的简单描述

上图可看出是对哈希码进行签名。

- 数字签名方案
    - Elgamal 数字签名方案
    - Schnorr 数字签名方案
    - DSA 方法

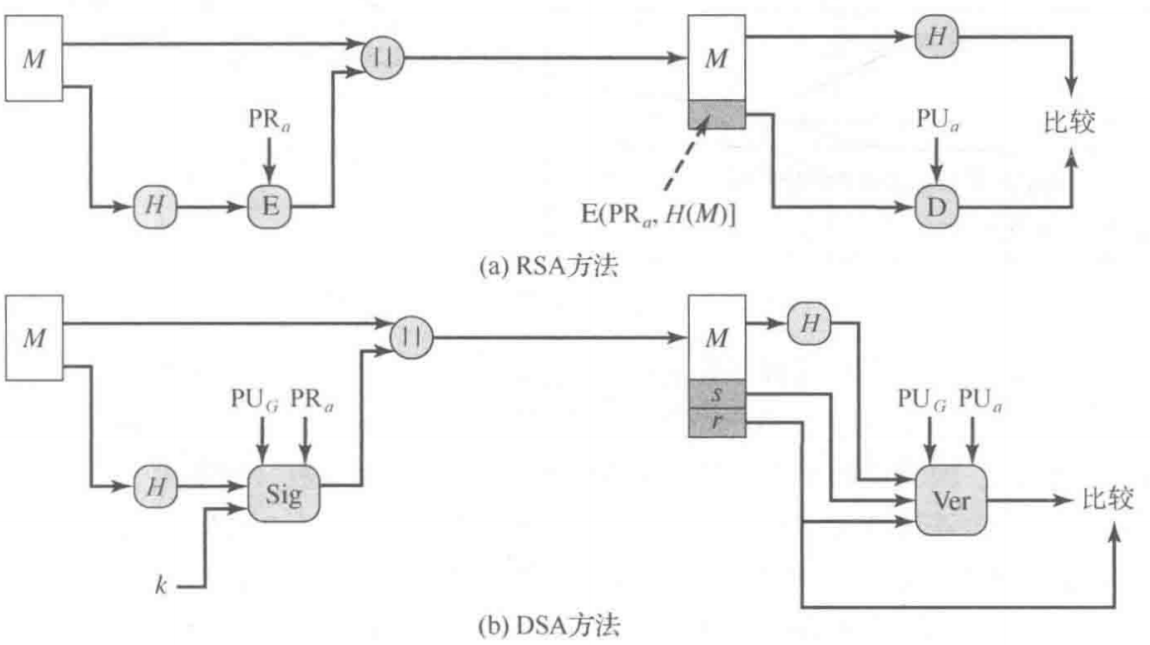

图 13.2　两种数字签名方法

- DSA 的公开参数的选择与 Schnorr 签名方案一样

思考题

13.1

> 列出消息认证中出现的两种争议。

发送方否认发过消息，接收方伪造消息。

13.2

> 数字签名应该具有哪些性质?

1. 能验证签名者、签名时间
2. 能验证被签名的内容
3. 签名由第三方仲裁

13.5

> 签名函数和保密函数应以何种顺序作用于消息？为什么?

先签名再加密。🤔 可以保护签名人：在签名之后又做了一层加密，即使第三方截获了这段消息，也没办法知道是谁发送的；也可以防止恶意更改签名：若先加密，再签名，第三方截获后可以用公钥去掉签名，并加上自己的签名。

13.6

> 直接数字签名方法中会遇到哪些威胁?

1. 发送方声称私钥丢失，否认自己发送过消息
2. X 的私钥可能在时刻 T 被盗用，到攻击者可用 X 的签名签发一条消息并加盖 T 或 T 之前的时间戳。

仲裁数字签名的操作如下。从发送者 X 到接收者 Y 的每个签名消息都首先到达仲裁者 A，仲裁者对该消息及其签名进行测试，以检查其来源和内容。然后将该消息标上时间戳并发送给 Y，同时注明消息已得到仲裁者的核实。