PART 10

数字签名

目 录 CONTENTS

10.1 数字签名简介

10.2 几个常见的数字签名算法

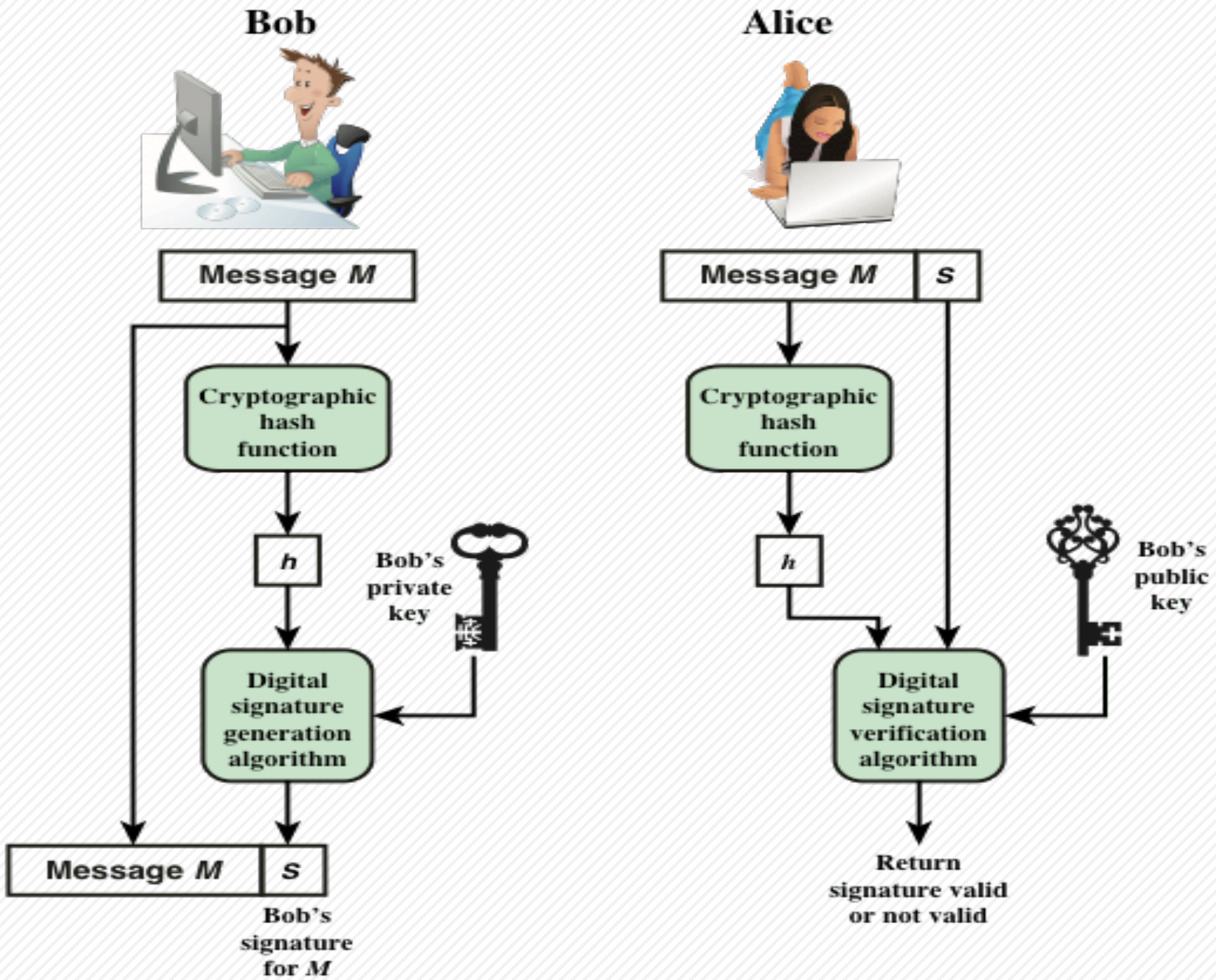
10.1 数字签名简介

- **手写签名**:Alice**对一个文档利用手写签名后，人们就可以验证她的签名，并且其他人很难模仿她的签名。**
- **数字签名**(digital signature)，**也称电子签名，就是对电子文档利用电子手段进行签名，电子签名必须至少具备手写签名的两个性质，即可验证性与不可伪造性。**

- 公钥密码体制可提供数字签名：

✓ 用私钥d对文档签名。

✓ 用公钥e对签名进行验证。



(a) Bob signs a message

(b) Alice verifies the signature

数字签名的基本概念

- 数字签名是一种以电子形式给一个消息签名的方法。
- 数字签名在ISO7498—2（Information processing systems）标准中定义为：“附加在数据单元上的一些数据，或是对数据单元所作的密码变换，这种数据和变换允许数据单元的接收者用以确认数据单元来源和数据单元的完整性，并保护数据，防止被人（例如接收者）进行伪造”。
- 数字签名主要用于对数字消息进行签名，以防消息的冒名伪造或篡改，也可以用于通信双方的身份鉴别。
- 简单说，数字签名是个加密的过程，数字签名的验证是一个解密的过程。

认证模型

- 密码学上，这种用私钥加密信息达到身份认证目的的运算称为“签名”。
- 基于公钥体制的身份认证基本原理：发送方A 使用自己的私钥pri签名（本质是加密运算）原始消息，将签名值S 与原始消息发送给接收方B。接收方B使用发送方A公开的密钥pub对签名值S进行验证（本质是解密运算），运算结果如果与接收到的原始消息一致，说明原始消息是使用与该公钥 pub 相匹配的私钥进行签名的。以此来保障了数据完整性、系统可用性、实体认证性和行为不可抵赖性。数字签名的目的是提供一个手写签名的数字化副本。

数字签名属性

- 它必须核实作者和签名的日期和时间
- 它必须在签名时对内容进行身份验证
- 为了解决争端，它必须能被第三方核查

数字签名要求

- 签名必须是依赖于被签名的消息的位模式
- 签名必须使用一些发送方特有的信息，以防止伪造和拒绝
- 生成数字签名必须相对容易
- 必须相对容易地识别和验证数字签名
- 伪造数字签名必须在计算上是不可行的，否则可以为现有的数字签名构造新的消息，也可以为给定的消息构造伪造的数字签名
- 在存储中保留数字签名的副本必须是可行的

数字签名主要方法与功能

- 数字签名是非对称密钥加密技术与数字摘要技术的应用，分为普通数字签名和特殊数字签名。
- 普通数字签名有RSA、EIGamal、Schnorr、椭圆曲线数字签名算法和有限自动机数字签名算法等。
- 特殊数字签名有不可否认签名、门限签名、盲签名、代理签名等。

主要功能：

(1)确认信息是由签名者发送的；

(2)确认消息自签名后到收到为止，未被修改过；

(3)签名者无法否认签名是由自己发送的。

数字签名的设计目标

- 签名的比特模式是依赖于消息报文的，也就是说，数据签名是以消息报文作为输入计算出来的，签名能够对消息的内容进行鉴别；
- 数据签名对发送者来说必须是惟一的，能够防止伪造和抵赖；
- 产生数字签名的算法必须相对简单易于实现，且能够在存储介质上保存备份；
- 对数字签名的识别、证实和鉴别也必须相对简单，易于实现；
- 伪造数字签名在计算上是不可行的，无论攻击者采用何种方法（利用数字签名伪造报文，或者对报文伪造数字签名）。

一个数字签名方案包括3个部分

(1) **密钥生成**:产生公钥与私钥如公钥密码体制;

(2) **签名算法**:利用私钥对文档签名;

(3) **验证算法**:利用公钥对签名进行验证。

数字签名的形式化定义

- **一个签名方案是一个5元组（M,A, K,S,V），满足如下的条件：**

（1）M是一个可能消息的有限集；

（2）A是一个可能签名的有限集；

（3）密钥空间K是一个可能密钥的有限集；

（4）对每一个k=（k1，k2）K，都对应一个签名算法Sig $\in_{K_2}$S和验证算法Ver $\in_{K_1}$V。

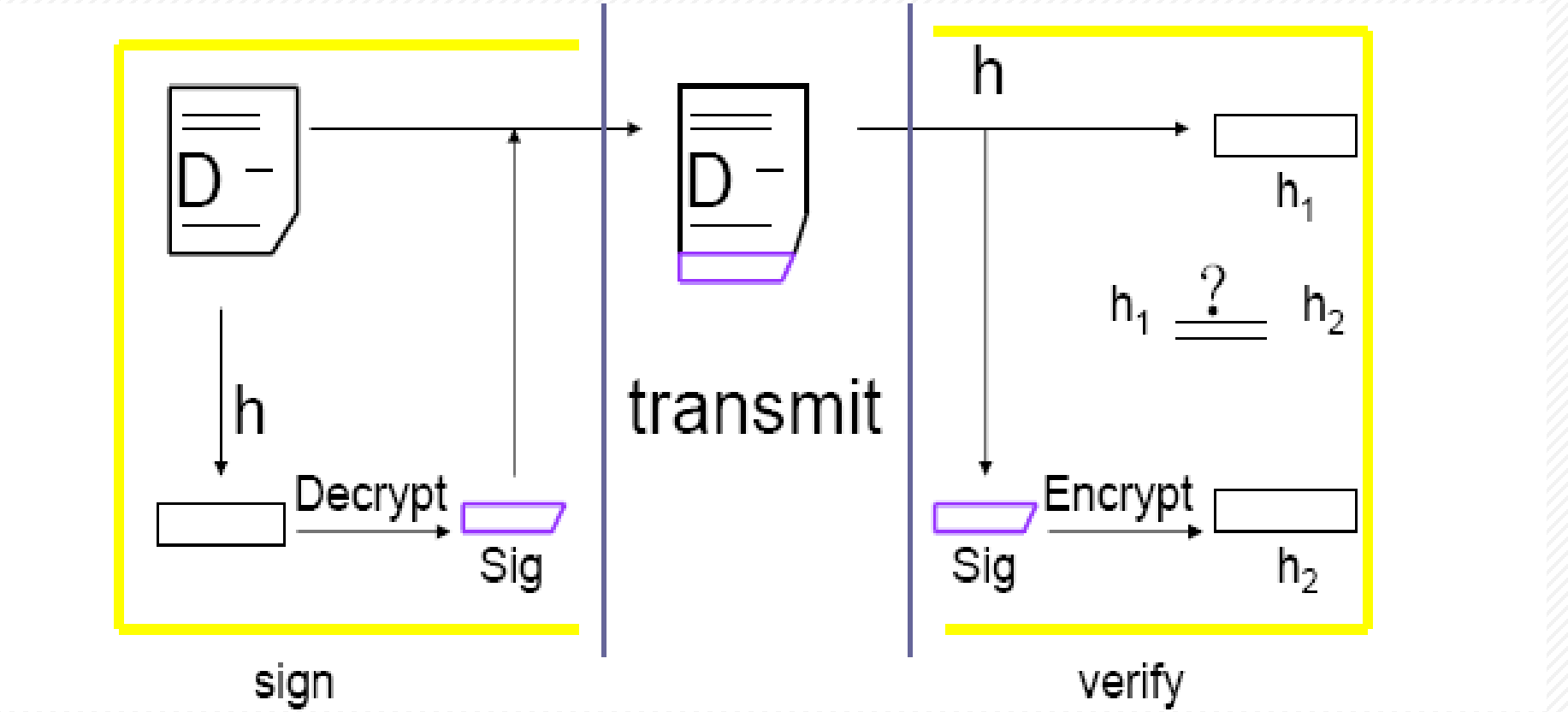
每一个Sig: M - >A和Ver: M - > A{TRUE ,FALSE}是一个对每一个消息x∈M和每一个签名y A满足下列方程的函数：

$$\text{Ver(x,y)}=\begin{cases} TRUE \text{当} y = Sig_{K_2}(x) \\ FALSE \text{当} y \neq Sig_{K_2}(x) \end{cases}$$

（5）对每一个k，函数Sig和Ver都是多项式时间可计算的函数。Ver是一个公开函数，k1称作公钥；而Sig是一个秘密函数，k2称作私钥，由用户秘密地保存。

利用公钥密码体制构造数字签名的方法

方法如下



10.2 几个常见的数字签名算法

RSA数字签名

- RSA数字签名是基于RSA公钥密码体制的签名方案。
- RSA公钥加密算法是一种非对称加密技术，它能够抵抗到目前为止已知的所有密码攻击，已被ISO推荐为公钥数据加密标准。
- RSA算法基于一个十分简单的数论事实：将两个大素数相乘十分容易，但那时想要对其乘积进行因式分解却极其困难，因此可以将乘积公开作为加密密钥。

注：ISO全称为International Standard Organized （国际标准化组织）

国际标准化组织（ISO）是由各国标准化团体（ISO成员团体）组成的世界性的联合会。制定国际标准工作通常由ISO的技术委员会完成。中国是ISO的正式成员，代表中国的组织为中国国家标准化管理委员会（Standardization Administration of China，简称SAC）。

RSA数字签名算法的实现

(1)秘密地选取两个大素数p和q。

(2)计算n=p*q，$\phi(n)=(p-1)(q-1)$ 。公开n，保密 $\phi(n)$

(3)随机地选取正整数1 < e < $\phi(n)$ ，满足gcd（e,$\phi(n)$）=1

(e为公开的密钥)

(4)计算d，满足d*e=1（mod （$\phi(n)$）） 。

(d为保密的密钥)

(5)签名变换：对于消息m$\in Z_n$，签名为Sig（m）= m^d mod n。

(6)签名验证：对于m，s $\in Z_n$，如果m=S^e mod n，则认为s为消息m的有效签名。

ElGamal数字签名方案

- ElGamal签名方案是由T.ElGamal于1985年提出的，其安全性主要基于有限域上离散对数问题的难解性。它是ElGamal公钥密码体制的直接应用。
- ElGamal的密钥和参数的产生过程如下：
- 它先选定一个足够大的素数 p， 然后在比p小的正数中选取一个随机数g和随机数x， 并且计算出$y= g^x(\mod p)$。然后，{y,g,p }作为公钥，而x则作为保密认证的私钥。
- 如果你想获取他人的私人信息，那么，你就必须在已知 {y,g, p} 的情况下计算出x(当然，如果要获得明文，还必须攻破或获取签名时使用的Hash函数)。

ElGamal数字签名方案及其一般化的模型

系统参数：设p是一大素数，g是Z的一个生成元，定义

K={（p,g,y,x）:$y= g^x \bmod p$}其中$x\in Z$。

公开密钥 y,p,g ； 私有密钥 x

签名算法：对于K=（p,g,y,x）、随机数$k\in Z$和待签消息m,定义Sig(x,k)=(r,s). 这里的$r=g^k \bmod p$； $s=(m-xr)k^{-1} \bmod (p-1)$.

（r,s）即为生成的签名。

验证算法：Ver(m,r,s)=TRUE

$$y^r r^s = g^m \bmod p$$

注：1.Elgamal数字签名每次签名中的k应选择不同,否则有可能私钥a能被计算出。

2.Elgamal数字签名没有RSA数字签名的效率高，并且有两倍的消息扩张。

3.Elgaml数字签名有很多种变形。

4.存在Elgamal数字签名的变形在某些假设下能被证明在选择消息攻击下是安全的。

5.就像Elgamal密码体制一样,Elgamal数字签名也可以推广到合适的循环群中。

Schnorr数字签名方案

- **系统参数**

(1) 选择素数p、q，使得q是p-1的素因子；

(2) 选择整数g，使得 $g^q=1 \bmod p$. 值g、p和q构成全局公钥参数，在用户组内的每个用户都可以取此值。

(3) 选择随机整数 x，$0<x<q$，作为用户的私钥。

(4) 计算$y= g^x \bmod p$,作为用户公钥。

- **签名算法**

对于待签消息$m \in Z$，选择随机数$k(1<k<q)$,计算$r=g^k \bmod p$, $e=h(r,m)$, 从签名方程 $s=k-xe \bmod q$ 中计算出s，消息对（e,s）即为生成的签名。

- **验证算法**

收方在收到消息m和数字签名(e,s)后, 计算$r'=g^s y^e \bmod p$, 则

$$Ver(m,(e,s))=TRUE$$

$$h(r',m)=e$$

Schnorr数字签名方案的安全性分析

(1) EIGAMAL系统中 g 为Z_p中的本原元，而于Schnorr系统中则不是。从安全的角度来看，EIGAMAL安全性较高,这是因为本原元的阶为 p-1 ，而Schnorr系统中g的阶为q(>2^{160})，在此阶下，基于离散对数问题的体制是否安全有待进一步研究。

(2) Schnorr系统的签名文较短，e的长度由函数h决定。s的长度小于|q|。若h的输出长度为128位，|q|为160位，则其签名长度为288位，比EIGAMAL系统的小。

(3) Schnorr首先提出r= g^kmod p可以事先计算，由于 k 是与 m 无关的随机数，故Schnorr系统在签名中只需一次乘法及减法(模运算)，比EIGAMAL系统快很多。因此，Schnorr数字签名方案特别适合于智能卡的应用。


海南大学
Hainan university