密 码 学

第十一讲　数字签名（1）

张焕国

武汉大学计算机学院

空天信息安全与可信计算教育部重点实验室

内容简介

第一讲 信息安全概论
第二讲 密码学的基本概念
第三讲 数据加密标准（DES）
第四讲 高级数据加密标准（AES）
第五讲 中国商用密码（SMS4）
第六讲 分组密码的应用技术
第七讲 序列密码
第八讲 复习
第九讲 公钥密码（1）

内容简介

第十讲 公钥密码（2）

第十一讲 数字签名（1）

第十二讲 数字签名（2）

第十三讲 HASH函数

第十四讲 认证

第十五讲 密码协议

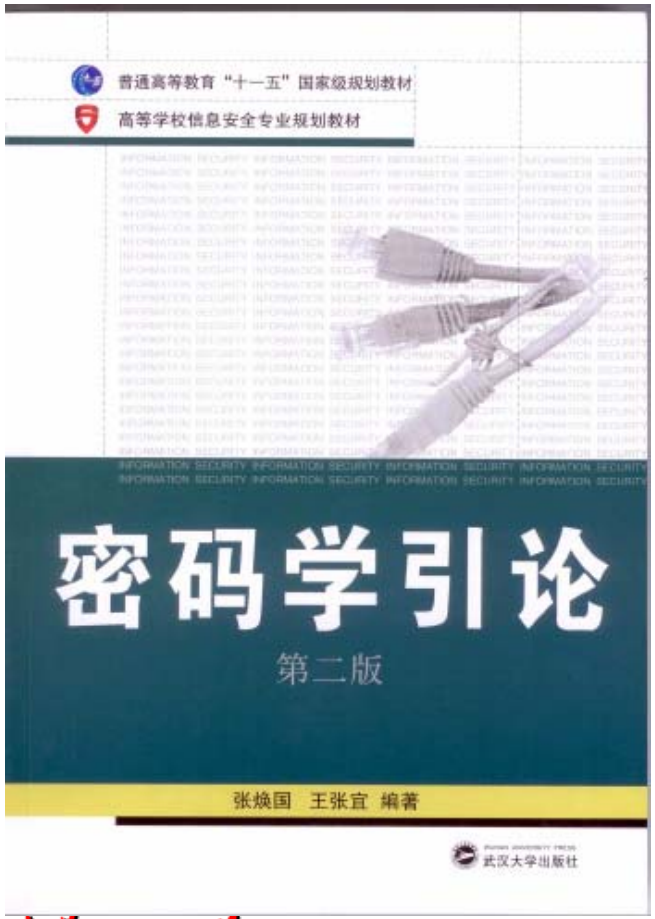
第十六讲 密钥管理（1）

第十七讲 密钥管理（2）

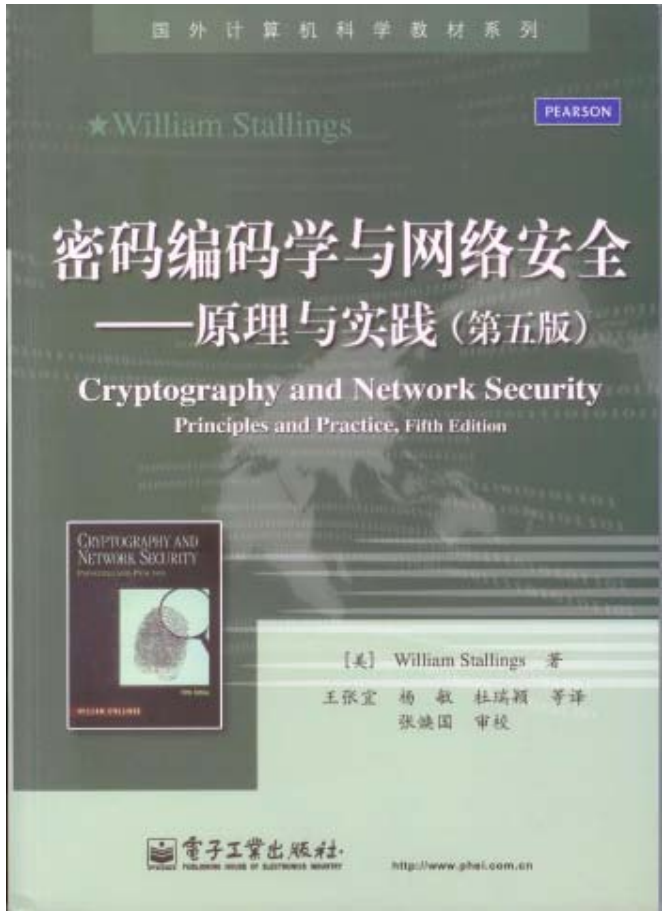
第十八讲 复习

教材与主要参考书

教材



参考书



一、数字签名的基本概念

①在人们的工作和生活中，许多事物的处理需要当事者签名。

②签名起到确认、核准、生效和负责任等多种作用。

③签名是证明当事者的身份和数据真实性的一种信息。

④签名可以用不同的形式来表示。

一、数字签名的基本概念

⑤在传统的以书面文件为基础的事物处理中，采用书面签名的形式：

手签、印章、手印等

⑥书面签名得到司法部门的支持。

⑦在以计算机文件为基础的现代事物处理中，应采用电子数字形式的签名，即数字签名（**Digital Signature**）。

⑧数字签名已得到中国和其它一些国家的法律支持。

一、数字签名的基本概念

⑨一种完善的签名应满足以下三个条件：

- 签名者事后不能抵赖自己的签名；
- 任何其他人不能伪造签名；
- 如果当事的双方关于签名的真伪发生争执，能够在公正的仲裁者面前通过验证确认其真伪。

一、数字签名的基本概念

⑩数字签名基于密码技术，其形式是多种多样的：

通用签名、仲裁签名、盲签名、群签名、门限签名，代理签名等。

- 1994年月美国政府正式颁布了美国数字签名标准DSS（Digital Signature Standard）。
- 1995年我国也制定了自己的数字签名标准（GB15851－1995）。
- 2004年我国颁布了《中华人民共和国电子签名法》。

二、数字签名的模型

- 一个数字签名体制包括两个方面的处理：
  - 施加签名
  - 验证签名。
- 设施加签名的算法为SIG，产生签名的密钥为K，被签名的数据为M，产生的签名信息为S，则有

$$S = \mathrm{SIG}(M, K)$$

二、数字签名的模型

- 设验证签名的算法为 **VER** ，用**VER**对签名**S**进行验证，可鉴别 **S**的真假。即

$$\mathrm{VER}(S, K) = \begin{cases} \text{真，当} S = \mathrm{SIG}(M, K) \\ \text{假，当} S \neq \mathrm{SIG}(M, K) \end{cases}$$

二、数字签名的模型

- 签名函数必须满足以下条件，否则文件内容及签名被篡改或冒充时均无法发现：

① 当$M' \neq M$时，有$SIG(M', K) \neq SIG(M, K)$。

- 条件①要求签名S至少和被签名的数据M一样长。当M太长时，应用很不方便。
- 将条件①改为：虽然当$M' \neq M$时，存在$S = S'$，但对于给定的M或S，要找出相应的M'在计算上是不可能的。

二、数字签名的模型

② 签名 S 只能由签名者产生，否则别人便可伪造，于是签名者也就可以抵赖。

③ 收信者可以验证签名S的真伪。这使得当签名S为假时收信者不致上当。

④ 签名者也应有办法鉴别收信者所出示的签名是否是自己的签名。这就给签名者以自卫的能力。

三、利用公钥密码实现数字签名

1、一般方法

- 对于一个公钥密码，如果满足

$$E(D(M, K_d), K_e) = M$$

则可确保数据的真实性。

- 凡是能够确保数据真实性的公钥密码都可用来实现数字签名。例如：
  - RSA密码
  - ElGamal密码
  - 椭圆曲线密码
  - 其它密码

三、利用公钥密码实现数字签名

1、一般方法：

- 为了实施数字签名，应成立管理机构；
  - 制定规章制度，
  - 统一技术标准，
  - 用户登记注册，
  - 纠纷的仲裁，
  - 其它。

三、利用公钥密码实现数字签名

1、一般方法

● 签名通信协议： $A \xrightarrow{M} B$

① A用自己的解密钥 K_{dA}对数据 M进行签名：

$$S_A = D(M, K_{dA})$$

②如果不需要保密，则 A直接将 S_A 发送给用户B。

③如果需要保密，则A用B的公开的加密钥K_{eB} 对 S_A 加密，得到密文C，

$$C = E(S_A, K_{eB})$$

④最后，A把 C发送给 B，并将 S_A或 C 留底。

三、利用公钥密码实现数字签名

⑤B收到后，若是不保密通信，则用A的公开加密钥K_{eA}对签名进行验证：

$$E(S_A, K_{eA}) = E(D(M, K_{dA}), K_{eA}) = M$$

⑥若是保密通信，则B先用自己的保密的解密钥K_{dB}对C解密，然后再用A的公开加密钥K_{eA}对签名进行验证：

$$D(C, K_{dB}) = D(E(S_A, K_{eB}), K_{dB}) = S_A$$

$$E(S_A, K_{eA}) = E(D(M, K_{dA}), K_{eA}) = M$$

⑦如果能够恢复出正确的M，则说明S_A是A的签名，否则S_A不是A的签名。

⑧B对受到的C或S_A留底。

三、利用公钥密码实现数字签名

- 签名通信协议安全分析：

① 因为只有A才拥有K_{dA}，而且由公开的K_{eA}在计算上不能求出保密的解密钥K_{dA}。因此签名的操作只有A才能进行，任何其他人都不能进行。所以，K_{dA}就相当于A的印章或指纹，而S_A就是A对M的签名。对此A不能抵赖，任何其他人不能伪造。

② 事后如果A和B关于签名的真伪发生争执，则他们应向公正的仲裁者出示留底的签名数据，由仲裁者当众验证签名，解决纠纷。

三、利用公钥密码实现数字签名

- 签名通信协议的问题：

①验证签名的过程就是恢复明文的过程。而B事先并不知道明文M，否则就用不着通信了。那末B怎样判定恢复出的M是否正确呢？

②怎样阻止B或A用A以前发给B的签名数据，或用A发给其他人的签名数据来冒充当前A发给B的签名数据呢？

- 仅仅靠签名本身并不能解决这些问题。

三、利用公钥密码实现数字签名

- 解决问题的一种办法：

①合理设计明文的数据格式：

发方标识	收方标识	报文序号	时间	数据	纠错码

M=< A，B，I，T，DATA，CRC >

②记 其中 H = < A，B，I，T > 。

于是，A以 < H，SIG(M,K_{dA}) > 为最终报文发给B，其中H为明文形式。

三、利用公钥密码实现数字签名

- 解决问题的一种办法：

③只要用A的公钥验证签名并恢复出正确的附加信息 $H = <A, B, I, T>$，便可断定明文M是否正确。

④设附加信息 $H=<A, B, I, T>$ 的二进制长度为 L，则错判概率

$$p_e \leqslant 2^{-L}。$$

三、利用公钥密码实现数字签名

- 改进：
  - 保留上述方法的报头处理，数据签名改为：对Hash（M）签名，而不直接对M签名。

数据 M	Hash(M)

S ＝ SIG (Hash（M）, K_{dA})

传输格式：< M，S >

数据 M	签名S

  - 设收到的数据为< M' ， S' >，仅当Hash(M')=E(S',K_{eA})且报头是正确时，判定M是正确的。

三、利用公钥密码实现数字签名

2、利用RSA密码实现数字签名：

- 对于RSA密码

$$D(E(M))=(M^e)^d=M^{ed}=(M^d)^e=E(D(M)) \bmod n ,$$

所以RSA可同时确保数据的秘密性和真实性。

- 因此利用RSA密码可以同时实现数字签名和数据加密。

三、利用公钥密码实现数字签名

2、利用RSA密码实现数字签名：

⑴、签名算法

- 设M为明文，K_{eA}=<e,n>是A的公开加密钥，

  K_{dA}=<d,p,q, $\phi(n)$>是A的保密的解密钥，

则A对M的签名过程是，

$$S_A = D(M, K_{dA}) = (M^d) \bmod n$$

S_A便是A对M的签名。

- 验证签名的过程是，

$$E(S_A, K_{eA}) = (M^d)^e \bmod n = M$$

三、利用公钥密码实现数字签名

⑵、对RSA数字签名的攻击

①一般攻击:

- 因为e和n是用户A的公开密钥，所以任何人都可以获得并使用e和n。攻击者可随意选择一个数据Y，并用A的公钥计算

$$X = (Y)^e \bmod n$$

- 因为 $Y = (X)^d \bmod n$ ，于是可以用Y伪造A的签名。因为Y是A对X的一个有效签名。
- 注意：这样的 X 往往无正确语义！因此，这种攻击在实际上有效性不大！

三、利用公钥密码实现数字签名

⑵、对RSA数字签名的攻击

②利用已有的签名进行攻击:

- 攻击者选择随机数据 M_3，且$M_3=M_1M_2 \bmod n$ 。
- 攻击者设法让A对M_1和M_2签名:

  $S_1=(M_1)^d \bmod n$ ， $S_2=(M_2)^d \bmod n$
- 于是可以由S_1和S_2计算出A对M_3的签名。因为

$S_1S_2=(M_1)^d(M_2)^d \bmod n=(M_3)^d \bmod n=S_3$

- 对策：A不直接对数据M 签名，而是对HASH(M)签名。

三、利用公钥密码实现数字签名

⑵、对RSA数字签名的攻击

②利用已有的签名进行攻击:

- 此时:

$S_1=(\text{HASH}(M_1))^d \bmod n$， $S_2=(\text{HASH}(M_2))^d \bmod n$

而，

$(\text{HASH}(M_1))^d\,(\text{HASH}(M_2))^d \neq (\text{HASH}(M_1M_2))^d \bmod n$

- 所以：$S_3 \neq S_1S_2$
- 于是不能由S_1和S_2计算出A对M_3的签名。

三、利用公钥密码实现数字签名

⑵、对RSA数字签名的攻击

③攻击签名获得明文:

- 攻击者截获C，$C=(M)^e \bmod n$ 。
- 攻击者选择小的随机数r，计算：

$$x = r^e \bmod n，\ y = xC \bmod n，\ t = r^{-1} \bmod n$$

- 攻击者让A对y签名，于是攻击者又获得：

$$S = y^d \bmod n$$

- 攻击者计算$tS = r^{-1}y^d = r^{-1}x^dC^d = C^d = M \bmod n$
- 对策：A不直接对数据M签名，而是对HASH(M)签名。

三、利用公钥密码实现数字签名

⑵、对RSA数字签名的攻击

- 结论:
  - ■不直接对数据M签名，而是对HASH(M)签名。
  - ■使用时间戳
  - ■对于同时确保秘密性和真实性的通信，应当先签名后加密。

三、利用公钥密码实现数字签名

⑶、RSA数字签名的应用：PGP

- 数据*M*经MD5处理，得到MD5（*M*）
- 利用RSA对HASH(*M*)签名,得到M的签名*S*
- 使用ZIP对< *M*, *S* >压缩
- 再用IDEA对压缩数据加密： IDEA(ZIP(*M*, *S*))
- 用RSA对IDEA的密钥加密：RSA(*k*)
- 形成数据：< IDEA(ZIP(*M*,*S*)), RSA(*k*)>
- 将数据转换成ASCII码。

作 业 题

1、p189第2题。

2、p189第3题。

谢　谢！