《现代密码学》第八讲

数字签名

上章内容回顾

- 对称密码体制面临的问题
- 公钥密码体制的发展
- 单向陷门函数及构造
- RSA加密算法及其应用
- ElGmal加密算法
- 椭圆曲线加密码体制简介

本章主要内容

- 数字签名的基本概念
- 一般数字签名算法
  - RSA数字签名技术
  - DSA数字签名技术
  - 基于离散对数的数字签名
  - 椭圆曲线数字签名
- 加密认证方式与签密

本章主要内容

- 数字签名的基本概念
- 一般数字签名算法
  - RSA数字签名算法
  - DSA数字签名算法
  - 基于离散对数的数字签名算法
  - 椭圆曲线数字签名算法
- 加密认证方式与签密

数字签名的基本概念

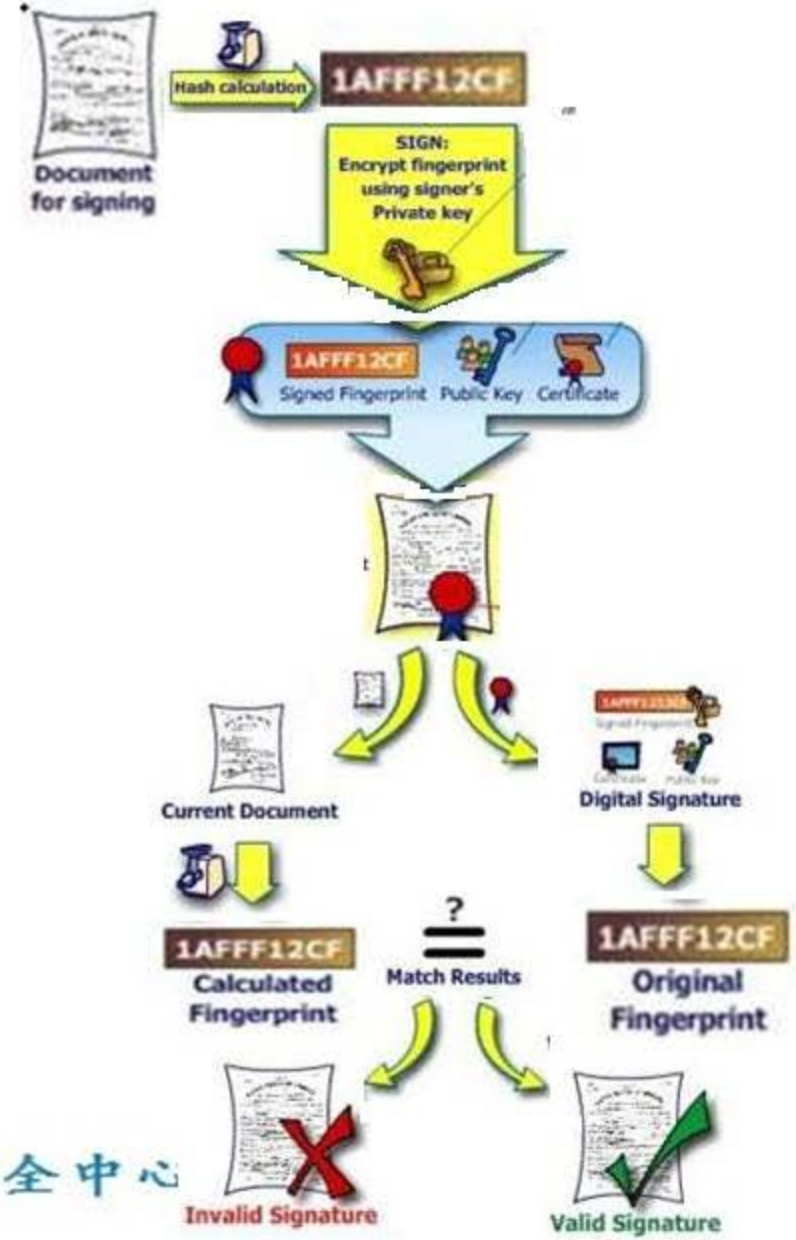
手写签名（如写信、签订协议、支付确认、批复文件等）是一种传统的确认方式.

- 手写签名是所签文件的物理组成部分；
  - 数字信息无绑定的物理载体。
- 手写签名通过与标准签名比较或检查笔迹来验证；
  - 数字信息肉眼无法辨识含义。
- 手写签名不易模仿复制；
  - 数字信息十分容易复制、粘贴。

数字签名的基本概念

数字签名（Digital Signature），也称电子签名，是指附加在某一电子文档中的一组特定的符号或代码，它是利用数学方法对该电子文档进行关键信息提取并与用户私有信息进行混合运算而形成的，用于标识签发者的身份以及签发者对电子文档的认可，并能被接收者用来验证该电子文档在传输过程中是否被篡改或伪造.

数字签名的基本概念


Document for signing
Hash calculation
1AFFF12CF
SIGN:
Encrypt fingerprint using signer's Private key
1AFFF12CF
Signed Fingerprint
Public Key
Certificate
Current Document
Digital Signature
1AFFF12CF
Calculated Fingerprint
?
Match Results
1AFFF12CF
Original Fingerprint
Invalid Signature
Valid Signature

数字签名的基本概念

数字签名模型：

- 密钥生成：概率算法，输入一个二进制的安全参数 $1^k \in N$，为签名者生成一对密钥(PK_A, SK_A)，PK_A是公开钥，SK_A是秘密密钥；
- 签名：概率算法或确定算法(如图)，签名者A首先对待签消息m进行摘要提取$h(m)$，然后用私钥对其签名 $S=Sig_{SK_A}(m)$；
- 验证：确定算法，任何验证者获取A的公钥，并验证消息m及其签名S是否正确

$$Ver_{PK_A}(S,\ m)=\begin{cases}True\\False\end{cases}$$

数字签名的基本概念

安全模型

攻击者资源：

- 惟密钥攻击：攻击者只有用户的公开密钥.
- 已知消息攻击：攻击者拥有一些消息的合法签名，但是消息不由他选择.
- 选择消息攻击：攻击者可以自由选择消息并获取消息相应的签名.

攻击结果：

- 完全破译：攻击者恢复出用户的私有密钥.
- 一致伪造：攻击者对于任意消息可以伪造其签名.
- 选择性伪造：攻击者可以对一个自己选取的消息伪造签名.
- 存在性伪造：攻击者可以生成一些消息的签名，但在伪造前对该消息一无所知.

数字签名的基本概念

- 1976年， W Diffie 和 M Hellman 在“New Directions in Cryptography”，首先提出了数字签名的思想并猜测存在这样的方案.
- 1978年，R Rivest，A Shamir，和 L Adleman 发明的RSA算法可以用作数字签名算法.
- 1984年， S Goldwasser，S Micali，和 R Rivest 首次粗略提出数字签名算法的安全性要求.
- 1991年，美国NIST公布的联邦信息处理标准FIPS PUB 186，其中采用了SHA和签名算法DSA.
- 2004年，中国颁布电子签章法.
- 2012年，中国发布GM/T 0003-2012 《SM2椭圆曲线公钥密码算法》，其中包含数字签名算法标准.

数字签名的基本概念

- 特殊属性

➢ 1983年，Chaum, David. Blind signatures for untraceable payments. Crypto 82.

➢ 1979年，Leslie Lamport.Lamport one time signature.

1979年，Ralph Merkle. Merkle signature scheme. Ph.D. dissertation.

➢ 1979年，Adi Shamir and George Blakley (independently).(t, n)-threshold scheme. It is possible to define (*t*,*n*)-threshold signature scheme.

➢ 1991年，Chaum, David, van Heyst, Eugene. Group signatures. EUROCRYPT.

➢ 2001年，Ron Rivest, Adi Shamir, and Yael Tauman, Ring signatures, ASIACRYPT.

- 基于身份

➢ 1984年以色列科学家Shamir提出基于身份的密码体制同时，给出了一个采用RSA算法的IBS算法。

➢ 2000年，Sakai等人提出第一个利用双线性对的基于身份的签名方案。

➢ 2001年，Boneh等人提出了高效的基于双线性对的短签名方案。

本章主要内容

- 数字签名的基本概念
- 一般数字签名算法
  - RSA数字签名算法
  - DSA数字签名算法
  - 基于离散对数的数字签名算法
  - 椭圆曲线数字签名算法
- 加密认证方式与签密

RSA数字签名算法

1）密钥生成

① 选两个安全的大素数p和q.

② 计算$n=p\times q$，$\varphi(n)=(p-1)(q-1)$，其中$\varphi(n)$是n的欧拉函数值.

③ 选一整数e，满足$1<e<\varphi(n)$，且$\gcd(\varphi(n),e)=1$.

④ 计算d，满足$d\cdot e\equiv 1 \bmod \varphi(n)$，即$d$是$e$在模$\varphi(n)$下的乘法逆元。因$e$与$\varphi(n)$互素，故它的乘法逆元存在且唯一.

⑤ (e,n)为公开密钥，(d,n)为秘密密钥.

⑥ 选取一个hash函数h: $\{0,1\}^*\rightarrow\{0,1\}^t$，$t$为安全参数.

RSA数字签名算法

2）签名：

设待签名消息为m，用私钥对其签名

$$s \equiv \mathrm{h}(m)^d \bmod n$$

3）验证：

验证者获取签名者公钥$\{e,n\}$，对收到的消息签名对(m,s)计算下列等式是否成立

$$\mathrm{h}(m) \stackrel{?}{\equiv} s^e \bmod n$$

若成立，则发送方的签名有效.

本章主要内容

- 数字签名的基本概念
- 一般数字签名算法
  - RSA数字签名算法
  - DSA数字签名算法
  - 基于离散对数的数字签名算法
  - 椭圆曲线数字签名算法
- 加密认证方式与签密

DSA数字签名算法

- DSS (Digital Signature Standard)是美国NIST公布的联邦信息处理数字签名标准FIPS PUB 186;
- 采用了算法SHA和DSA (Digital Signature Algorithm).
- DSS最初公布于1991年，在考虑了公众对其安全性的反馈意见后， NIST于1993年公布了其修改版.

DSA数字签名算法

1）密钥生成

① 选择一大素数p, 满足$2^{L-1}<p<2^{L}$，其中$512\le L\le 1024$，且L是64的倍数.

②选取p-1的素因子q，满足$2^{159}<q<2^{160}$，即q长为160比特.

③任选一整数h, 满足$1<h<p-1$且使得$h^{(p-1)/q} \bmod p>1$; 计算$g\equiv h^{(p-1)/q} \bmod p$.

④ 任选小于q的随机数x，计算$y\equiv g^{x} \bmod p$;

⑤ 使用SHA-1函数h: $\{0,1\}^{*}\rightarrow\{0,1\}^{160}$.

⑥(y, g, p, q)为公开密钥，(x, g, p, q)为秘密密钥.

DSA数字签名算法

2）签名

设用户待签消息为m，用私钥对其签名

①选取随机数k，满足$0<k<q$，计算

$$r\equiv(g^k \bmod p) \bmod q,$$

$$s\equiv[k^{-1}(\mathrm{h}(m)+xr)] \bmod q,$$

② 用户对消息m的签名为(r,s)

DSA数字签名算法

3）验证：

验证者获取签名者公钥$(y,\ g, p, q)$，对收到的消息签名对(m,r,s)计算下列等式是否成立

$$r^s \overset{?}{\equiv} g^{\mathrm{h}(m)} y^r \bmod p$$

若成立，则发送方的签名有效.

DSA数字签名算法

4) 正确性

因为若(m,r,s)为用户生成的合法签名，则

$$
\begin{aligned}
r^{s} &\equiv r^{[k^{-1}(h(m)+xr)]\bmod q} \bmod p \\
&\equiv g^{k[k^{-1}(h(m)+xr)]\bmod q} \bmod p \\
&\equiv g^{(h(m)+xr)\bmod q} \bmod p \\
&\equiv g^{h(m)} g^{xr} \bmod p \\
&\equiv g^{h(m)} y^{r} \bmod p
\end{aligned}
$$

5）安全性：

DSA安全性基于有限域上求离散对数的困难性.

DSA数字签名算法

6）离线在线签名

签名产生过程中的运算主要是求r的模指数运算$r=(g^k \bmod p) \bmod q$，而这一运算与待签的消息m无关，因此能被预先计算.

事实上，用户可以预先离线计算出很多r和k^{-1}，需对消息m签名时，只需在线进行模乘和模加运算，从而可大大加快产生签名的速度。

7）随机参数

随机数k不可泄露，也不可重复使用.

本章主要内容

- 数字签名的基本概念
- 一般数字签名算法
  - RSA数字签名算法
  - DSA数字签名算法
  - 基于离散对数的数字签名算法
  - 椭圆曲线数字签名算法
- 加密认证方式与签密

基于离散对数数字签名算法

基于离散对数问题的数字签名体制是数字签名体制中最为常用的一类，其中包括

ElGamal签名体制、

DSA签名体制、

Shnorr签名体制等.

基于离散对数数字签名算法

1）参数和密钥生成

① 选择一大素数p, 满足$2^{L-1}<p<2^{L}$，其中$512\le L\le 1024$，且L是64的倍数.

②选取p-1的素因子q，满足$2^{159}<q<2^{160}$，即q长为160比特.

③任选一整数h, 满足$1<h<p-1$且使得$h^{(p-1)/q} \bmod p>1$; 计算$g\equiv h^{(p-1)/q} \bmod p$.

④ 任选小于q的随机数x，计算$y\equiv g^{x} \bmod p$;

⑤ 选取一个hash函数h: $\{0,1\}^{*}\rightarrow\{0,1\}^{t}$, t为安全参数.

⑥(y, g, p, q)为公开密钥，(x, g, p, q)为秘密密钥.

基于离散对数数字签名算法

2) 签名的产生过程

对于待签名的消息m，签名者执行以下步骤：

① 计算m的杂凑值$\mathrm{h}(m)$。

② 选择随机数k，使得$1<k<q$，计算

$$r \equiv (g^k \bmod p) \bmod q.$$

③ 从签名方程$ak \equiv b+cx \bmod q$中解出s，以(r, s)作为产生的数字签名.

基于离散对数数字签名算法

方程的系数（a,b,c）共有120中选择方法：

1	$\pm r$	$\pm s$	$\mathrm{h}(m)$
2	$\pm \mathrm{h}(m)*r$	$\pm s$	1
3	$\pm \mathrm{h}(m)*r$	$\pm \mathrm{h}(m)*s$	1
4	$\pm \mathrm{h}(m)*r$	$\pm sr$	1
5	$\pm \mathrm{h}(m)*s$	$\pm sr$	1

基于离散对数数字签名算法

例：(a,b,c) 从第一行选取，都只选正号

1） $a=r,\ b=s,\ c=\mathrm{h}(m)$;

2） $a=r,\ b=\mathrm{h}(m),\ \mathrm{c}=s$;

3） $a=s,\ b=r,\ c=\mathrm{h}(m)$;

4） $a=s,\ b=\mathrm{h}(m),\ c=r$;

5） $a=\mathrm{h}(m),\ b=r,\ c=s$;

6） $a=\mathrm{h}(m),\ b=s,\ c=r$.

基于离散对数数字签名算法

例： (a,b,c)的值从第一行选取，共有24中取法

1） a=r, b=s, c=h(m);
2） a=r, b=h(m), c=s;
3） a=s, b=r, c=h(m);
4） a=s, b=h(m), c=r;
5） a=h(m), b=r, c=s;
6） a=h(m), b=s, c=r.
7） a=-r, b=s, c=h(m);
8） a=-r, b=h(m), c=s;
9） a=s, b=-r, c=h(m);
10） a=s, b=h(m), c=-r;
11） a=h(m), b=-r, c=s;
12） a=h(m), b=s, c=-r.
13） a=r, b=-s, c=h(m);
14） a=r, b=h(m), c=-s;
15） a=-s, b=r, c=h(m);
16） a=-s, b=h(m), c=r;
17） a=h(m), b=r, c=-s;
18） a=h(m), b=-s, c=r.
19） a=-r, b=-s, c=h(m);
20） a=-r, b=h(m), c=-s;
21） a=-s, b=-r, c=h(m);
22） a=-s, b=h(m), c=-r;
23） a=h(m), b=-r, c=-s;
24） a=h(m), b=-s, c=-r.

基于离散对数数字签名算法

3) 签名的验证过程

接收方在收到消息m和签名(r,s)后，可以按照以下验证方程检查签名是否有效.

$$Ver(y,(r,s),m)=True \Leftrightarrow r^a \equiv g^b y^c \bmod p\,.$$

基于离散对数数字签名算法

签名等式	验证等式
1) $rk \equiv s + h(m)x \pmod{q}$	$r^r \equiv g^s y^{h(m)} \pmod{p} \pmod{q}$
2) $rk \equiv h(m) + sx \pmod{q}$	$r^r \equiv g^{h(m)} y^s \pmod{p} \pmod{q}$
3) $sk \equiv r + h(m)x \pmod{q}$	$r^s \equiv g^r y^{h(m)} \pmod{p} \pmod{q}$
4) $sk \equiv h(m) + rx \pmod{q}$	$r^s \equiv g^{h(m)} y^r \pmod{p} \pmod{q}$
5) $h(m)k \equiv s + rx \pmod{q}$	$r^{h(m)} \equiv g^s y^r \pmod{p} \pmod{q}$
6) $h(m)k \equiv r + sx \pmod{q}$	$r^{h(m)} \equiv g^r y^s \pmod{p} \pmod{q}$

本章主要内容

- 数字签名的基本概念
- 一般数字签名算法
  - RSA数字签名算法
  - DSA数字签名算法
  - 基于离散对数的数字签名算法
  - 椭圆曲线数字签名算法
- 加密认证方式与签密

椭圆曲线数字签名

1） 密钥生成

①设GF(p)为有限域，选取一条椭圆曲线$E_p(a,b)$，取$E_p(a,b)$的一个生成元G，G的阶为满足安全要求的素数q.

②选取一个hash函数h: $\{0,1\}^* \rightarrow E_p(a,b)$.

③用户A选小于q的随机数x，并计算$P_A=x_AG$

④公开钥为(a,b,p,G,P)，秘密密钥为(a,b,p,G,x).

椭圆曲线数字签名

2) 签名

对于待签名的消息m，签名者执行以下步骤：

① 计算m的杂凑值$h_1=\mathrm{h}(m)$.

② 选择随机数k，使得$1<k<q$，计算

$$kG=(k_x,k_y)，\ 令r=k_x,$$

③ 计算$s=(h_1+rx)\,k^{-1} \bmod q$.

④ 对消息m的签名值为(r,s).

椭圆曲线数字签名

3) 验证签名

接收方在收到消息m和签名(r,s)后，可以按照以下验证方程检查签名是否有效.

① 计算m的杂凑值$h_1=\mathrm{h}(m)$.

② 计算

$$u = s^{-1} h_1 \bmod q, \quad v = s^{-1} r \bmod q,$$

③ 计算椭圆曲线上的点

$$(x,y) = uG+vY,$$

④ 然后比较$r=x \bmod p$是否成立；成立则签名有效.

椭圆曲线数字签名

4）正确性

因为 $s=(h_1+rx)\,k^{-1}\bmod q$,

所以 $k=(h_1+rx)\,s^{-1}\bmod q$.

所以 $kG=(s^{-1}h_1+s^{-1}r^{*}x)\,G$

$=(u+vx)G$

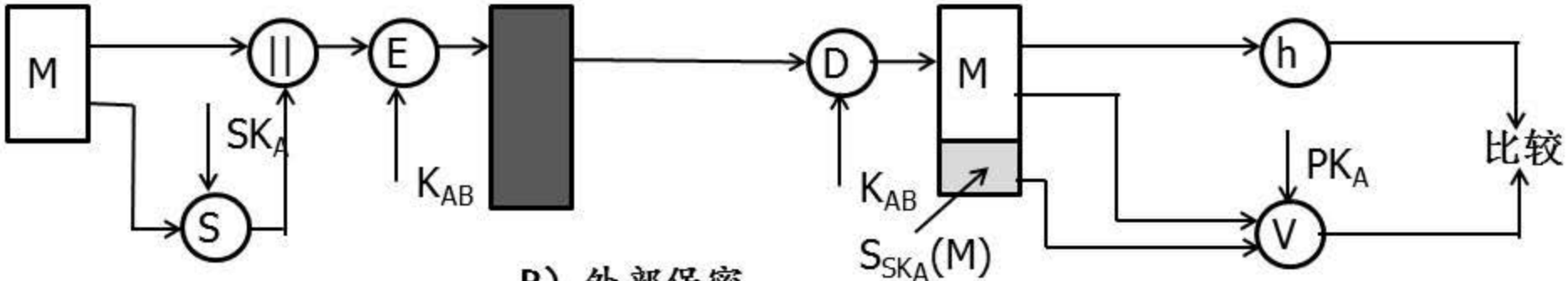
$=uG+vY$

本章主要内容

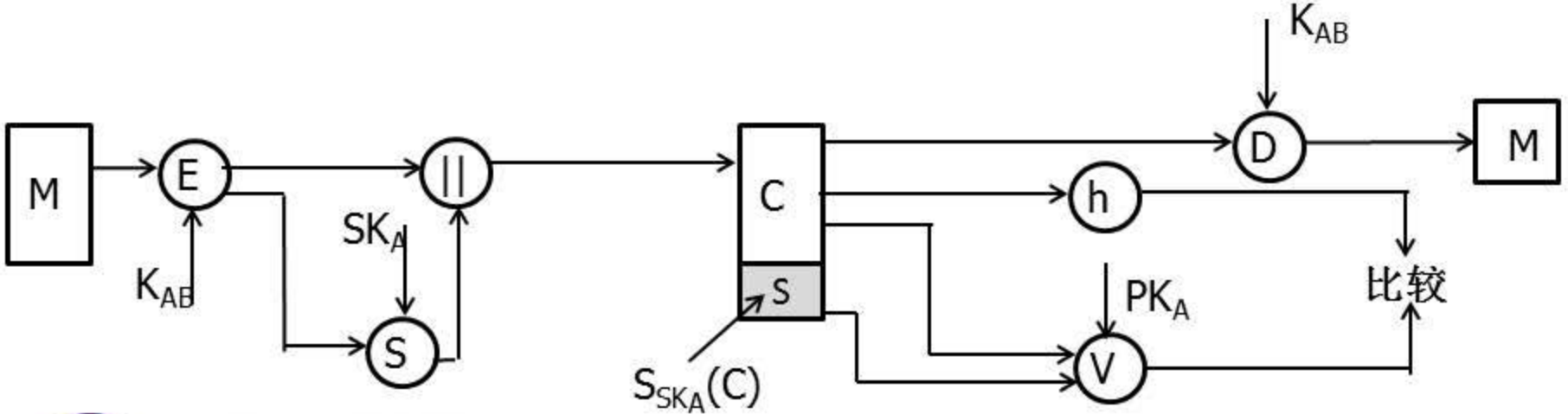
- 数字签名的基本概念
- 一般数字签名算法
  - RSA数字签名技术
  - DSA数字签名技术
  - 基于离散对数的数字签名
  - 椭圆曲线数字签名
- 加密认证方式与签密

加密认证方式与签密

- 外部保密方式是指对消息直接生成数字签名；
- 内部保密方式是指对已加密的消息生成数字签名.



B）外部保密



C）内部保密

加密认证方式与签密

- 外部保密方式便于解决争议，接收方可将明文消息及其数字签名存储下来，第三方在处理争议时，很容易检查签名和对应明文消息是否匹配.
- 采用内部保密方式，接收方可将明文消息、密文及其数字签名存储下来，但是由于签名是对应于密文的，所以第三方必须得到消息的解密密钥后才能验证明文消息及签名是否匹配.

加密认证方式与签密

签密（Digital Signcryption）

- Y. Zheng. Digital signcryption or how to achieve cost (signature & encryption). Cost (signature) + cost (encryption). Advances in Cryptology-CRYPTO'97, LNCS 1294: 165-179, Springer-Verlag, 1997.

- 签密算法同时取得机密性、完整性、认证和不可否认性.
- 签密算法在计算量和通信成本上都要低于传统的“先签名后加密”方法;
- 签密算法允许并行计算一些昂贵的密码操作.

加密认证方式与签密

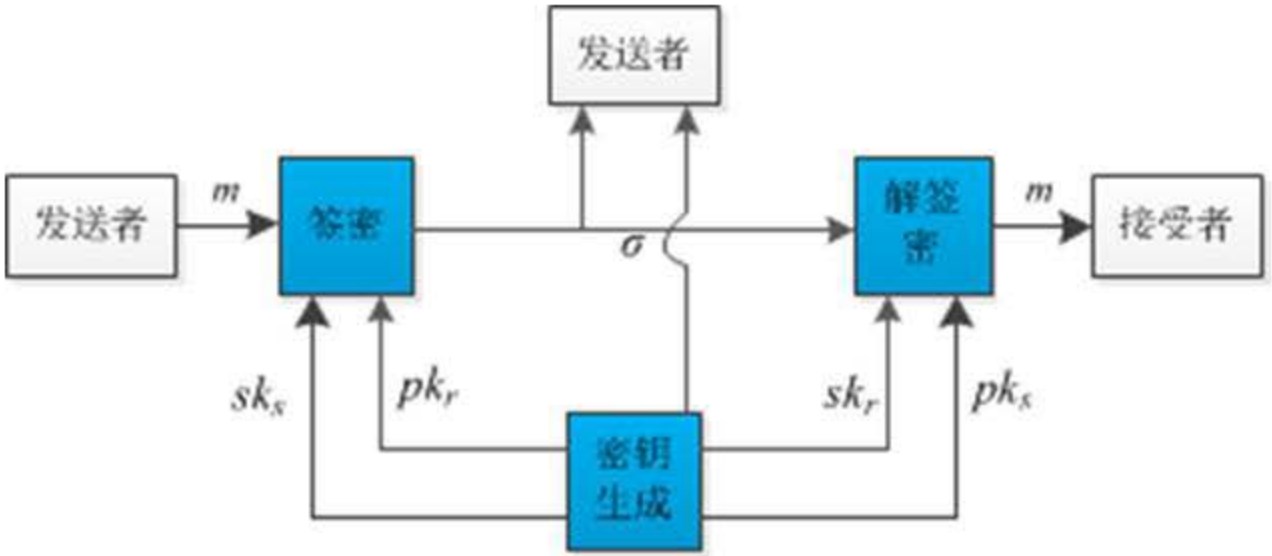
签密方案一般由以下三个算法组成：

- 密钥生成：输入1^k（k是安全参数），输出发送者的公钥/私钥对(pk_s, sk_s)，和接收者的公钥/私钥对(pk_r, sk_r).
- 签密：输入消息m, 发送者的私钥sk_s和接收者的公钥pk_r，输出密文$\sigma = \text{Signcrypt}(m, sk_s, pk_r)$.
- 解签密：输入密文σ，发送者的公钥pk_s和接收者的私钥sk_r，输出消息m 或者错误符号.

$$m = \text{Unsigncrypt}(\sigma, pk_s, sk_r).$$

加密认证方式与签密

- 一致性约束：如果σ= Signcrypt(m,sk_s,pk_r)，那么一定输出m =Unsigncrypt(σ, pk_s, sk_r).

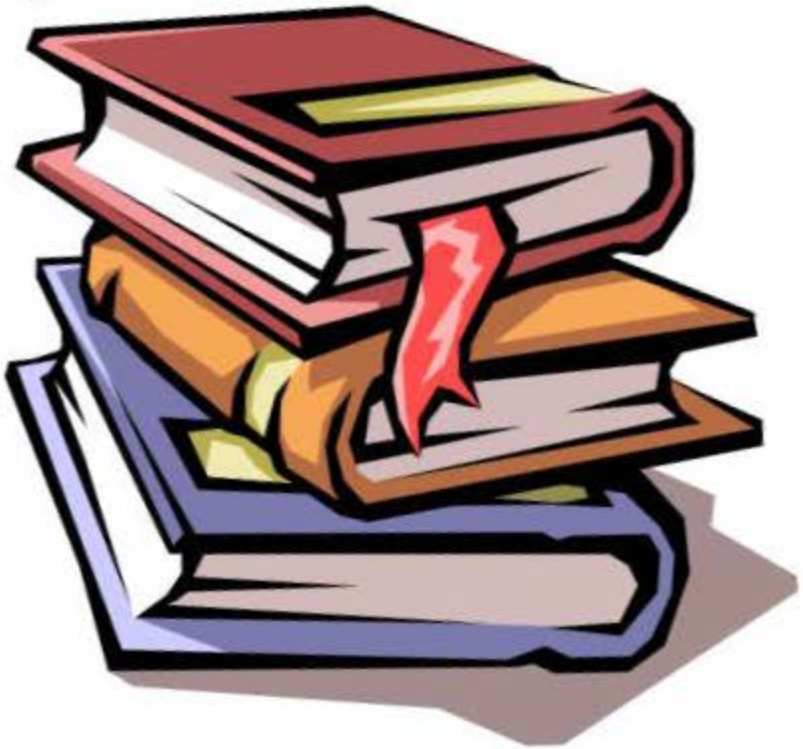


本章主要内容

- 数字签名的基本概念
- 一般数字签名算法
  - RSA数字签名技术
  - DSA数字签名技术
  - 基于离散对数的数字签名
  - 椭圆曲线数字签名
- 加密认证方式与签密

北京郵電大學
BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICA

THE END!



BUPT ISC 信息安全中心