# 密 码 学

## 第十七讲　密钥管理（2）

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

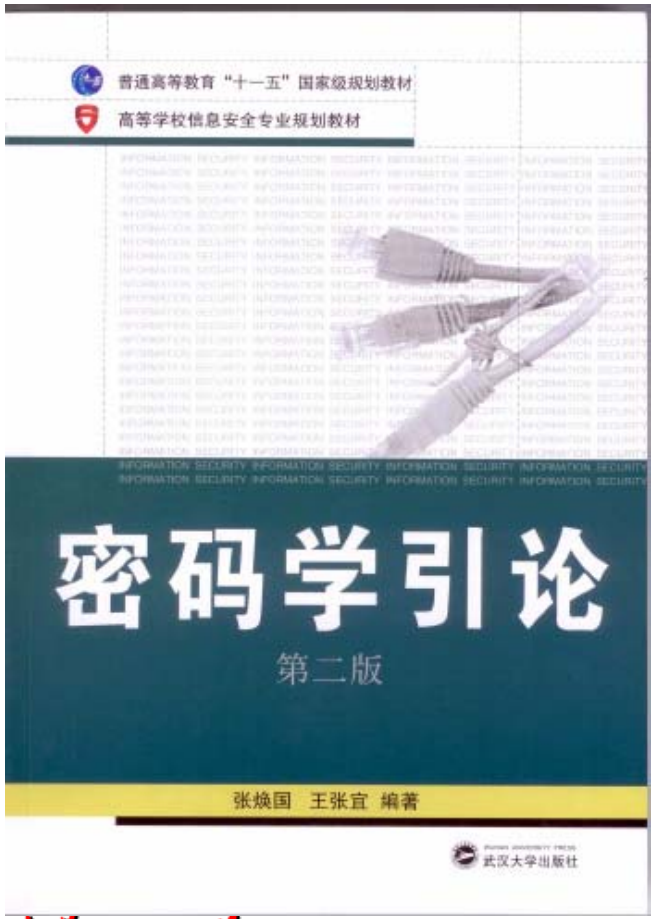
第一讲 信息安全概论
第二讲 密码学的基本概念
第三讲 数据加密标准（DES）
第四讲 高级数据加密标准（AES）
第五讲 中国商用密码（SMS4）
第六讲 分组密码的应用技术
第七讲 序列密码
第八讲 复习
第九讲 公钥密码（1）

# 内容简介

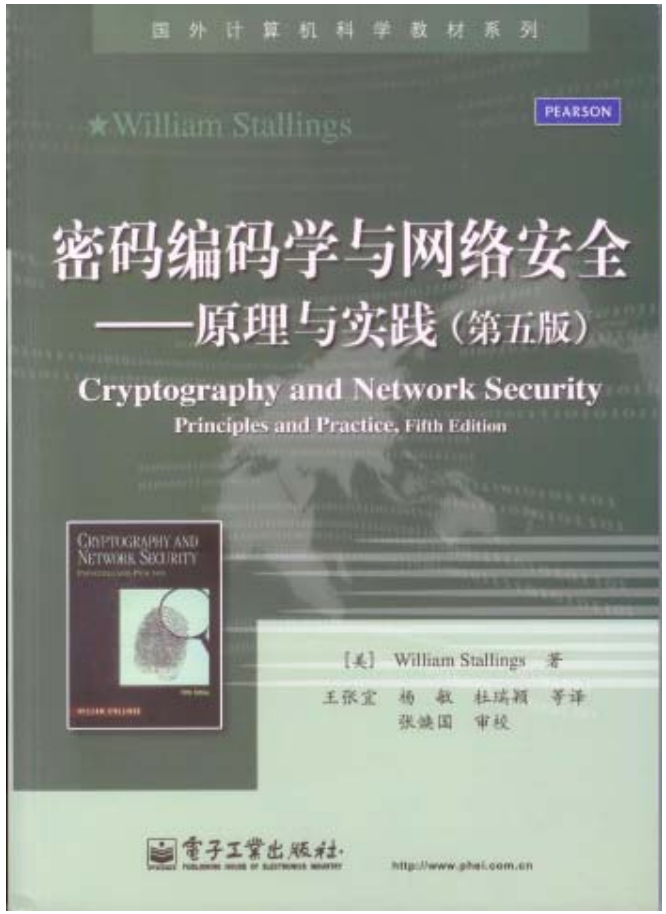
第十讲 公钥密码（2）
第十一讲 数字签名（1）
第十二讲 数字签名（2）
第十三讲 HASH函数
第十四讲 认证
第十五讲 密码协议
第十六讲 密钥管理（1）
第十七讲 密钥管理（2）
第十八讲 复习

# 教材与主要参考书

教材




参考书



# 一、公钥密码密钥管理的概念

- 密码体制不同，密钥的管理方法也不同。因此公钥密码的密钥管理与传统密码的密钥管理大不相同：
- 传统密码只有一个密钥，加密钥等于解密钥（$K_e = K_d$）。因此，密钥的秘密性、真实性和完整性都必须保护。
- 公开密钥密码有两个密钥，加密钥与解密钥不同（$K_e \neq K_d$），而且由加密钥在计算上不能求出解密钥，所以加密钥的秘密性不用确保。

# 一、公钥密码密钥管理的概念

- 虽然公开密钥密码体制的加密钥可以公开，其秘密性不需要保护，但其完整性和真实性却必须严格保护。
- 公开密钥密码体制的解密钥的秘密性、真实性和完整性都必须保护。

# 二、公钥密码的密钥产生

- 传统密码体制的密钥本质上是一种随机数或随机序列，因此传统密码体制的密钥产生本质上是产生具有良好密码学特性的随机数或随机序列。

- 公开密钥密码体制本质上是一种单向陷门函数，它们都是建立在某一数学难题之上的。不同的公开密钥密码体制所依据的数学难题不同，因此其密钥产生的具体要求不同。但是，它们都必须满足密码安全性和应用的有效性对密钥所提出的要求。

# 二、公钥密码的密钥产生

## 1. RSA密码的密钥产生

- 对于RSA密码，其秘密解密密钥为<p,q,φ(n),d>，公开加密钥为<n,e>，因此其密钥的产生主要是根据安全性和工作效率来合理的产生这些密钥参数。
- p和q越大则越安全，但工作效率就越低。反之，p和q越小则工作效率就越高，但安全性就越低。根据目前的因子分解能力，对于一般应用，p和q至要有512位，以使n至少有1024位；而对于重要应用，p和q至少要有1024位，以使n至少有2048位。p和q 要随机；p和q的差要大；（p-1）和（q-1）的最大公因子要小；e和d都不能太小；等等。

# 二、公钥密码的密钥产生

## 2. 椭圆曲线密码的密钥产生

- 椭圆曲线密码，由下面的六元组所描述：

$$T=<p,a,b,G,n,h>$$

其中，p为大素数，p确定了有限域GF（p）；元素a,b∈GF(p)，a和b确定了椭圆曲线；G为循环子群$E_1$的生成元，n为素数且为生成元G的阶。

- 私钥定义为一个随机数d，

  d∈{0,1,2,…,n-1}，d既不能太小，也不能太大。

- 公钥定义为Q点，

  Q=dG 。

# 二、公钥密码的密钥产生

- 对于椭圆曲线密码，其用户的私钥d和公钥Q的生成并不困难。
- 困难的是其系统参数<p,a,b,G,n>的选取。也就是椭圆曲线的选取。
- 美国NIST推荐了15条椭圆曲线。
- 中国的商用密码SM2使用了自己的椭圆曲线。
- 我们用演化密码的方法产生了大量的椭圆曲线。
- 目前椭圆曲线的参数n和p的规模应大于$2^{160}$。
- 参数的越大，越安全，但运算越困难，资源的消耗也越多。

# 三、公钥密码的密钥分配

- 和传统密码一样，公钥密码也需要进行密钥分配。但是，公钥密码的密钥分配与传统密码体制的密钥分配有着本质的差别。
- 在密钥分配时必须做到：
  - 因为公钥是公开的，因此不需确保秘密性。但必须确保公钥的真实性和完整性
  - 确保私钥的秘密性、真实性和完整性。

# 三、公钥密码的密钥分配

- 如果公钥的真实性和完整性受到危害，则基于公钥的各种应用的安全将受到危害。
- 举例：C冒充A欺骗B的攻击方法

①攻击者C在PKDB中用自己的公钥$K_{eC}$替换用户A的公钥$K_{eA}$。

②C用自己的解密钥签名一个消息冒充A发给B。

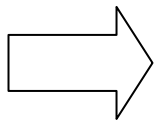
$$C \rightarrow B: <A, D(M, K_{dC})>$$

③B验证签名：因为此时PKDB中A的公开钥已经替换为C的公开钥，故验证为真。

# 三、公钥密码的密钥分配

**PKDB**

| | |
|---|---|
| A | $K_{eA}$ |
| B | $K_{eB}$ |
| C | $K_{eC}$ |



**PKDB**

| | |
|---|---|
| A | $K_{eC}$ |
| B | $K_{eB}$ |
| C | $K_{eC}$ |

**攻击者C篡改PKDB**

# 三、公钥密码的密钥分配

- 结果
  - 因验证签名为真，于是B认为攻击者C就是A。
  - 若B要发送加密的消息给A，则B要用A的公开钥进行加密，但A的公开钥已被换成C的公开钥，因此B实际上是用C的公开钥进行了加密。
  - C从网络上截获B发给A的密文。由于这密文实际上是用C的公开钥加密的，所有C可以解密得到明文。A反而不能正确解密。

# 三、公钥密码的密钥分配

- 上述攻击成功的原因：

①对存入**PKDB**的公开钥没有采取保护措施，致使公开加密钥被替换而不能发现；

②存入**PKDB**的公开钥与用户的标识符之间没有绑定关系，致使**A**的公钥替换成**C**的公钥后不能发现公开钥与用户的标识符之间的对应关系被破坏。

# 四、公钥证书的概念

- 采用数字签名技术可以克服上述两个缺点，确保公开加密钥的安全分配。
- 经过可信实体签名的一组信息的集合被称为证书（Certificate），而可信实体被称为签证机构 CA（Certification Authority）。
- 一般地讲，证书是一个数据结构，是一种由一个可信任的权威机构签署的信息集合。
- 在不同的应用中有不同的证书。例如公钥证书PKC（Public Key Certificate）、PGP证书、SET证书等。

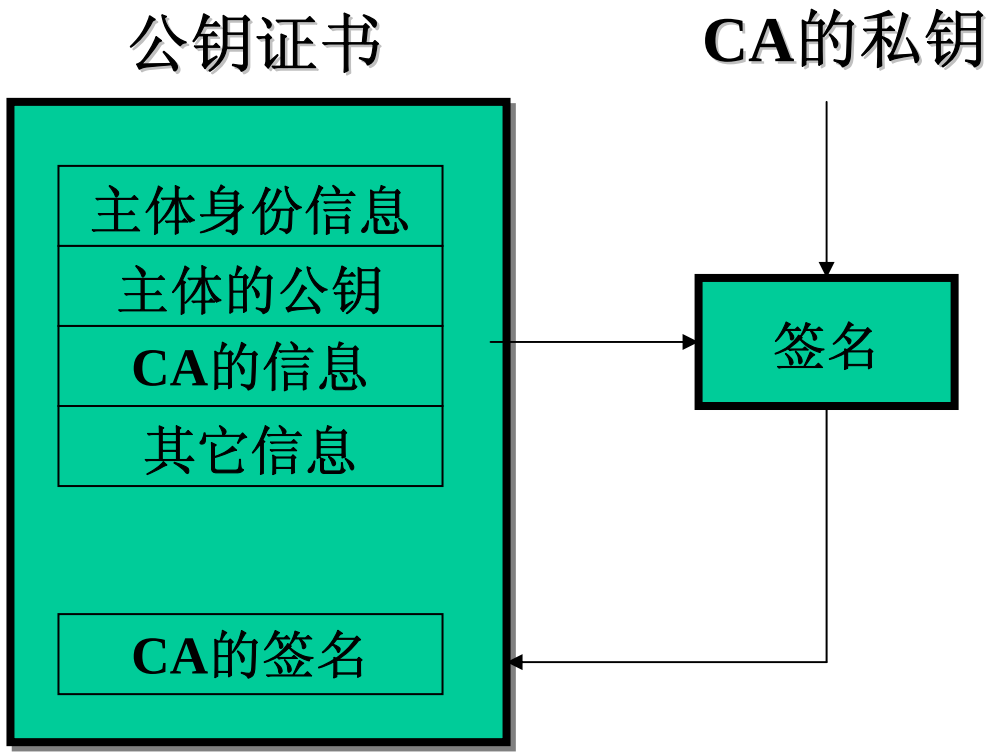
# 四、公钥证书的概念

- 公钥证书 PKC是一种包含持证主体标识、持证主体公钥等信息，并由可信签证机构（CA）签署的信息集合。
- 公钥证书主要用于确保公钥的安全，确保公钥与用户标识符之间绑定关系的安全。这个公钥就是证书所标识的那个主体的合法的公钥。
- 公钥证书的持证主体可以是人、设备、组织机构或其它主体。
- 公钥证书可以明文的形式进行存储和分配。

# 四、公钥证书的概念

- 任何一个用户只要知道签证机构的公钥，就能检查对证书签名的合法性。如果检查正确，那么用户就可以相信那个证书所携带的公钥是真实的，而且这个公钥就是证书所标识的那个主体的合法的公钥。
- 日常生活中有许多使用证书的例子，例如汽车驾照。驾照由可信的公安机关签发，以标识驾驶员的驾驶资格。由于有公安机关的签章，任何人都可以验证驾照的真实性。又由于驾照上印有驾驶员的照片并盖了钢印，从而实现驾驶员与驾照之间的严格绑定。

# 四、公钥证书的概念




简单公钥证书示意图

# 四、公钥证书的概念

- 有了公钥证书系统后，如果某个用户需要任何其他已向CA注册的用户的公钥，可向持证人（或证书机构）直接索取公钥证书。
- 用CA的公钥验证CA的签名，从而获得对公钥的信任。
- 由于公钥证书不需要保密，可以在网络上分发，从而实现公钥的安全网络分配。
- 又由于公钥证书有CA的签名，攻击者不能伪造合法的公钥证书。因此，只要CA是可信的，公钥证书就是可信的，其公钥就是可信的。

# 四、公钥证书的概念

- 使用公钥证书的主要好处：

①用户只要获得用户的证书，就可以获得用户的公钥。

②用户只要获得CA的公钥，就可以安全地认证用户的公钥。

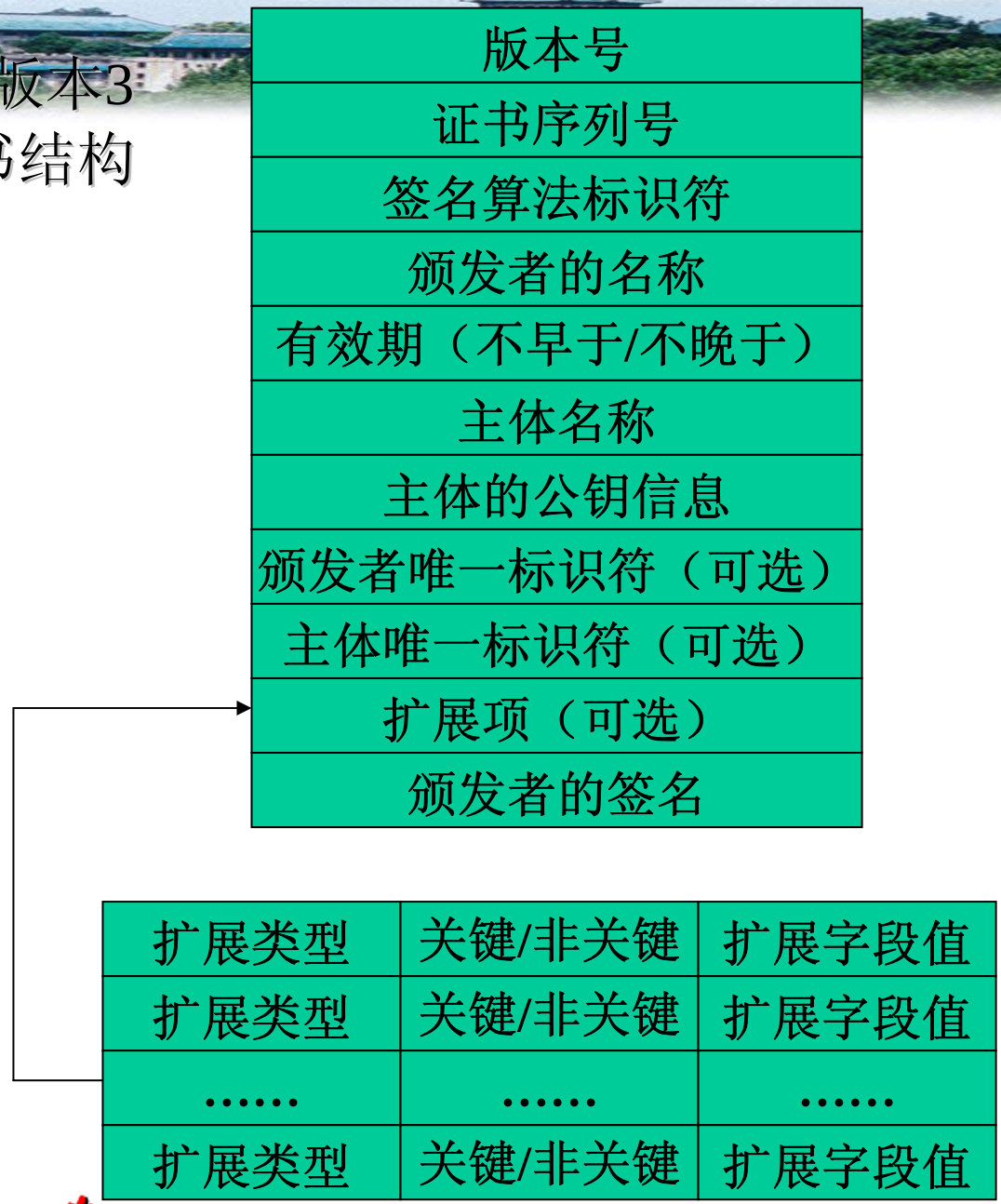
③因此公钥证书为公钥的分发奠定了基础，成为公钥密码在大型网络系统中应用的关键技术。

这就是电子政务、电子商务等大型网络应用系统都采用公钥证书的原因。

# 四、公钥证书的概念

- X.509证书
  - 目前应用最广泛的证书格式是国际电信联盟ITU（International Telecommunication Union）提出的X.509版本3格式。
  - X.509标准最早于1988年颁布。在此之后又于1993年和1995年进行过两次修改。
  - INTERNET工程任务组（IETF）针对X.509在INTERNET环境的应用，颁布了一个作为X.509子集的RFC2459。从而使X.509在INTERNET环境中得到广泛应用。

# X.509版本3的证书结构



# 五、公钥基础设施PKI

- 公钥证书、证书管理机构、证书管理系统、围绕证书服务的各种软硬件设备以及相应的法律基础共同组成公开密钥基础设施**PKI**（**Public Key Infrastructure**）。

- 公开密钥基础设施提供一系列支持公开密钥密码应用（加密与解密、签名与验证签名）的基础服务。
- 本质上，**PKI**是一种标准的公钥密码的密钥管理平台。

# 五、公钥基础设施PKI

- 公钥证书是PKI中最基础的组成部分。
- 此外，PKI还包括签发证书的机构（CA），注册登记证书的机构（RA），存储和发布证书的目录，密钥管理，时间戳服务，管理证书的各种软件和硬件设备，证书管理与应用的各种政策和法律，以及证书的使用者。所有这些共同构成了PKI。

# 五、公钥基础设施PKI

## 1、签证机构CA

- 在PKI中，CA负责签发证书、管理和撤销证书。CA严格遵循证书策略机构所制定的策略签发证书。CA是所有注册用户所信赖的权威机构。

- CA在给用户签发证书时要加上自己的签名，以确保证书信息的真实性。为了方便用户对证书的验证，CA也给自己签发证书。这样，整个公钥的分配都通过证书形式进行。

# 五、公钥基础设施PKI

## 1、签证机构CA

- 对于大范围的应用，一个CA是远远不够的，往往要许多CA。
- 例如对于某一行业，国家建立一个最高级的CA，为根CA。
- 每个省建立一个省CA，每个地市也都可以建立CA，甚至一个企业也可以建立自己的CA。
- 不同的CA服务于不同的范围，履行不同的职责。

# 五、公钥基础设施PKI

## 2、注册机构RA

- RA（Registration Authority）是专门负责受理用户申请证书的机构。根据分工，RA并不签发证书，是负责对证书申请人的合法性进行认证，并决定是批准或拒绝证书申请。
- 接收证书申请人的注册信息，并对其合法性进行认证；
- 批准或拒绝证书的申请；
- 批准或拒绝恢复密钥的申请；
- 批准或拒绝撤销证书的申请；

# 五、公钥基础设施PKI

## 2、注册机构RA

- 对于一个小范围的系统，由CA兼管RA的职能是可以的。但随着用户的增多，CA与RA应当职责分开。
- 申请注册有不同的方式，有在线的方式和离线的方式。在INTERNET环境中可以WEB浏览器方式进行在线注册。注册的过程是用户与CA建立信任关系的一个重要步骤。

# 五、公钥基础设施PKI

## 3、证书的签发

- 经过RA的注册批准后，便可向CA申请签发证书。与注册方式一样，向CA申请签发证书可以在线申请，也可以离线申请。特别是在INTERNET环境中可以WEB浏览器方式在线申请签发证书，越来越受到欢迎。

# 五、公钥基础设施PKI

## 3、证书的签发

CA签发证书的过程如下：

- 用户向CA提交RA的注册批准信息及自己的身份等信息（或由RA向CA提交）；
- CA验证所提交信息的正确性和真实性；
- CA为用户产生密钥（或由用户自己产生并提供密钥），并进行备份；
- CA生成证书，并施加签名；
- 将证书存档入库，并将证书的一个副本交给用户。

# 五、公钥基础设施PKI

## 4、证书目录

- 证书产生之后，必须以一定的方式存储和发布，以便于使用。
- 为了方便证书的查询和使用，CA采用证书目录的式集中存储和管理证书。通常采用建立目录服务器证书库的方式为用户提供证书服务。
- 为了应用的方便，证书目录不仅存储管理用户的证书，还同时存储用户的相关信息（如，电子邮件地址，电话号码等）。因为证书本身是非保密的，因此证书目录也是非保密的。

# 五、公钥基础设施PKI

## 4、证书目录

- 证书目录提供了一种方便的证书存储和分发。
- 关于证书目录，目前尚没有一个统一的标准，但是基于X.500标准的目录正日益受到欢迎。
- 用于INTERNET环境的目录存取协议，并称为轻型目录存取协议LDAP（Lightweight Directory Access Protocol）。LDAP协议在目录模型上与X.500兼容，但比X.500更简单，实施更方便。

# 五、公钥基础设施PKI

## 5、证书的认证

证书认证主要包括以下内容：

① 验证证书上的CA签名是否正确。

② 验证证书内容的真实性和完整性。

③ 验证证书是否处在有效期内（由证书里的时间参数来限定有效期）。

④ 验证证书是否被撤销或冻结；

⑤ 验证证书的使用方式是否与证书策略和使用限制相一致。

# 五、公钥基础设施PKI

## 6、证书的撤销

- 每个证书都有一个有效使用期限，有效使用期限的长短由CA的政策决定。有效使用期限到期的证书应当撤销。
- 证书的公钥所对应的私钥泄露，或证书的持证人死亡，证书的持证人严重违反证书管理的规章制度等情况下也要撤销证书。
- 和证书的签发一样，证书的撤销也是一个复杂的过程。证书的撤销要经过申请、批准、撤销三个过程。

# 五、公钥基础设施PKI

## 7、信任模型

- 对于大范围的PKI（如一个行业或一个地区，甚至一个国家。），一个CA也是不现实的，往往需要多CA。
- 这些CA之间应当具有某种结构关系，以使不同CA之间的证书认证简单方便。
- 证书用户、证书主体、各个CA之间的证书认证关称为PKI的信任模型。
- 人们已经提出了树（层次）模型、森林模型等多种信任模型。

# 谢　谢！