

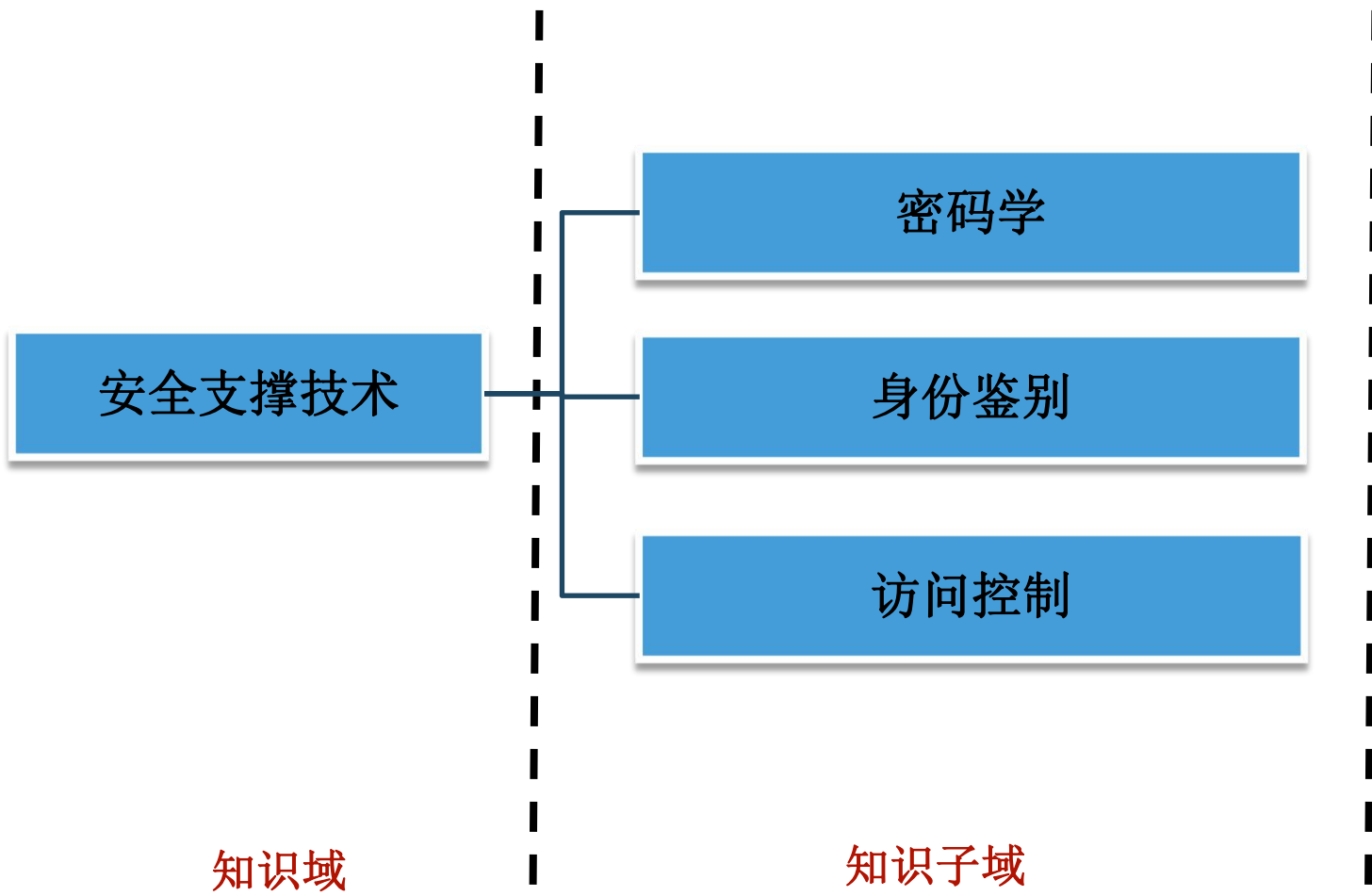
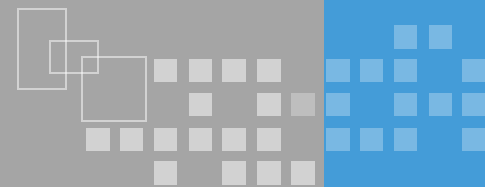


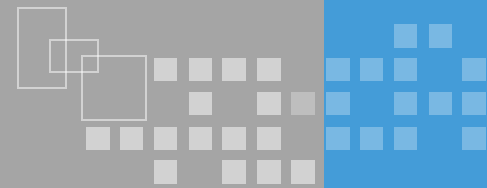
# 信息安全支撑技术

版本：4.2

河南信安世纪 齐文振

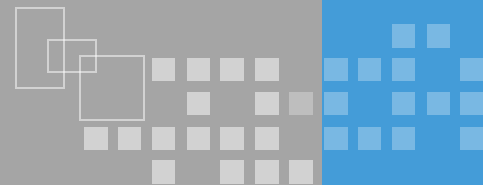
# 课程内容



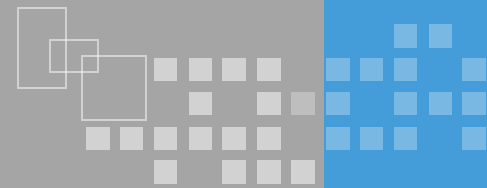


## ❖ 基本概念

- 了解古典密码、近代密码、现代密码等各密码学发展阶段的特点；
- 了解基本保密通信模型；
- 理解密码系统安全性相关概念（科克霍夫准则、密码系统安全性评估）
- 了解密码算法分类的概念。

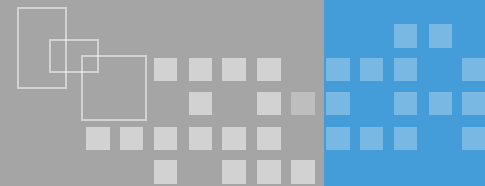


- ❖ 古典密码学（1949年之前）
  - 主要特点：数据的安全基于算法的保密
- ❖ 近代密码学（1949～1975年）
  - 主要特点：密码学真正成为一门科学
- ❖ 现代密码学（1976年以后）
  - 密码学的新方向—公钥密码学
  - 主要特点：解决了密钥分发和管理的问题



- ❖ 安全性在于保持算法本身的保密性
  - 不适合大规模生产
  - 不适合较大的或者人员变动较大的组织
  - 用户无法了解算法的安全性
- ❖ 主要分类
  - 替代密码
  - 置换密码
  - 替代密码与置换密码的组合

# 古典密码学



## ❖ 例如：凯撒密码

abcdefghijklmnopqrstuvwxyz  
DEFGHIJKLMNOPQRSTUVWXYZABC



明文

密文

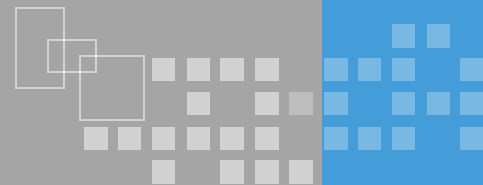
ATTACK NOW

DWWDFN QRZ

## ❖ 例如：ENIGMA

- ENIGMA是由Arthur Scherbius于1919年发明了密码转轮机，使用机电代替手工。在二次世界大战期间, Enigma曾作为德国陆、海、空三军最高级密码机

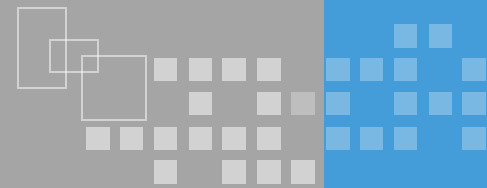




- ❖ 1949年，Shannon（香农）发表论文“The Communication Theory of Secret Systems”，将信息论引入了密码，从而把已有数千年历史的密码学推向了科学的轨道，奠定了密码学的理论基础。

密码学从此开始成为一门科学





- ❖ 解决了密钥分发、管理问题，并提供更多服务
  - 1976年，Diffie & Hellman的“New Directions in Cryptography”提出了非对称密钥密码



Whitfield\_Diffie



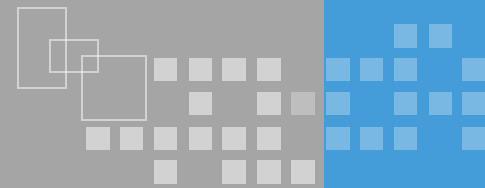
Martin-Hellman

密码学真正广泛在  
商业中应用



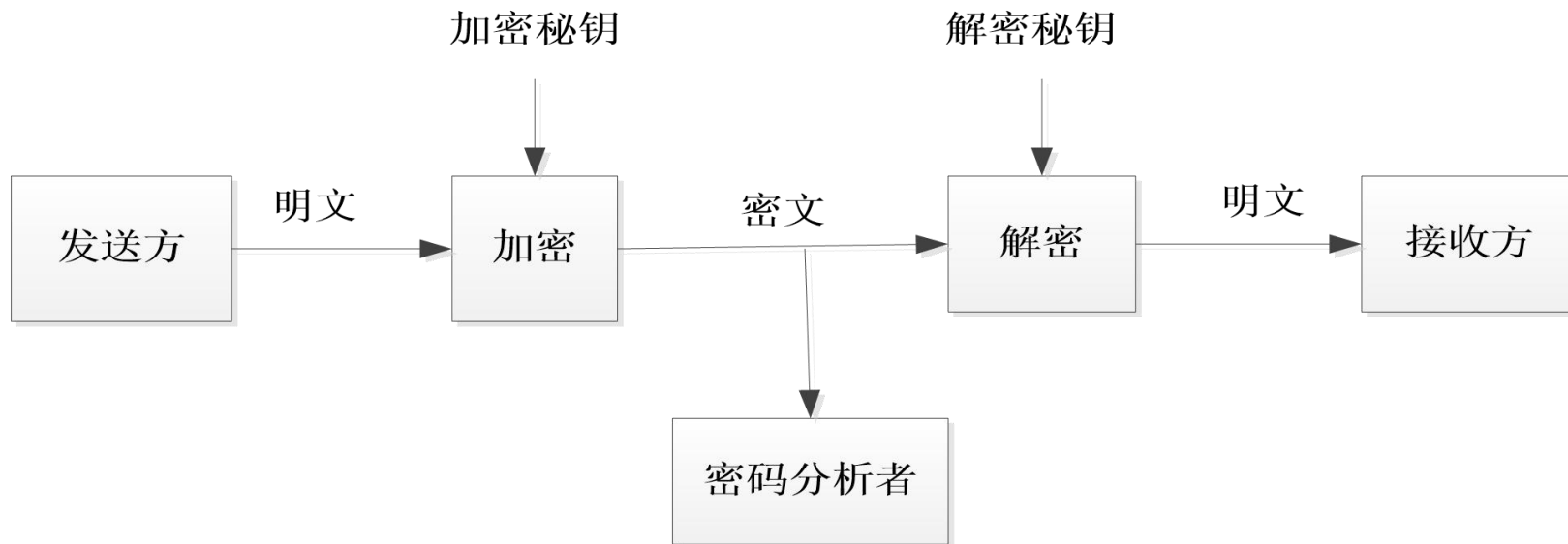


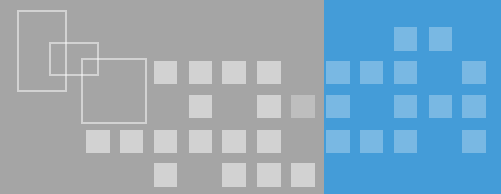
# 基本保密通信模型



## ❖ 基本概念

- 明文、密文
- 加密、解密、加密密钥、解密密钥
- .....





## ❖ 影响密码系统安全性的基本因素

- 密码算法复杂度、密钥机密性、密钥长度
- **科克霍夫（Kerckhoff）原则：**密码体制应该对外公开，仅需对密钥进行保密；如果一个密码系统需要保密的越多，可能的弱点也越多

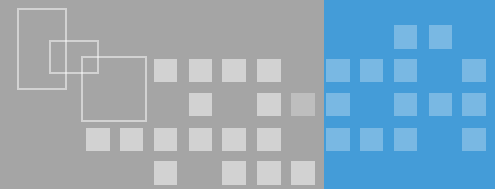
## ❖ 评估密码系统安全性的方法

- 无条件安全、计算安全性、可证明安全性

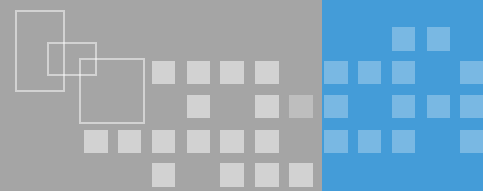
## ❖ 密码系统实际安全需要满足的准则：

- 破译该密码系统的实际计算量无法实现
- 破译该密码系统所需计算时间超过信息的生命周期
- 破译该密码系统的费用超过被加密信息本身的价值

# 密码学技术在信息安全中的应用



| 信息安全要素                                      | 所应付的典型威胁   | 可用的密码技术                    |
|---|--|----------------------------|
| 机密性<br>(Confidentiality)                    | <ul style="list-style-type: none"><li>● 窃听</li><li>● 非法窃取资料</li><li>● 敏感信息泄露</li></ul> | 对称加密和非对称加密<br>数字信封         |
| 完整性<br>(Integrity)                          | <ul style="list-style-type: none"><li>● 篡改</li><li>● 重放攻击</li><li>● 破坏</li></ul>       | 哈希函数和消息认证码<br>数据加密<br>数字签名 |
| 可鉴别性<br>(Authentication)                    | <ul style="list-style-type: none"><li>● 冒名</li></ul>                                   | 口令和共享秘密<br>数字证书和数字签名       |
| 不可否认性<br>(Non-repudiation)                  | <ul style="list-style-type: none"><li>● 否认已收到资料</li><li>● 否认已送资料</li></ul>             | 数字签名<br>证据存储               |
| 授权与访问控制<br>(Authorization & Access Control) | <ul style="list-style-type: none"><li>● 非法存取资料</li><li>● 越权访问</li></ul>                | 属性证书<br>访问控制               |



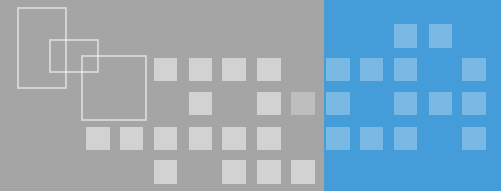
## ❖ 对称密码算法

- 理解对称密码算法的概念及算法特点；
- 了解DES、3DES、AES等典型对称密码算法。

## ❖ 公钥密码算法

- 理解非对称密码算法（公钥算法）的概念及算法特点；
- 了解RSA、SM2等典型非对称密码算法。

# 密码体制分类



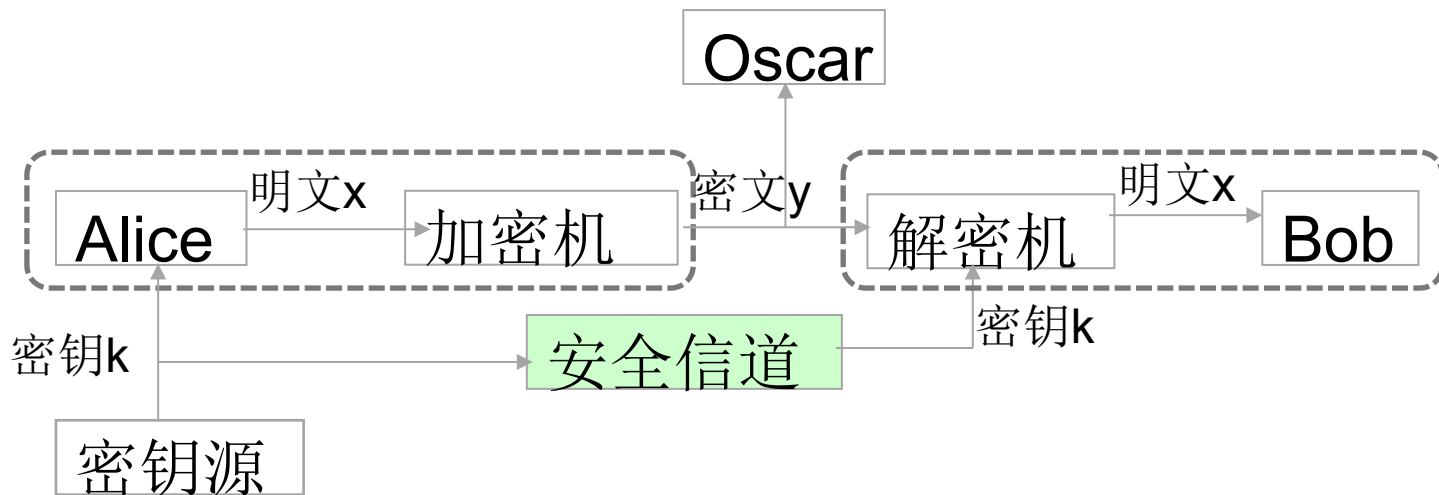
- (1) 受限制的算法 vs. 基于密钥的算法
- (2) 对称密码 vs. 非对称密码
- (3) 分组密码 vs. 流密码
- (4) 代替密码 vs. 置换密码

# 受限制的算法 vs. 基于密钥的算法

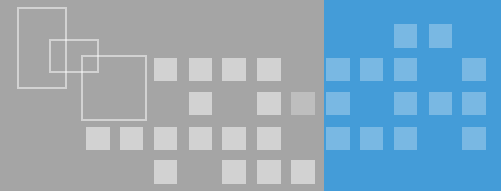
- ❖ **受限制的 (restricted) 算法**: 算法的保密性基于保持算法的秘密。
- ❖ **基于密钥 (key-based) 的算法**: 算法的保密性基于对密钥的保密。

# 对称密码算法

- ❖ **加密密钥和解密密钥相同**，或实质上等同
- ❖ 典型算法：DES、3DES、AES、IDEA等
- ❖ 优点：高效
- ❖ 不足：安全交换密钥问题及密钥管理复杂，无法解决消息的篡改、否认问题



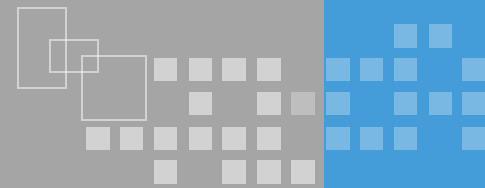
# 数据加密标准（DES）



- ❖ DES是一种对称密钥算法，密钥长度为56bits（加上奇偶校验，通常写成64bits）。
- ❖ 分组加密算法，64 bits为一个分组。
- ❖ 基本思想：
  - 混乱（Confusion）
  - 扩散（Diffusion）
- ❖ 使用标准的算术运算和逻辑运算。



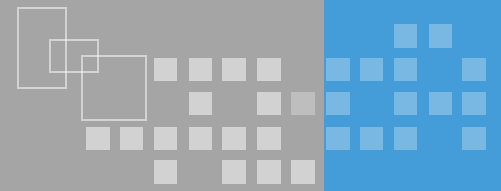
# 扩散 vs. 混乱



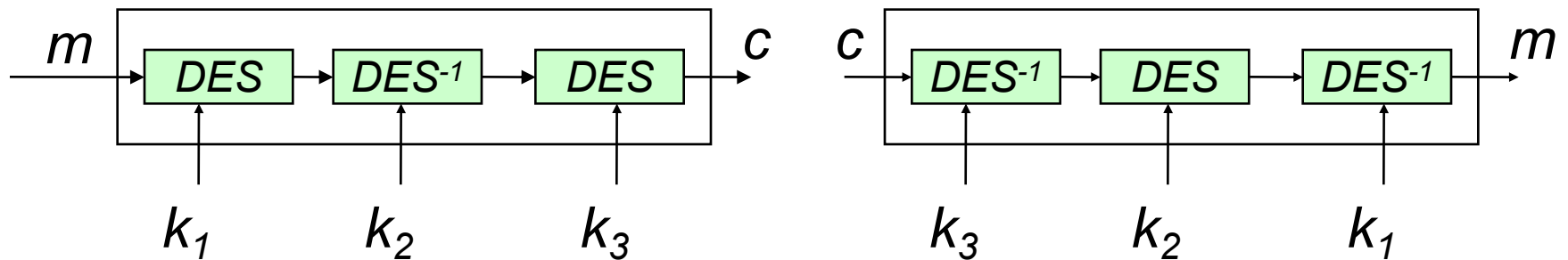
- ❖ **扩散 (Diffusion)** : 将每一位明文数字的影响尽可能地散布到多个输出密文数字中去, 以更隐蔽明文数字的统计特性。
- ❖ **混乱 (Confusion)** : 使得密文的统计特性与明文、密钥之间的关系尽量复杂化。

Shannon称: 在理想密码系统中, 密文的所有统计特性都与所使用的密钥独立。

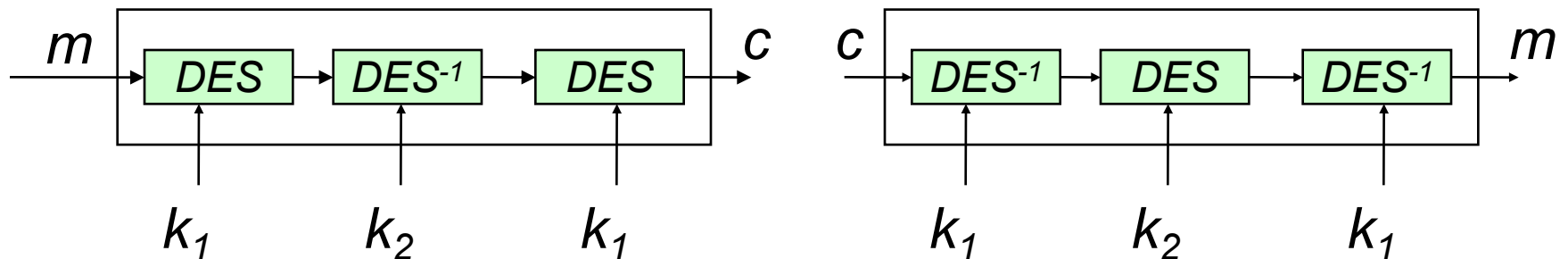
# 三重DES (3DES)



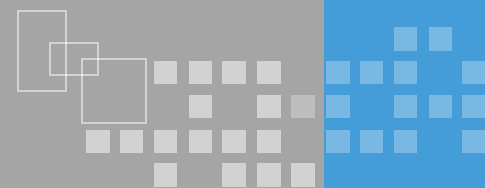
三重DES加密，密钥长度为168比特,  $k=k_1k_2k_3$



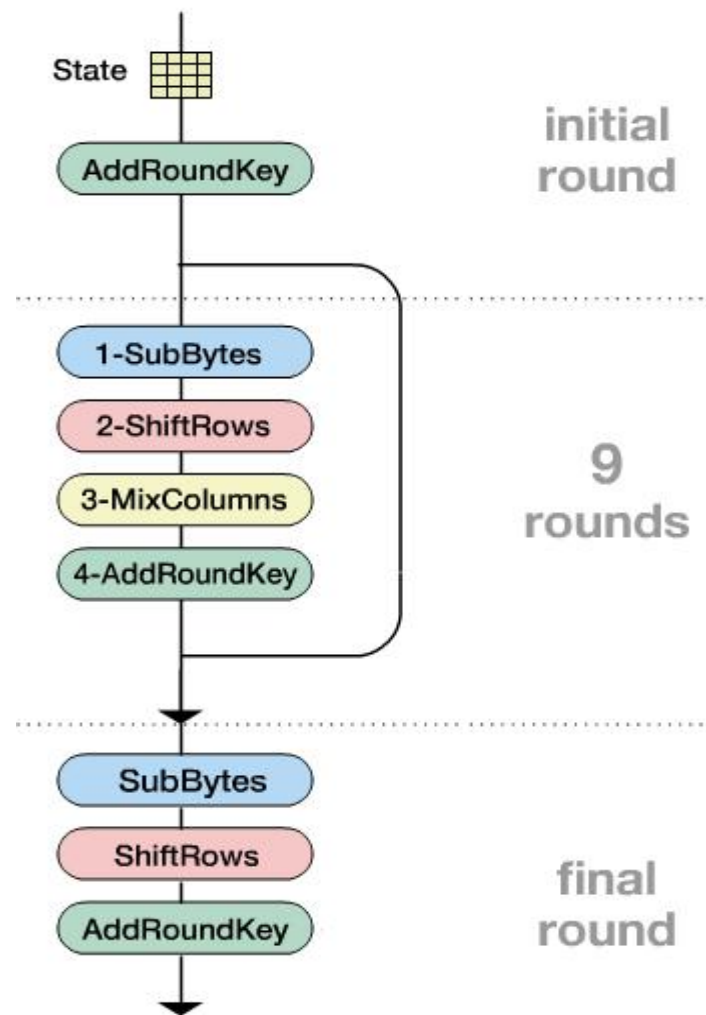
双密钥三重**DES**加密，密钥长度为**112**比特,  $k=k_1k_2$



# 高级数据加密标准 (AES)



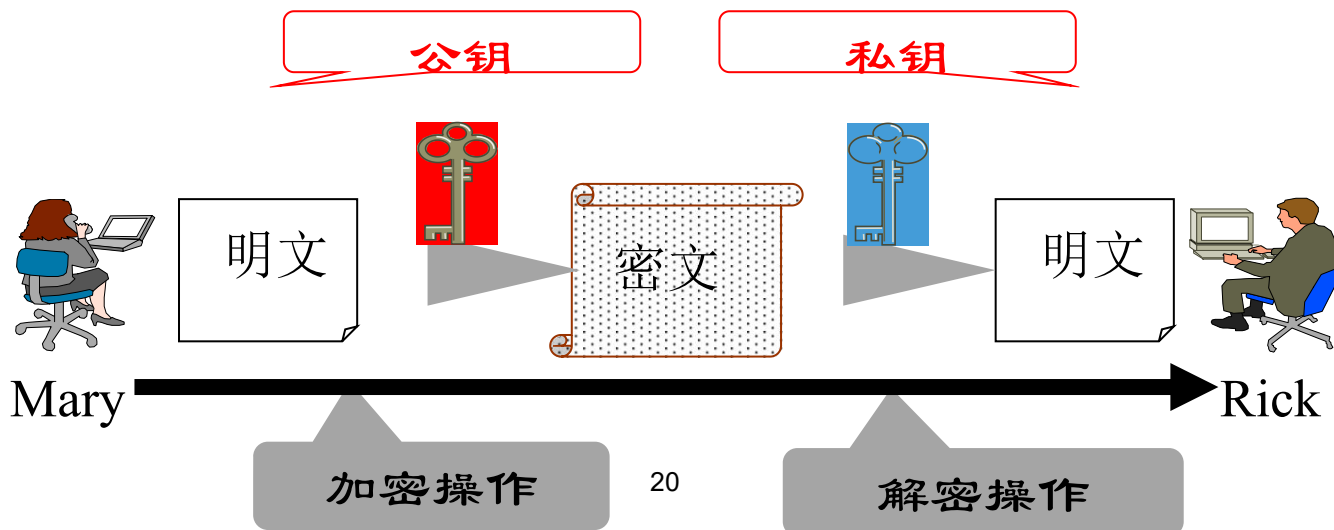
- 1、数据分组长度128bits;
- 2、密钥长度128/192/256 bits;
- 3、加密过程是在一个 $4 \times 4$ 的字节矩阵 (state) 上实施
- 4、能有效抵抗目前已知的攻击算法
  - 线性攻击、差分攻击



*AES-128*

# 非对称密码算法

- ❖ 密钥成对（公钥，私钥）
  - 公钥加密私钥解、私钥加密公钥解
- ❖ 典型算法：RSA、ECC、 ElGamal
- ❖ 优点：解决密钥传递问题、密钥管理简单、提供数字签名等其他服务
- ❖ 缺点：计算复杂、耗用资源大



# 常用的公钥密码算法



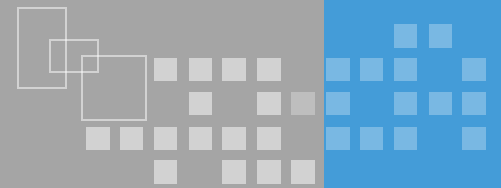
RSA (Rivest - Shamir – Adleman) , 1977

- 在一个算法中实现签名和加密
- 私钥：签名和解密
- 公钥：签名检验和加密

❖ RSA是一种分组加密算法。明文和密文在 $0 \sim n-1$ 之间， $n$ 是一个正整数。

❖ 该算法的数学基础是初等数论中的Euler（欧拉）定理，并建立在大整数因子的困难性之上。

❖ 目前应用最广泛的公钥密码算法。



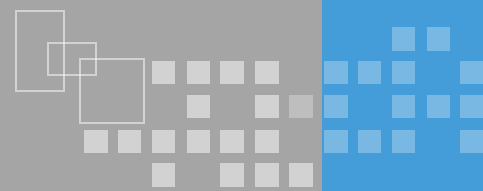
ECC (Elliptic Curve Cryptosystem), 1985

- 基于有限域上椭圆曲线有理点群的密码系统
- 更快的具有更小密钥长度的公开密码系统
- 功能同RSA: 数字签名, 密钥管理, 加密

## 椭圆曲线密钥协商

- 基于椭圆曲线的密钥协商问题, 即ECC Diffie-Hellman

# 公钥密码体制的优缺点



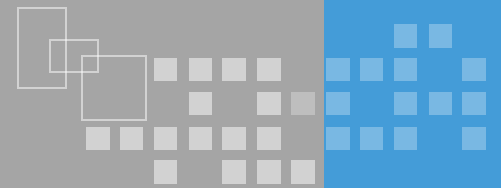
## ❖ 优点：

- 解决密钥传递的问题
- 大大减少密钥持有量
- 提供了对称密码技术无法或很难提供的服务（数字签名）

## ❖ 缺点：

- 计算复杂、耗用资源大
- 非对称会导致得到的密文变长

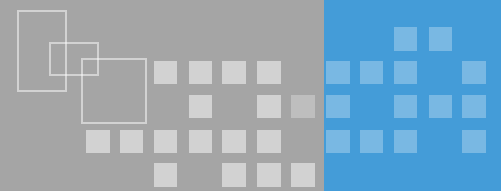
# 分组密码 vs. 流密码



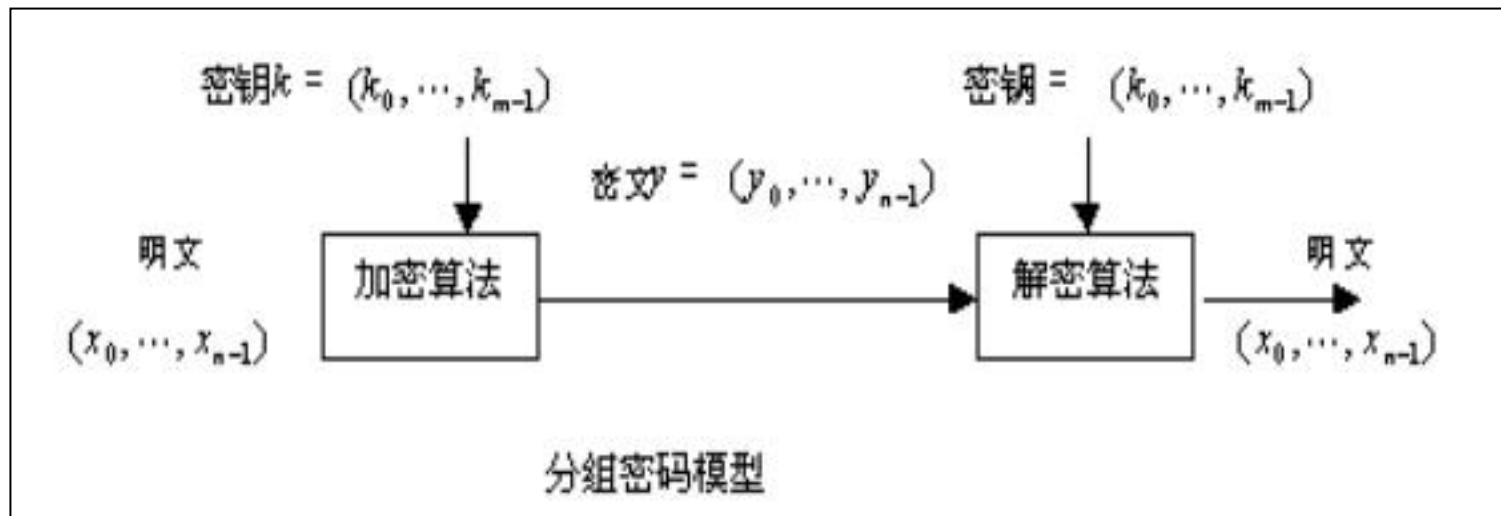
- ❖ **分组密码 (Block cipher)** : 将明文分成固定长度的组, 用同一密钥和算法对每一块加密, 输出也是固定长度的密文。——DES、IDEA、RC2、RC5
- ❖ **序列密码 (Stream cipher)** : 又称**流密码**, 序列密码每次加密一位或一字节的明文。——One-time padding、Vigenère、Vernam



# 分组密码模型



**分组密码**是将明文消息编码表示后的数字（简称明文数字）序列，划分成长度为 $n$ 的组（可看成长度为 $n$ 的矢量），每组分别在密钥的控制下变换成等长的输出数字（简称密文数字）序列。



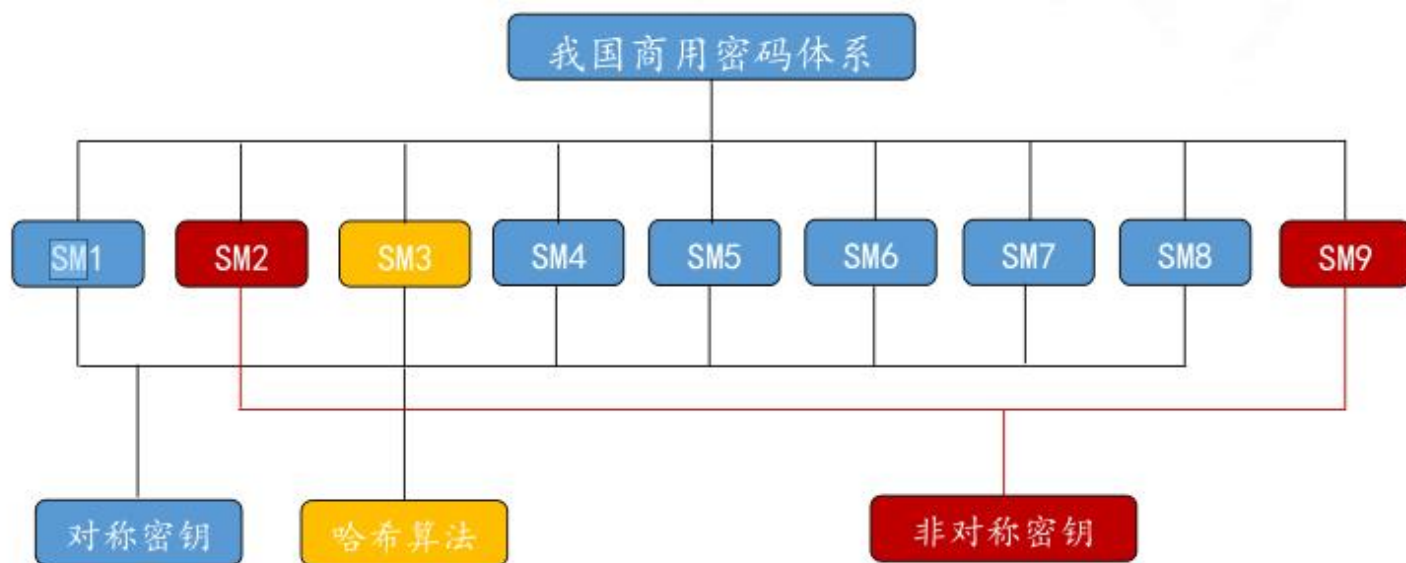
# 代替密码 Vs. 置换密码



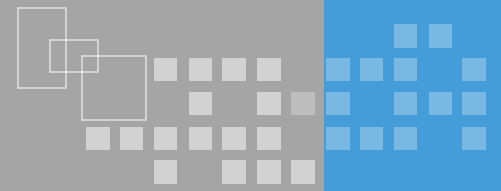
❖ **代替密码 (Substitution Cipher)** : 就是明文中的每一个字符被替换成密文中的另一个字符。接收者对密文做反向替换就可以恢复出明文。

❖ **置换密码 (Transposition Cipher)** : 明文的字母保持相同, 但顺序被打乱了。

# 我国密码体系

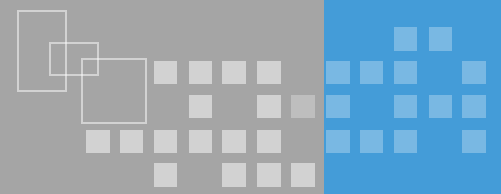


为了保障商用密码的安全性，国家商用密码管理办公室制定了一系列密码标准，包括SSF33、SM1 (SCB2)、SM2、SM3、SM4、SM7、SM9、祖冲之密码算法那等等。其中SSF33、SM1、SM4、SM7、祖冲之密码是对称算法；SM2、SM9是非对称算法，并于2017年成为ISO国际标准；SM3是哈希算法。



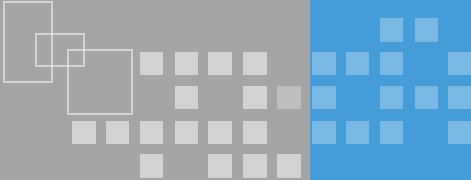
以下关于代替密码的说法正确的是：

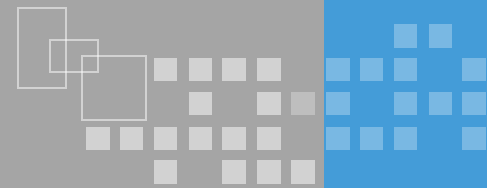
- ❖ A. 明文根据密钥被不同的密文字母代替
- ❖ B. 明文字母不变，仅仅是位置根据密钥发生改变
- ❖ C. 明文和密钥的每个 bit 异或
- ❖ D. 明文根据密钥作了移位



分组密码算法是一类十分重要的密码算法，下面描述中，错误的是（）

- ❖ A. 分组密码算法要求输入明文按组分成固定长度的块
- ❖ B. 分组密码算法每次计算得到固定长度的密文输出块
- ❖ C. 分组密码算法也称为序列密码算法
- ❖ D. 常见的 DES、IDEA 算法都属于分组密码算法

- 
- ❖ 关于密钥管理，下列说法错误的是：
  - ❖ A. 科克霍夫原则指出算法的安全性不应基于算法的保密，而应基于密钥的安全性
  - ❖ B. 保密通信过程中，通信方使用之前用过的会话密钥建立会话，不影响通信安全
  - ❖ C. 密钥管理需要考虑密钥产生、存储、备份、分配、更新、撤销等生命周期过程的每一个环节
  - ❖ D. 在网络通信中。通信双方可利用 Diffie-He11man 协议协商出会话密钥



## ❖ 其他密码服务

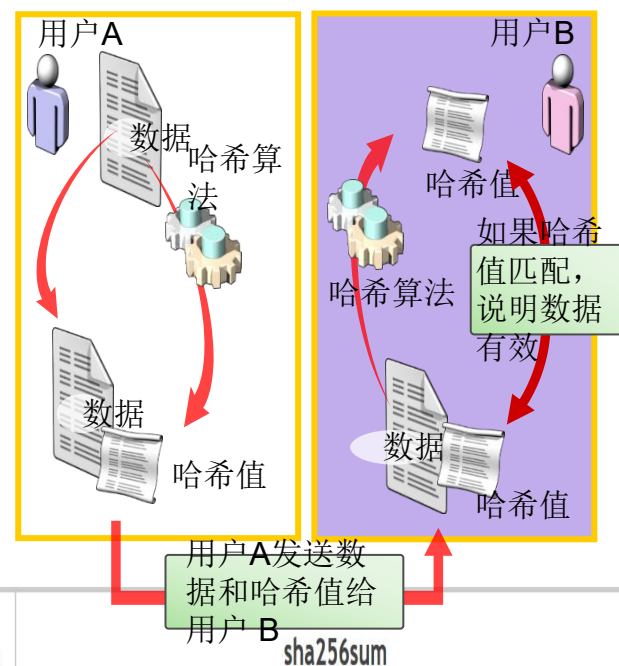
- 理解哈希函数、消息认证码、数字签名等密码服务的作用。

## ❖ 公钥基础设施

- 了解PKI的基本概念及PKI体系构成；
- 理解CA及其他组件在PKI体系中的作用；
- 掌握PKI的应用场景。

# 哈希函数

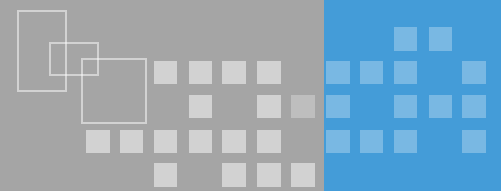
- ❖ 哈希函数是能将任意长度的数据映射成为一个定长的字段的函数
- ❖ 作用：数据完整性检查
- ❖ 典型算法：MD5、SHA-1
- ❖ 数学性质
  - 单向性
  - 弱抗碰撞性
  - 强抗碰撞性



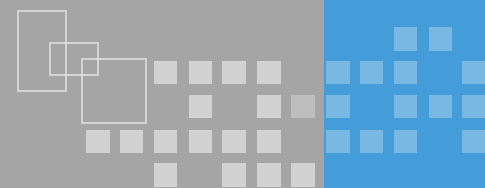
| Version |   |
|---------|---|
| 2018.2  | 56f677e2edfb2efcd0b08662dde824e254c3d53567ebbbcd9bf5c03efd9bc0f |



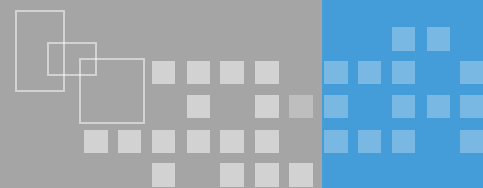
# 哈希函数的特点



- ❖ H能够应用到任意长度的数据上。
- ❖ H能够生成大小固定的输出。
- ❖ 对于任意给定的 $x$ ,  $H(x)$ 的计算相对简单。
- ❖ 对于给定的散列值 $h$ , 要发现满足 $H(x) = h$ 的 $x$ 在计算上是不可行的。
- ❖ 对于给定的消息 $x$ , 要发现另一个消息 $y$ 满足 $H(y) = H(x)$ 在计算上是不可行的。



- ❖ 在网络通信中，有一些针对消息内容的攻击方法
  - 伪造消息
  - 篡改消息内容
  - 改变消息顺序
  - 消息重放或者延迟
- ❖ 消息认证：对收到的消息进行验证，证明确实是来自声称的发送方，并且没有被修改过。
  - 如果在消息中加入时间及顺序信息，则可以完成对时间和顺序的认证



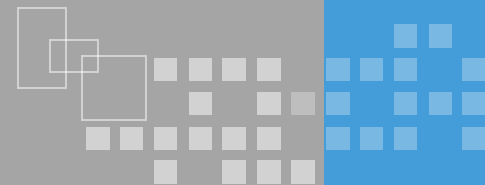
## ❖ 基本特点

- 也称消息鉴别码（Message Authentication Code，MAC）
- 利用密钥来生成一个固定长度的短数据块，并将该数据块附加在消息之后

## ❖ 作用：完整性校验、时间和顺序验证

## ❖ 实现算法

- 分组链消息鉴别码（CBC-MAC）
- 基于哈希函数的MAC（HMAC）



## ❖ 把HASH值和一个Key结合起来

- 不需要可逆

## ❖ 目标

- 既能使用当前的HASH函数，又可容易升级为新的HASH函数，并能保持散列函数的安全性
- 简单，并易进行密码学分析

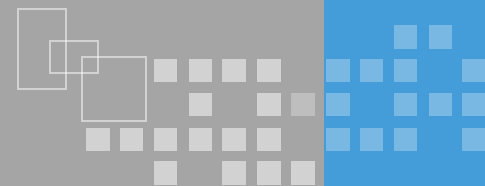
## ❖ 发送者否认发送过消息，声称是别人伪造。

## ❖ 接收者伪造消息，声称其由某发送者发送。

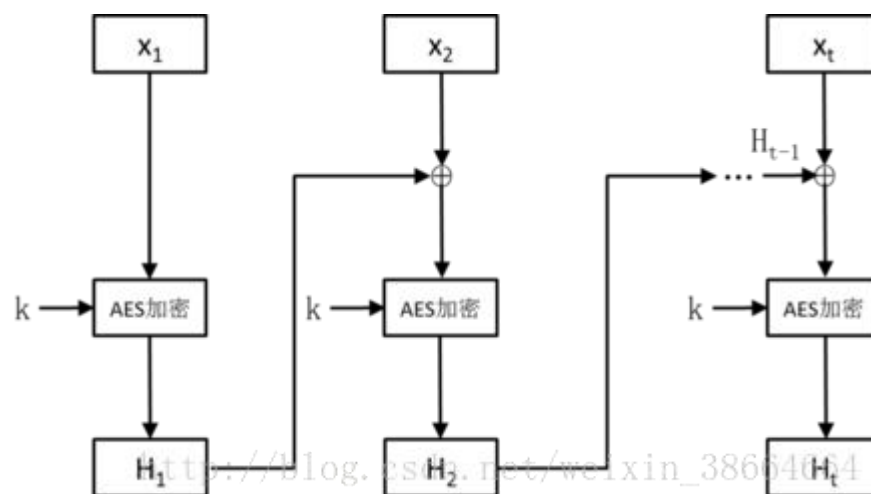
## ❖ 解决办法

- 不可否认性

# CBC-MAC



CBC MAC是基于IEEE 802.1x认证的加密技术，以AES(Advanced Encryption Standard)为核心算法，采用CBC-MAC加密模式，具有分组序号的初始向量。



- 填充和分组：对消息 $x$ 进行填充，将填充得到的消息分成 $t$ 个 $n$ 比特的分组，记为 $x_1, x_2, \dots, x_t$ 。
- $H_t$ 就是 $x$ 的消息认证码

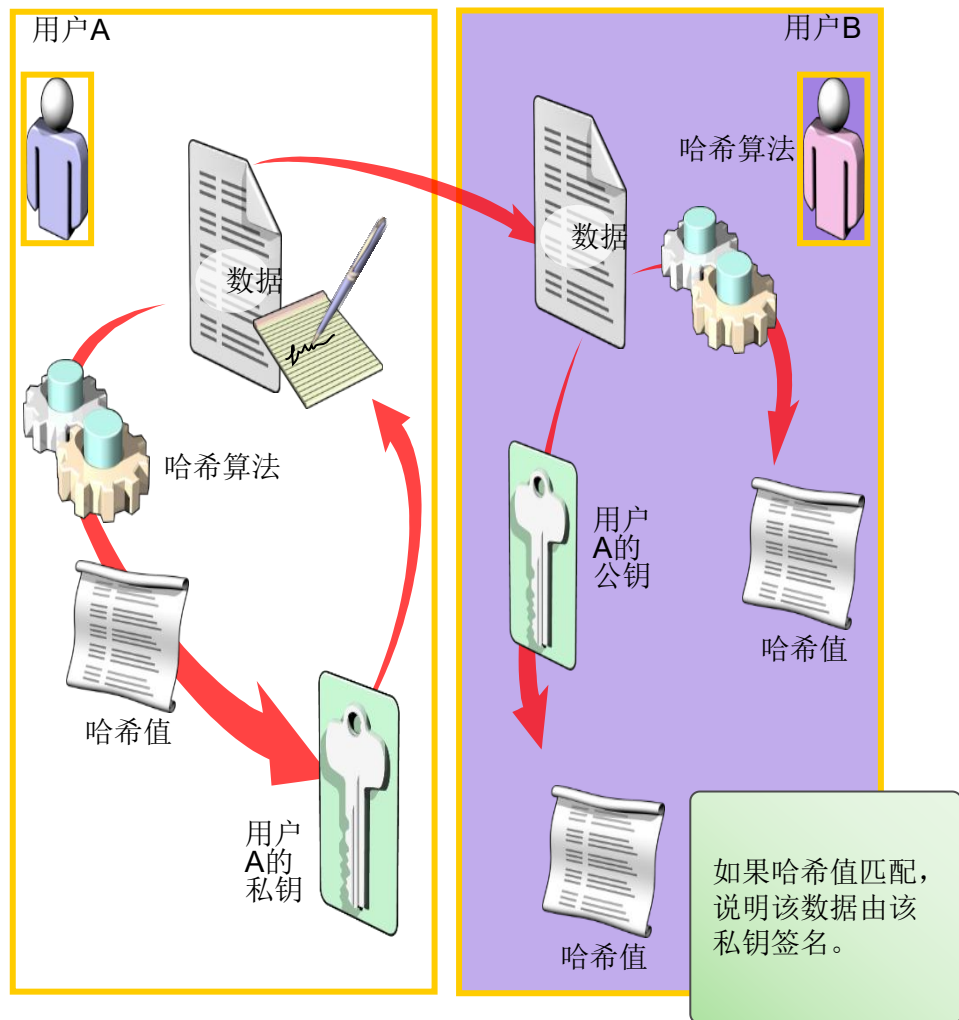
# 数字签名

## ❖ 基本特性

- 不可伪造性
- 不可否认性
- 完整性

## ❖ 应用示例

- 发送过程
- 接收过程



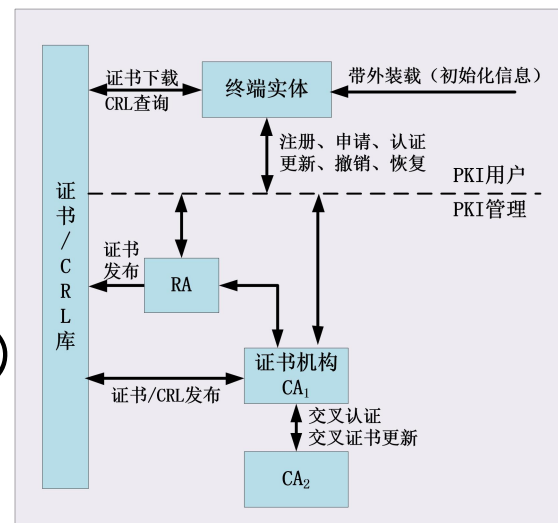
# 公钥基础设施 (PKI)

## ❖ 定义

- PKI是一个包括硬件、软件、人员、策略和规程的集合，用来实现基于公钥密码体制的密钥和证书的产生、管理、存储、分发和撤销等功能

## ❖ PKI 架构

- CA（认证权威）
- RA（注册权威）
- 证书存放管理（目录服务）
- 终端实体（证书持有者和应用程序）



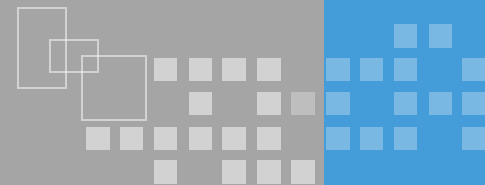
# CA: 认证权威

- ❖ 签发证书
- ❖ 更新证书
- ❖ 管理证书
  - 撤销、查询
  - 审计、统计
- ❖ 验证数字证书
  - 黑名单认证 (CRL)
  - 在线认证 (OCSP)

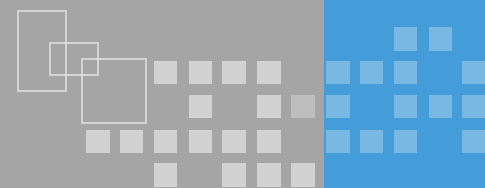


CA是PKI体系的核心





- ❖ 受理用户的数字证书申请
  - 对证书申请者身份进行审核并提交CA制证
  - 类似于申请身份证的派出所
- ❖ 提供证书生命期的维护工作
  - 受理用户证书申请
  - 协助颁发用户证书
  - 审核用户真实身份
  - 受理证书更新请求
  - 受理证书吊销

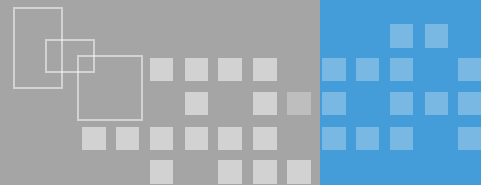


## ❖ 证书存放管理

- 信息的存储库，提供了证书的保存，修改，删除和获取的能力
- 采用LDAP标准的目录服务存放证书，其作用与数据库相同，优点是在修改操作少的情况下，对于访问的效率比传统数据库要高

## ❖ CRL (Certificate Revocation List) : 证书撤销列表，也称“证书黑名单”

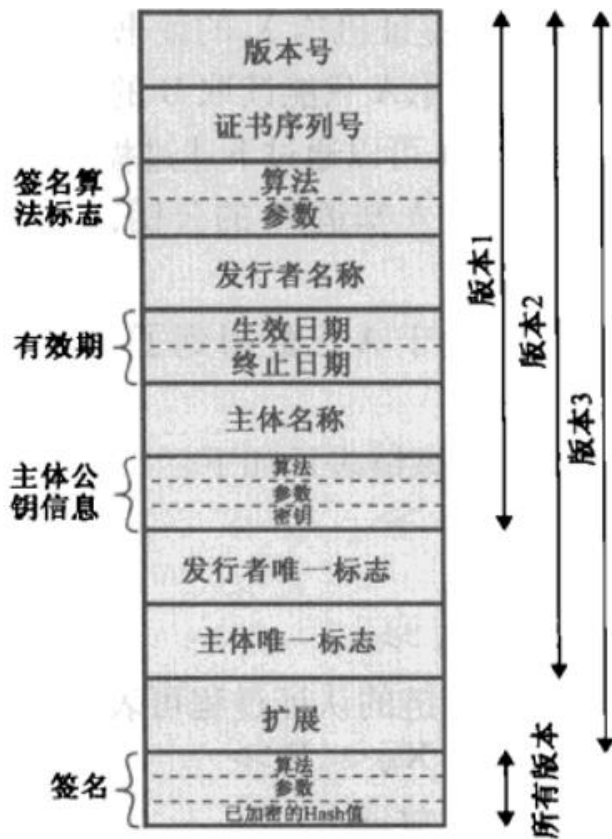
- 被撤销证书的序列号
- 证书有效期期间因为某种原因（人员调动、私钥泄漏等）导致证书不再真实可信，因此需要进行证书撤销



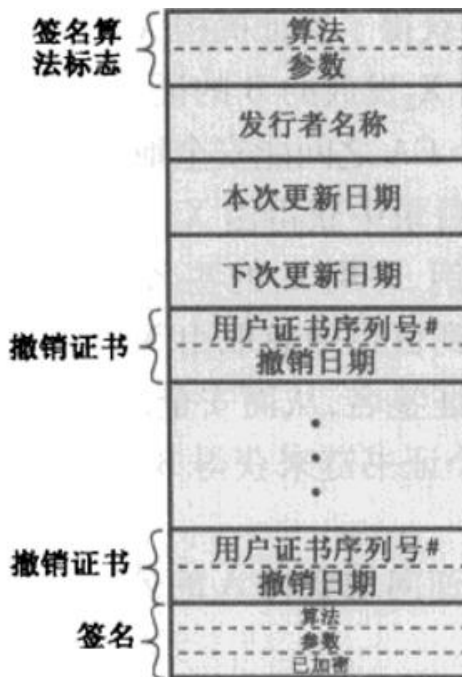
## ❖ 数字证书

- 经证书权威机构CA签名的、包含拥有者身份信息和公开密钥的数据体
  - 国际标准X. 509定义了电子证书的规范格式
- ❖ 拥有公私密钥对和相应公钥证书的最终用户，可以是人、设备、进程等

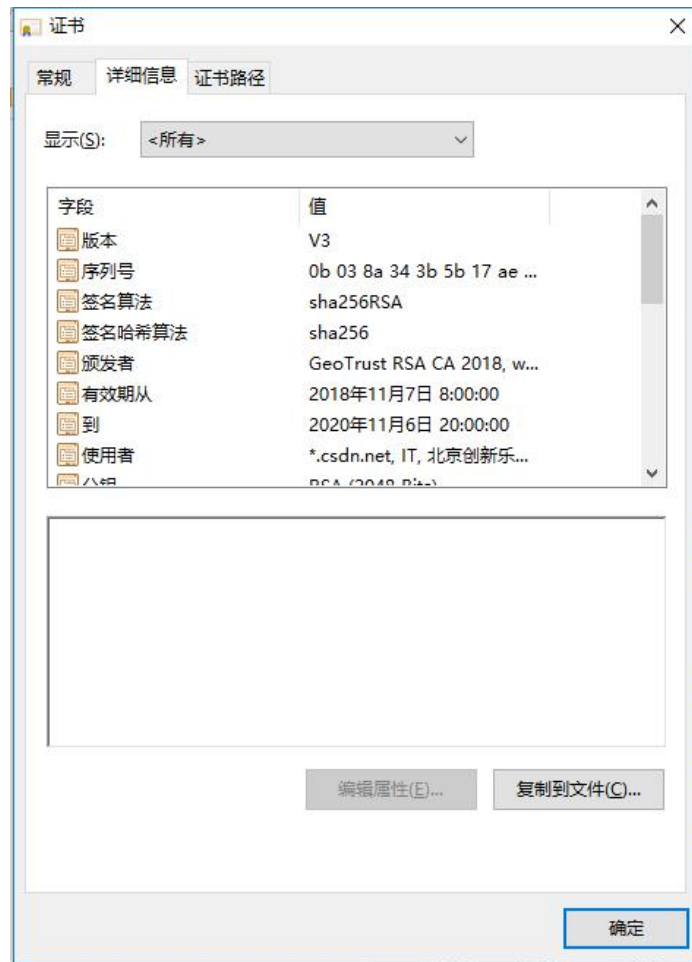
# 电子证书格式



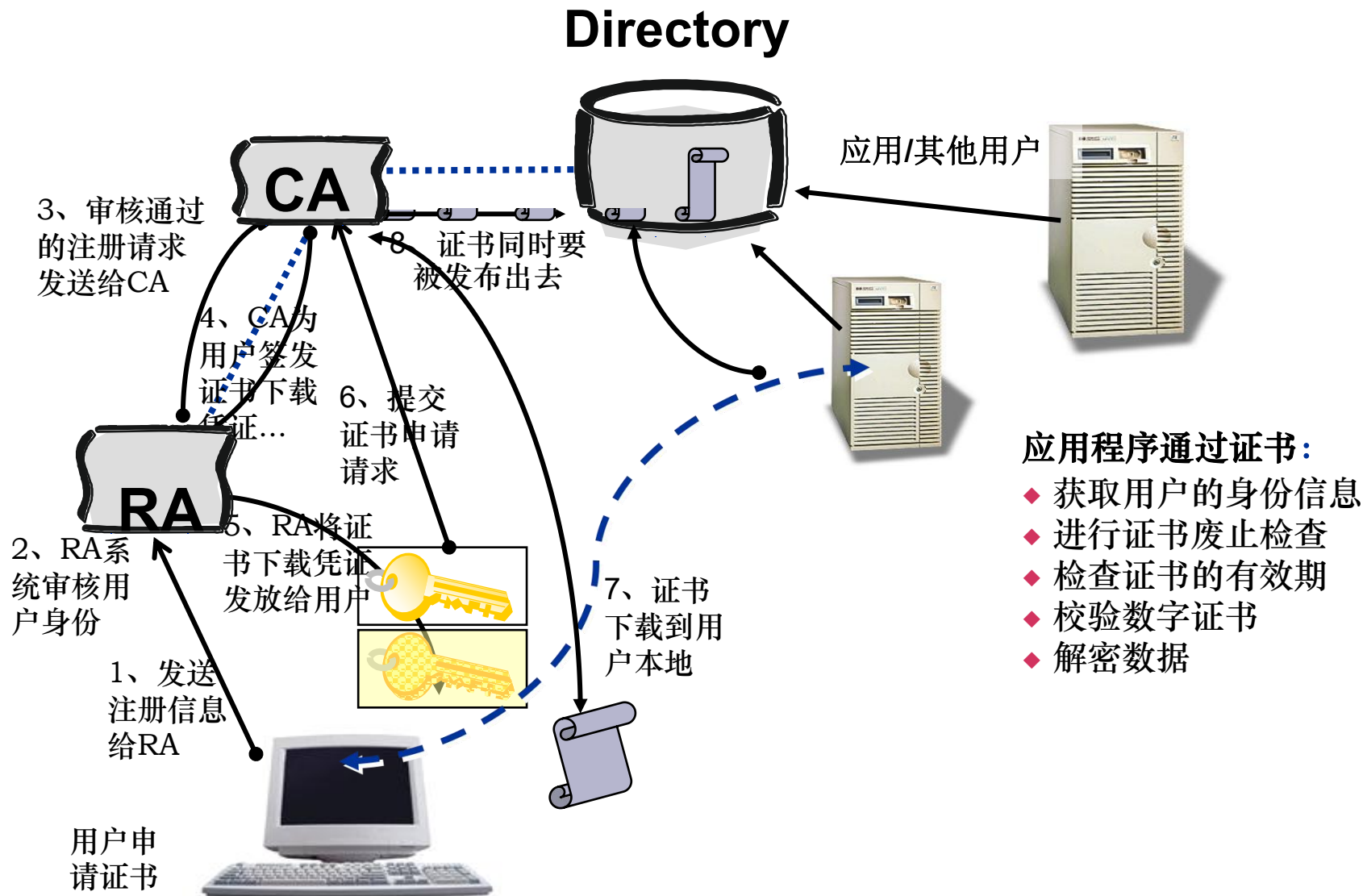
(a) X.509证书



(b) 证书撤销链

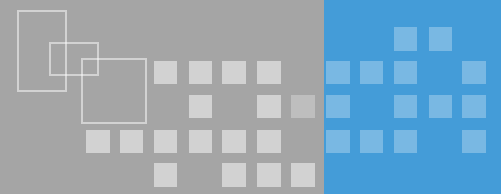


# PKI 体系工作流程

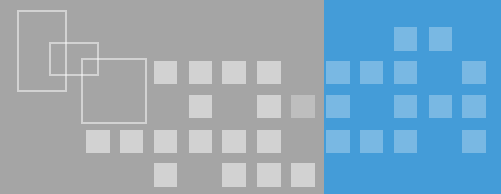


# PKI/CA技术的典型应用





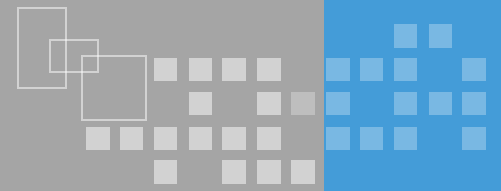
- ❖ 常用的混合加密 (Hybrid Encryption) 方案指的是:
- ❖ A. 使用对称加密进行通信数据加密, 使用公钥加密进行会话密钥协商
- ❖ B. 使用公钥加密进行通信数据加密, 使用对称加密进行会话密钥协商
- ❖ C. 少量数据使用公钥加密, 大量数据则使用对称加密
- ❖ D. 大量数据使用公钥加密, 少量数据则使用对称加密



为什么在数字签名中含有消息摘要？

- ❖ A. 防止发送方否认发送过消息
- ❖ B. 加密明文
- ❖ C. 提供解密密码
- ❖ D. 可以确认发送内容是否在途中被他人修改





公钥基础设施（**Public Key Infrastructure, PKI**）引入数字证书的概念，用来表示用户的身份。下图简要地描述了终端实体（用户）从认证权威机构**CA** 申请、撤销和更新数字证书的流程。请为中间框空白处选择合适选项（ ）

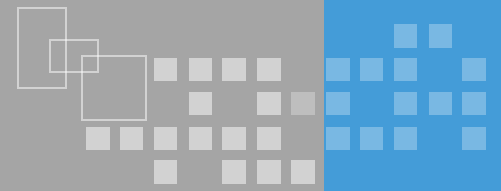


- A. 证书库
- B. RA
- C. OCSP
- D. CRL 库

下列哪个选项是公钥基础设施（**PKI**）的密钥交换处理流程？

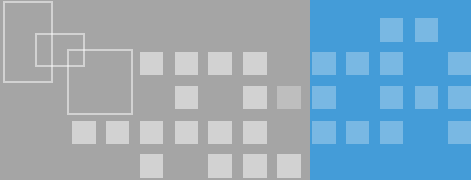
- 1) 接收者解密并获取会话密钥
- 2) 发送者请求接收者的公钥
- 3) 公钥从公钥目录中被发送出去
- 4) 发送者发送一个由接收者的公钥加密过的会话密钥

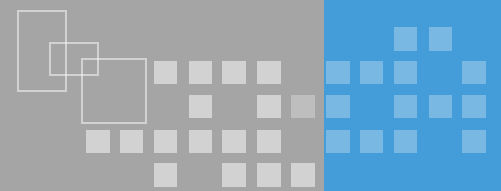
- A. 4,3,2,1
- B. 2,1,3,4
- C. 2,3,4,1
- D. 2,4,3,1



关于公钥基础设施/认证中心(PKI/CA)证书, 下面哪一种说法是错误的:

- ❖ A. 证书上具有证书授权中心的数字签名
- ❖ B. 证书上列有证书拥有者的基本信息
- ❖ C. 证书上列有证书拥有者的公开密钥
- ❖ D. 证书上列有证书拥有者的秘密密钥

- 
- ❖ 电子认证服务提供者签发认证证书内容不必须包括以下哪一项：
  - ❖ A. 电子认证服务提供者名称，证书持有人名称
  - ❖ B. 证书序列号，证书有效期
  - ❖ C. 证书使用范围
  - ❖ D. 电子认证服务提供者的电子签名



## ❖ 身份鉴别的概念

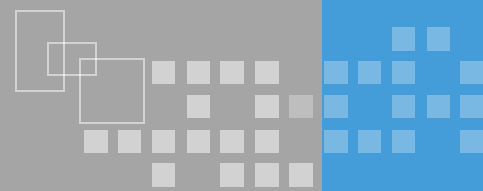
- 理解标识与鉴别、鉴别类型、鉴别方式等基本概念

## ❖ 基于实体所知的鉴别

- 理解基于实体所知的鉴别方式及特点；
- 了解口令破解、嗅探、重放攻击等针对实体所知鉴别方式的攻击方式；
- 掌握对抗口令破解的防御措施；
- 理解对抗嗅探攻击、重放攻击的防御措施。



- ❖ 标识的概念：标识是**实体身份**的一种计算机表达，每个实体与计算机内部的一个身份表达绑定
- ❖ 鉴别：**确认实体是它所声明的**，提供了关于某个实体身份的保证，某一实体确信与之打交道的实体正是所需要的实体
- ❖ 标识与鉴别的作用
  - 作为访问控制的一种必要支持，访问控制的执行依赖于确知的身份
  - 作为数据源认证的一种方法
  - 作为审计追踪的支持



## ❖ 鉴别系统的构成

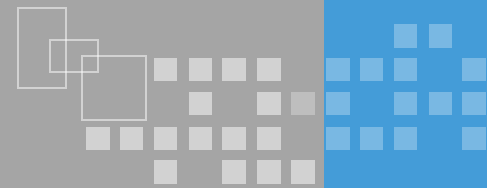
- 验证者、被验证者、可信赖者

## ❖ 鉴别的类型

- 单向鉴别、双向鉴别、第三方鉴别

## ❖ 鉴别的方式

- 基于实体所知（知识、密码、PIN码等）
- 基于实体所有（身份证、钥匙、智能卡、令牌等）
- 基于实体特征（指纹，笔迹，声音，视网膜等）
- 双因素、多因素认证

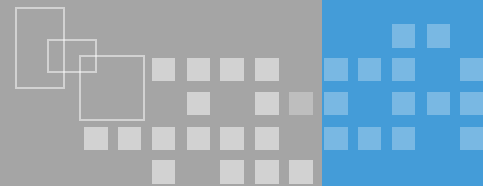


## ❖ 使用最广泛的身份鉴别方法

- 实现简单、成本低
- 提供弱鉴别

## ❖ 面临的威胁

- 暴力破解
- 木马窃取
- 线路窃听
- 重放攻击
- .....



## ❖ 暴力破解防护

- 使用安全的密码（自己容易记，别人不好猜）
- 系统、应用安全策略（帐号锁定策略）
- 随机验证码
  - 变形
  - 干扰
  - 滑块
  - 图像识别
  - .....

验证码:



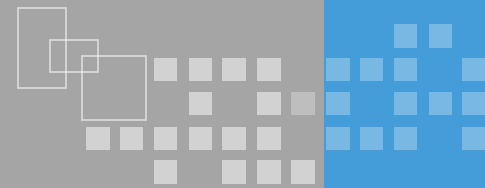


# 木马窃取密码安全防护

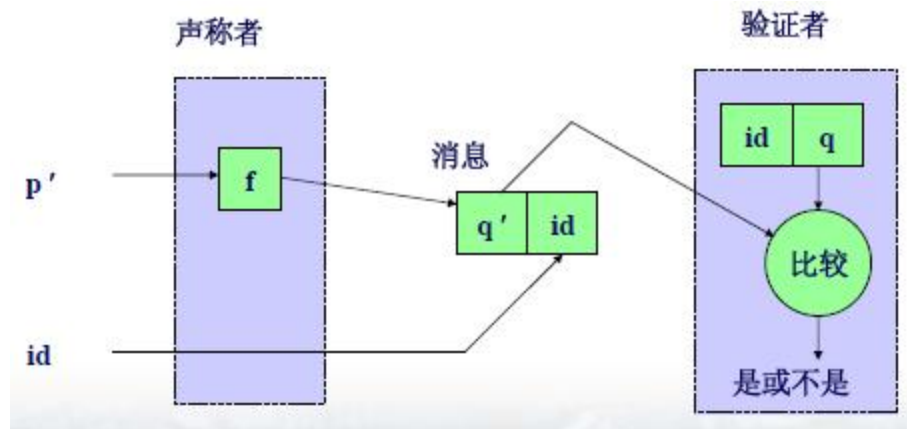
## ❖ 使用密码输入控件

- 安全的输入框，避免从输入框中还原密码
- 软键盘，对抗击键记录
- 随机排列字符，对抗屏幕截图重现

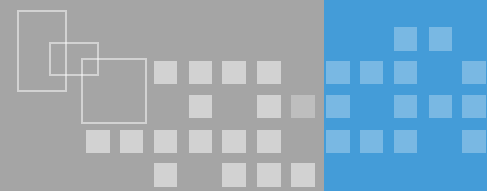




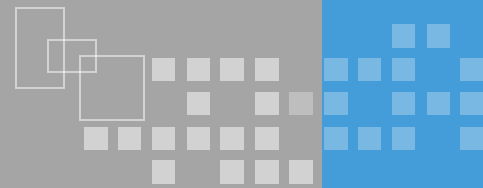
## ❖ 加密：单向函数



- ❖ 攻击者很容易构造一张 $q$ 与 $p$ 对应的表，表中的 $p$ 尽可能包含所期望的值
  - 解决办法：在口令中使用随机数

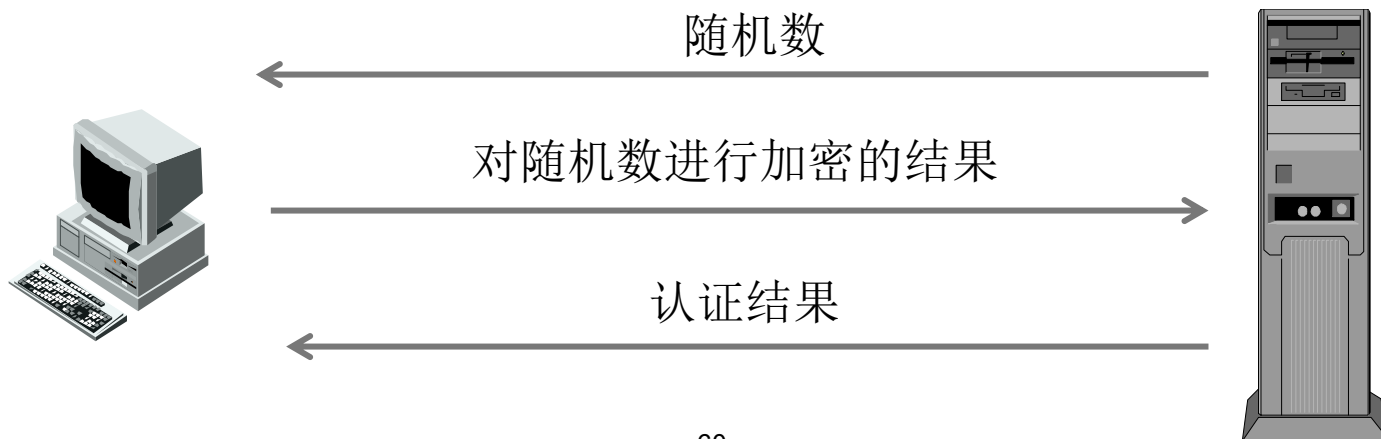


- ❖ 一次性口令：每次鉴别中所使用的密码不同
  - 有效应对密码嗅探及重放攻击
- ❖ 实现机制
  - 两端共同拥有一串随机口令，在该串的某一位置保持同步
  - 两端共同使用一个随机序列生成器，在该序列生成器的初态保持同步
  - 使用时间戳，两端维持同步的时钟



## ❖ 挑战机制

- 客户端：请求登录
- 服务器：给出随机数作为挑战请求
- 将登录信息（用户名、密码）与随机数合并，使用单向函数（如MD5）生产字符串，作为应答返回服务器
- 服务认证后返还结果





## ❖ 基于实体所有的鉴别

- 理解基于实体所有的鉴别方式及特点；
- 了解集成电路卡、内存卡、安全卡、CPU卡等常用鉴别物品。

## ❖ 基于实体特征的鉴别

- 理解基于实体特征的鉴别方式及特点；
- 了解指纹、虹膜、声纹等常用的生物识别技术；
- 理解基于实体特征鉴别有效性判定的方法。

# 基于实体所有的鉴别方法



## ❖ 采用较多的鉴别方法

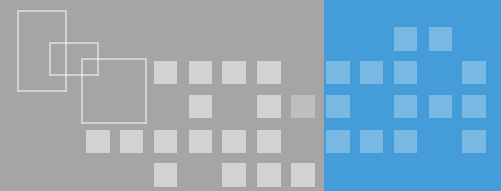
- 使用用户所持有的东西来验证用户的身份
- 用于鉴别的东西通常不容易复制

## ❖ 鉴别物体

- IC卡（Integrated Circuit Card）是将一个微电子芯片嵌入符合卡基，做成卡片形式的信息载体
  - 内存卡
  - 逻辑加密卡
  - CPU卡

## ❖ 特点

- 难以复制、安全性高



## ❖ 安全威胁及防护

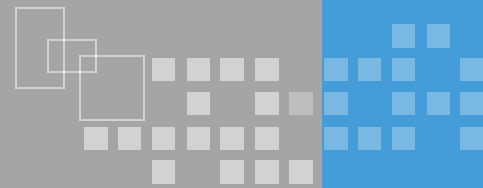
### ■ 损坏

- 封装应坚固耐用，承受日常使用中各种可能导致卡片损坏的行为

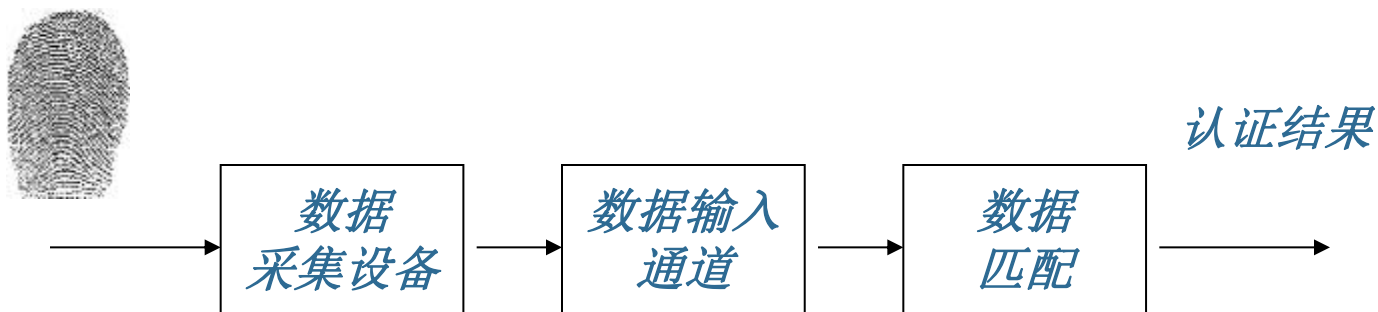
### ■ 复制

- 保证IC卡中存储和处理的各种信息不被非法访问、复制、篡改或破坏PIN码甚至其他技术实现对数据的安全防护
- 确保逻辑安全措施得到落实

# 基于实体特征的鉴别方法



## ❖ 使用每个人所具有的唯一生理特征



## ❖ 鉴别的方式

- 指纹、掌纹、静脉
- 虹膜、视网膜
- 语音
- 面部扫描



# 基于实体特征的鉴别-指纹、掌纹、静脉

## ❖ 指纹

- 手指上一些曲线和分叉以及一些非常微小的特征

## ❖ 手掌

- 手掌有折痕，起皱，还有凹槽
- 还包括每个手指的指纹
- 人手的形状（手的长度，宽度和手指）表示了手的几何特征



## ❖ 静脉

- 个人静脉分布图（指静脉、掌静脉）



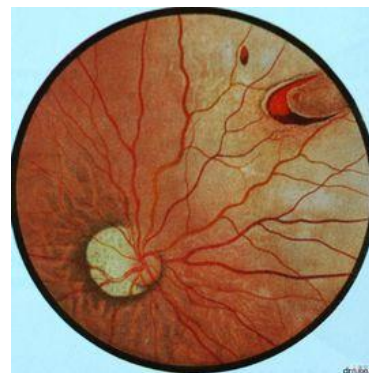
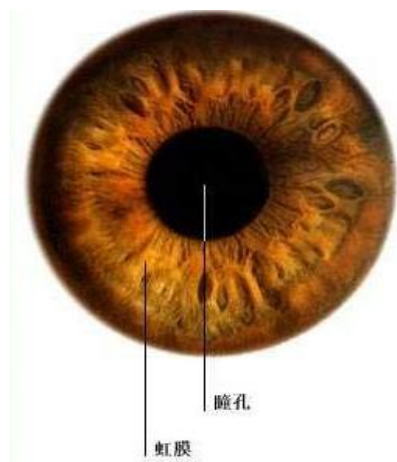
# 基于实体特征的鉴别-虹膜，视网膜

## ❖ 虹膜

- 使用环绕在瞳孔四周有色彩的部分作为识别特征
- 出生6~18个月成型后终生不变

## ❖ 视网膜

- 使用视网膜上面的血管分布作为识别特征



# 基于实体特征的鉴别-语音、面部

## ❖ 语音

- 使用语音、语速、语调等作为识别特征

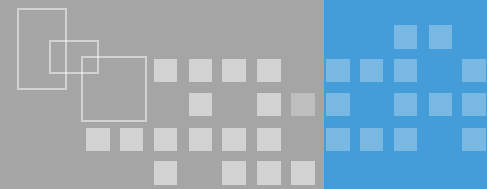
## ❖ 面部

- 人都有不同的骨骼结构，鼻梁，眼眶，额头和下颚形状

## ❖ 特点

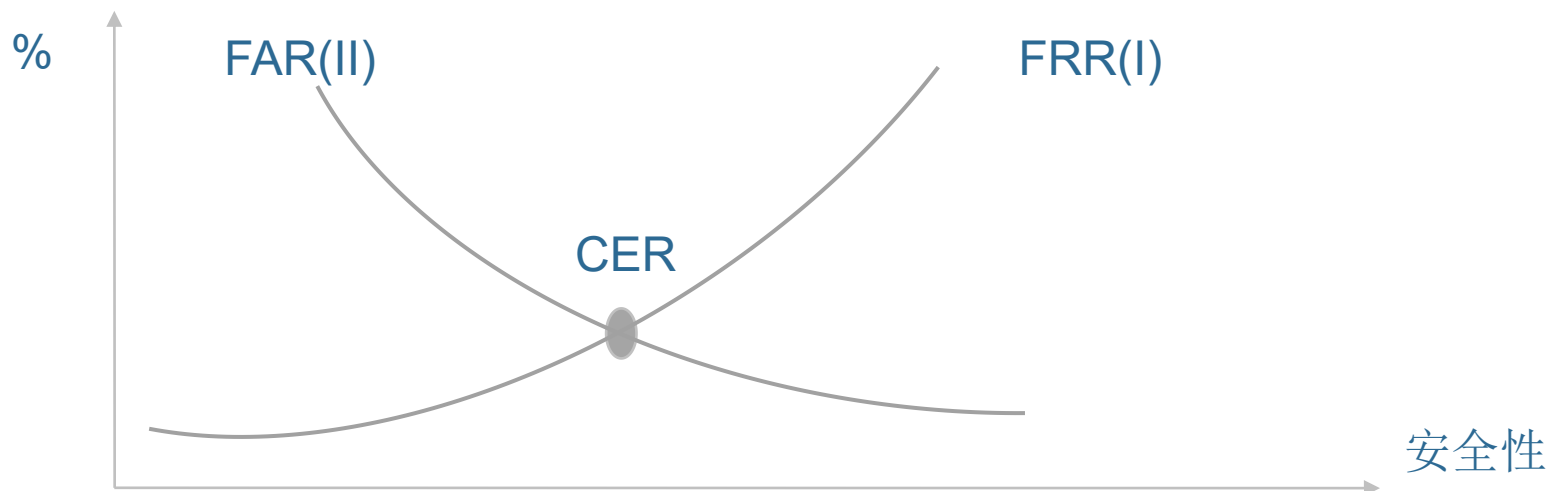
- 易于实现
- 安全性不高

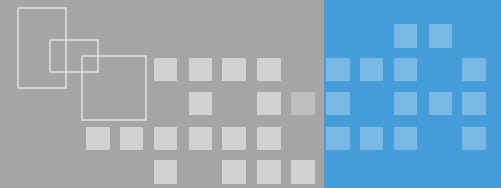




## ❖ 鉴别系统的有效性判断

- 错误拒绝率 (FRR)
- 错误接受率 (FAR)
- 交叉错判率 (CER) :  $FRR = FAR$  的交叉点, CER用来反映系统的准确度



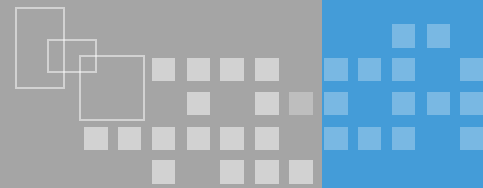


## ❖ kerberos体系

- 理解单点登录概念及其特点；
- 了解Kerberos体系架构及基本认证过程。

## ❖ 认证、授权和计费

- 了解AAA的概念及RADIUS、TACACS+协议特点。

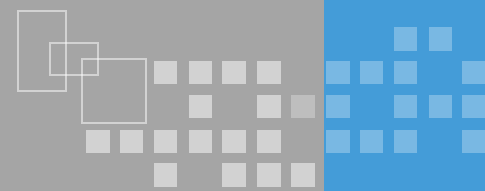


## ❖ 单点登录概念

- 单一身份认证，身份信息集中管理，一次认证就可以访问其授权的所有网络资源
- 单点登录实质是安全凭证在多个应用系统之间的传递或共享

## ❖ 单点登录的安全优势

- 减轻安全维护工作量，减少错误
- 提高效率
- 统一安全可靠的登录验证

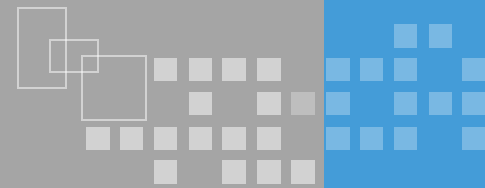


## ❖ 什么是Kerberos协议

- 1985年由美国麻省理工学院开发，用于通信实体间的身份认证，1994年V5版本作为Internet标准草案公布
- 基于对称密码算法为用户提供安全的单点登录服务
- 包含可信第三方认证服务

## ❖ Kerberos协议的优点

- 避免本地保存密码及会话中传输密码
- 客户端和服务端可实现互认



## ❖ 运行环境构成

- 密钥分发中心（KDC）
  - 系统核心，负责维护所有用户的账户信息
  - 由AS和TGS两个部分构成
    - 认证服务器（AS:Authentication Server）
    - 票据授权服务器（TGS:Ticket Granting Server）
- 应用服务器
- 客户端

## ❖ 其他概念

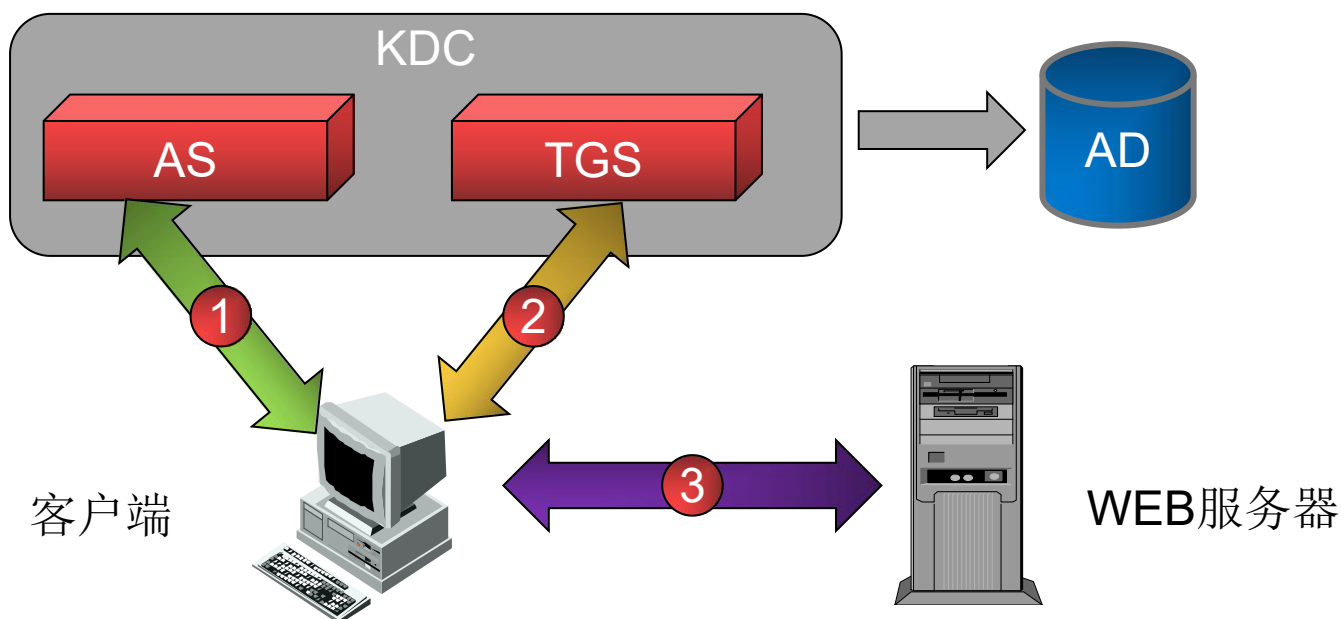
- 票据许可票据（TGT）
- 服务许可票据（SGT）



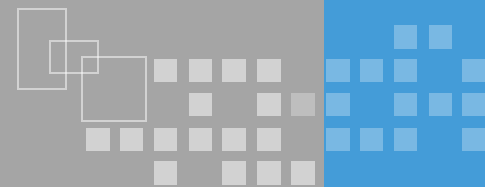
# Kerberos认证过程-三次通信

❖ 认证过程由三个阶段组成，例如需要访问OA

- 第一次：获得票据许可票据（TGT）
- 第二次：获得服务许可票据（SGT）
- 第三次：获得服务



# Kerberos工作过程-获得TGT

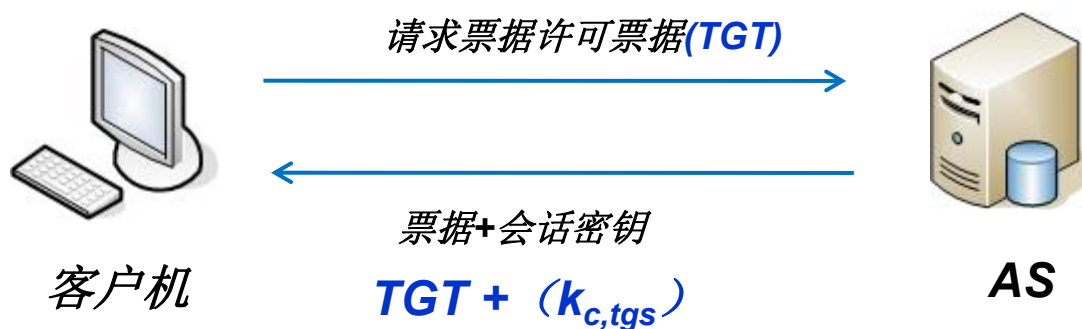


## ❖ 客户机向AS发送访问TGS请求（明文）

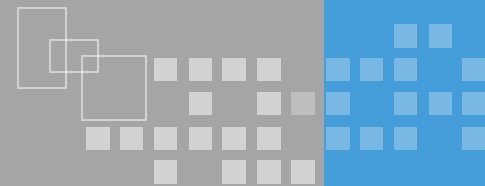
- 请求信息：用户名、IP地址、时间戳、随机数等
- AS验证用户（只验证是否存在）

## ❖ AS给予应答

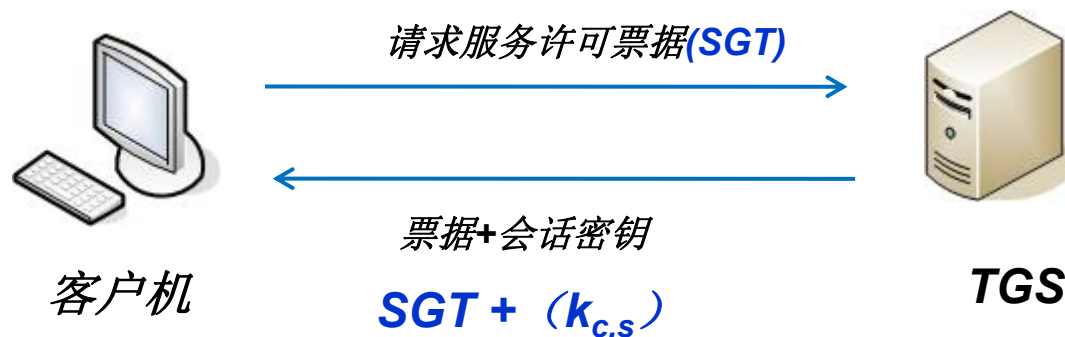
- TGT（包含TGS会话密钥），使用KDC密码加密
- 其他信息（包含TGS会话密钥），使用用户密码加密



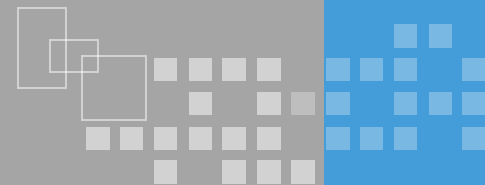
# Kerberos工作过程-获得SGT



- ❖ 客户机向TGS发送访问应用服务请求
  - 请求信息使用TGS会话密钥加密（包含认证信息）
  - 包含访问应用服务名称（http）
- ❖ TGS验证认证信息（包含用户名等）后，给予应答
  - SGT
  - 客户机与应用服务器之间的会话密钥



# Kerberos工作过程-获得服务

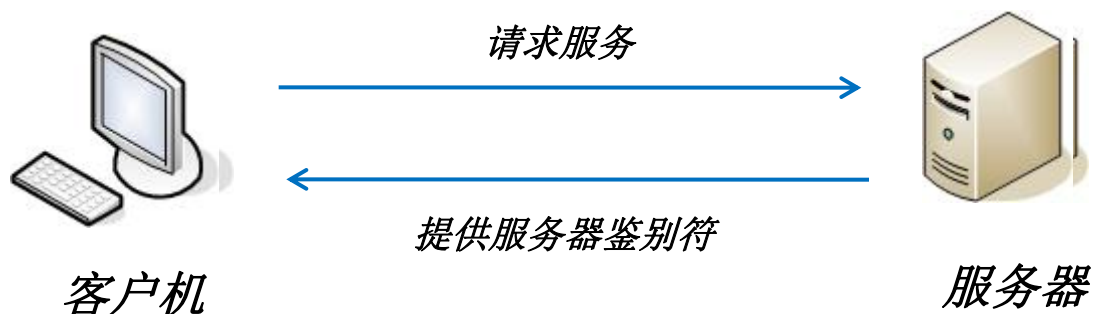


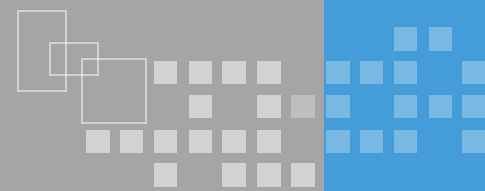
## ❖ 客户机向应用服务器请求服务

- SGT（使用http服务器密码加密）
- 认证信息

## ❖ 应用服务器（验证认证信息）

- 提供服务器验证信息（如果需要验证服务器）





## ❖ RADIUS协议

- 最初为拨号用户进行认证和计费，现为通用的认证协议
- 协议实现简单，传输简捷高效
- 仅对传输过程中的密码本身进行加密

## ❖ TACACS+协议（终端访问控制器访问控制系统）

- 运行于TCP协议，具有较高的可靠性
- 对包头外所有数据加密，安全性较高
- 大型网络中实时性较差

❖ 实体身份鉴别的方法多种多样，且随着技术的进步，鉴别方法的强度不断提高，常见的方法有利用口令鉴别、令牌鉴别、指纹鉴别等。如图，小王在登陆某移动支付平台时，首先需要通过指纹对用户身份进行鉴别。通过鉴别后，他才能作为合法用户使用自己的账户进行支付、转账等操作。这种鉴别方法属于下列选项中的（ ）

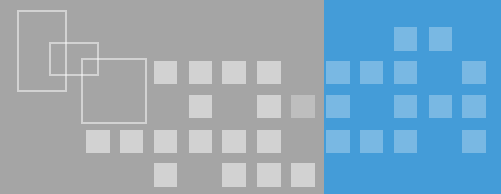
- ❖ A. 实体所知的鉴别方法
- ❖ B. 实体所有的鉴别方法
- ❖ C. 实体特征的鉴别方法
- ❖ D. 实体所见的鉴别方法



- ❖ Kerberos 协议是常用的集中访问控制协议，通过可信第三方的认证服务，减轻应用服务器和负担。Kerberos 的运行环境由密钥分发中心（KDC）、应用服务器和客户端三个部分组成。其中，KDC 分为认证服务器 AS 和票据授权服务器 TGS 两部分。下图展示了 Kerberos 协议的三个阶段，分别为（1）Kerberos 获得服务许可票据，（2）Kerberos 获得服务，（3）Kerberos 获得票据许可票据。下列选项中对这三个阶段的排序正确的是（）

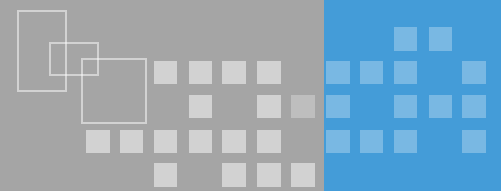
- ❖ A. (1) → (2) → (3)
- ❖ B. (3) → (2) → (1)
- ❖ C. (2) → (1) → (3)
- ❖ D. (3) → (1) → (2)





- ❖ 下列哪一种方法属于基于实体“所有”鉴别方法：
- ❖ A. 用户通过自己设置的口令登录系统，完成身份鉴别
- ❖ B. 用户使用个人指坟，通过指纹识别系统的身份鉴别
- ❖ C. 用户利用和系统协商的秘密函数. 对系统发送的挑战进行正确应答，通过身份鉴别
- ❖ D. 用户使用集成电路卡（如智能卡）完成身份鉴别



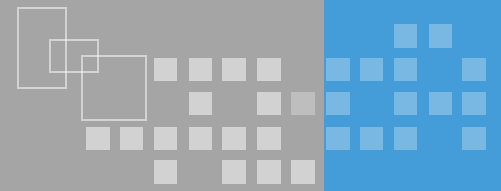


## ❖ 访问控制模型的基本概念

- 理解访问控制的概念、作用及访问控制模型的概念。

## ❖ 自主访问控制模型

- 理解自主访问控制模型相关概念及模型特点；
- 理解访问控制列表与访问能力表等自主访问控制模型的基本概念。



## ❖ 什么是访问控制

- 为用户对系统资源提供**最大限度共享**的基础上，对用户的**访问权限**进行管理，防止对信息的**非授权**篡改和滥用

## ❖ 访问控制作用

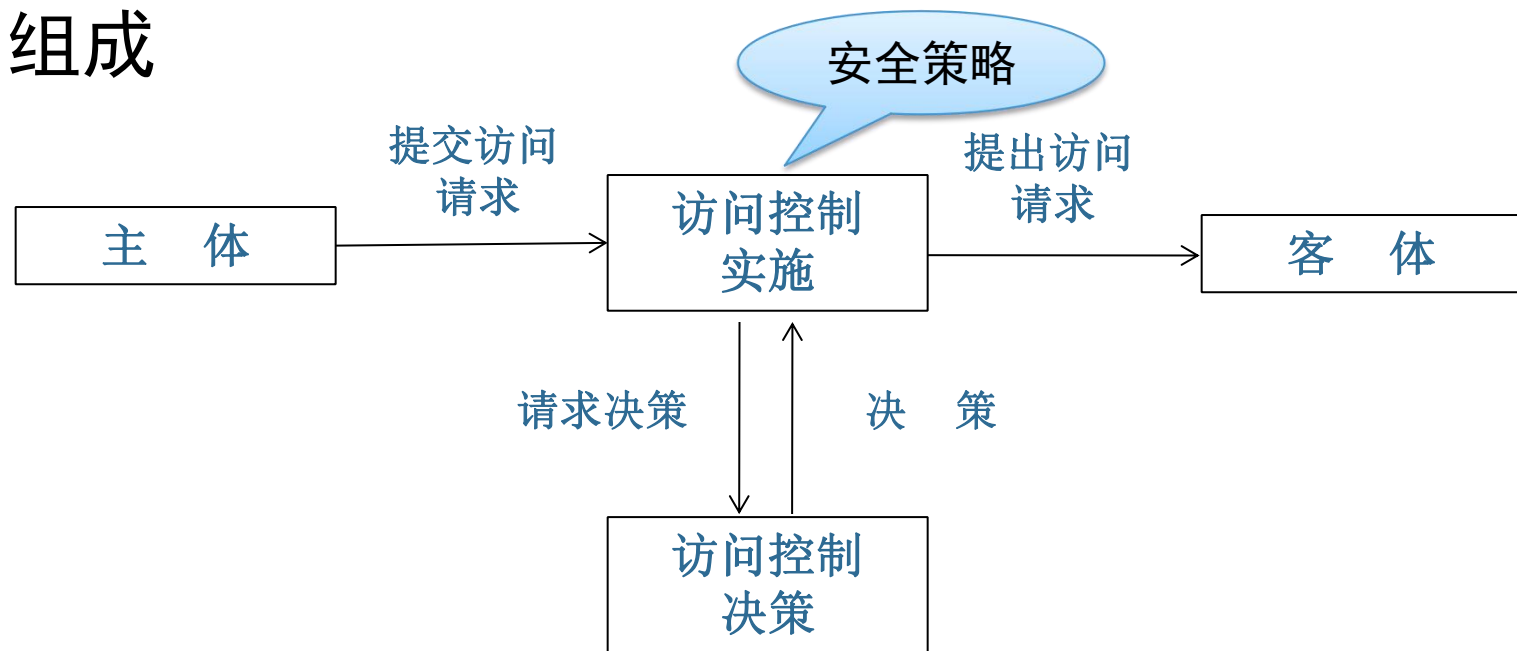
- 保证用户在**系统安全策略**下正常工作
- 拒绝非法用户的**非授权**访问请求
- 拒绝合法用户**越权**的服务请求

# 访问控制基本概念-访问控制模型

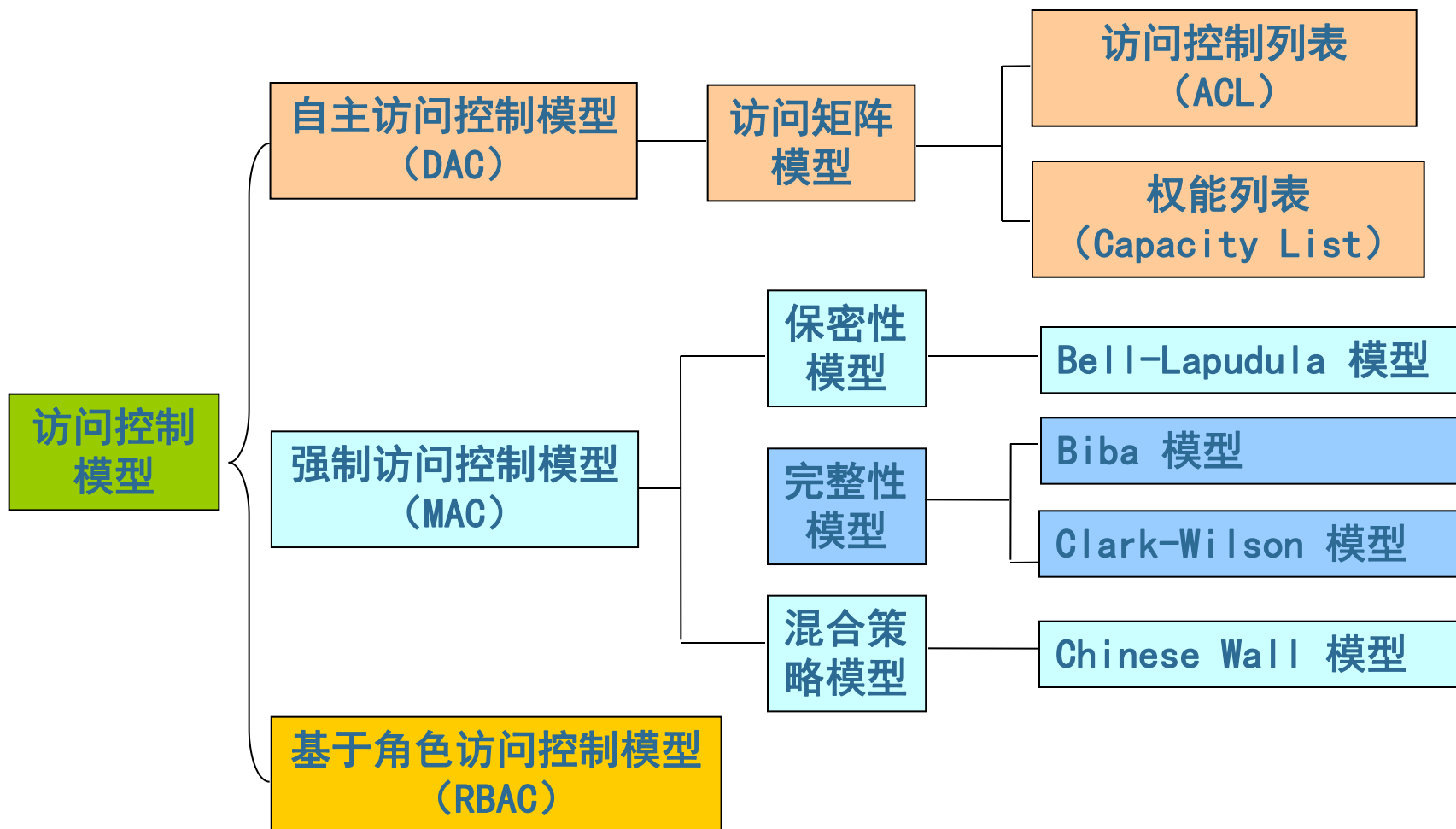
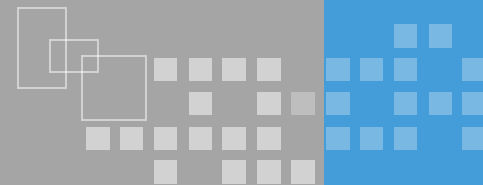
## ❖ 什么是访问控制模型

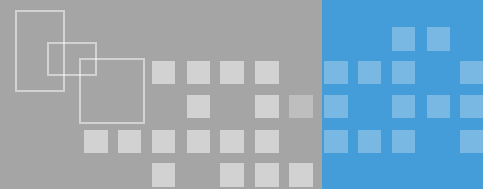
- 对一系列访问控制规则集合的描述，可以是非形式化的，也可以是形式化的。

## ❖ 组成



# 访问控制模型的分类





## ❖ 什么是自主访问控制模型（DAC）

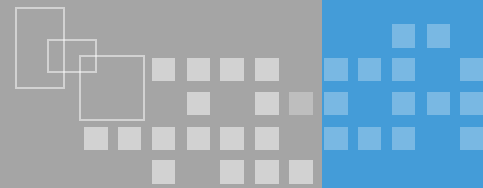
- 客体的属主（创建者）决定该客体的访问权限
- **灵活**，具有较好的易用性和可扩展性
- 主体权限容易被改变，安全性不高

## ❖ 实现机制

- 访问控制表/矩阵

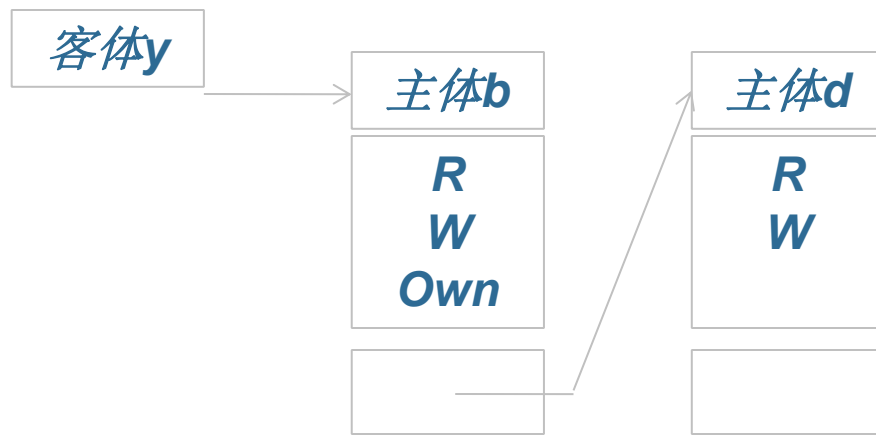
| <div>目标<br/>用户</div> | 目标x     | 目标y     | 目标z     |
|----------------------|---------|---------|---------|
| 用户a                  | R、W、Own |         | R、W、Own |
| 用户b                  |         | R、W、Own |         |
| 用户c                  | R       | R、W     |         |
| 用户d                  | R       | R、W     |         |

# 自主访问控制模型实现方式



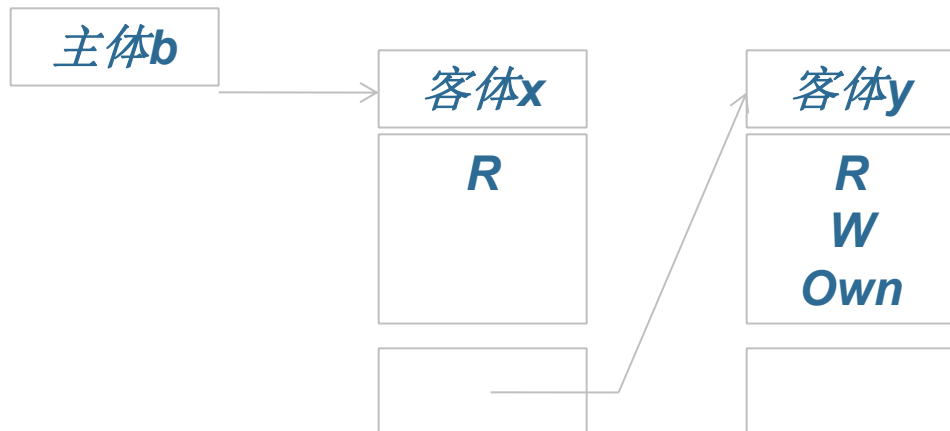
## ❖ 访问控制表

- 权限与客体关联
- 在客体上附加一个主体明细表的方法来表示访问控制矩阵的

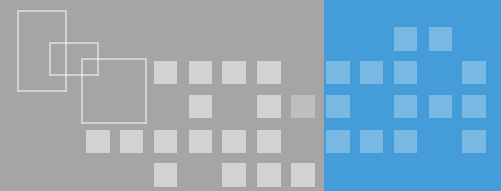


## ❖ 访问能力表

- 权限与主体关联
- 为每个用户维护一个表，表示主体可以访问的客体及权限



# 自主访问控制的特点



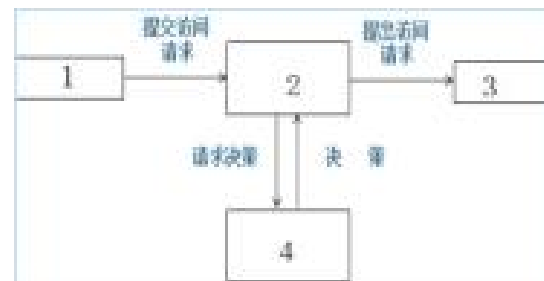
## ❖ 优点：

- 根据主体的身份和访问权限进行决策
- 具有某种访问能力的主体能够自主地将访问权的某个子集授予其它主体
- 灵活性高，被大量采用

## ❖ 缺点：

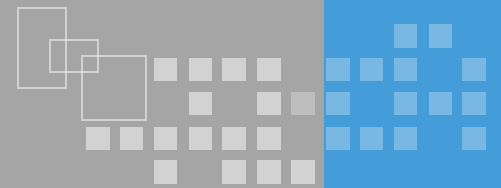
- 安全性不高
- 信息在传递过程中其访问权限关系会被改变

❖ 下图排序你认为那个是正确的：



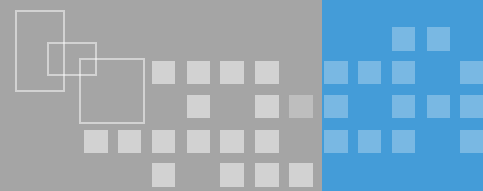
- ❖ A. 1是主体，2是客体，3是实施，4是决策
- ❖ B. 1是客体，2是主体，3是决策，4是实施
- ❖ C. 1实施，2是客体，3是主体，4是决策
- ❖ D. 1是主体，2是实施，3是客体，4是决策





## ❖ 强制访问控制模型

- 理解强制访问控制模型的概念及特点；
- 了解Bell-LaPadula模型的作用及特点；
- 了解Biba模型的作用及特点；
- 了解Clark-Wilson的作用及特点；
- 了解Chinese Wall模型的作用及特点。

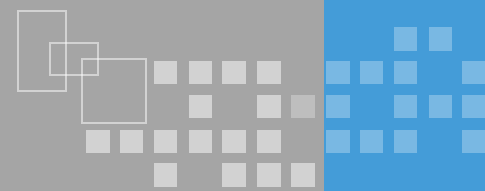


## ❖ 什么是强制访问控制(MAC)

- 主体和客体都有一个**固定**的安全属性，系统用该安全属性来决定一个主体是否可以访问某个客体

## ❖ 特点

- 安全属性是强制的，任何主体、客体都**无法变更**
- 安全性较高，应用于军事等安全要求较高的系统



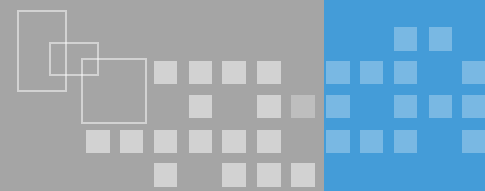
## ❖ BLP模型概念

- 由D. Elliott Bell和Leonard J. LaPadula于1973年提出的一种模拟军事安全策略的计算机访问控制模型，简称为BLP模型
- 第一个严格形式化的安全模型
- 多级访问控制模型，用于保证系统信息的机密性

## ❖ BLP模型访问控制策略

- 包括自主安全策略与强制安全策略
- 强制安全策略为每一个主体和客体都分配了安全级，根据安全级进行访问控制

# BLP模型的构成



## ❖ 安全级

- 密级：绝密、机密、秘密、公开
- 范畴：军事，外交，商务.....

## ❖ 安全级之间支配关系（密级高于或等于、范畴包含）

- 例如 $L = \langle \text{机密}, \{\text{外交}, \text{商务}\} \rangle$ ,  $L' = \langle \text{秘密}, \{\text{商务}\} \rangle$ , 则 $L$ 支配 $L'$

当主体的安全级可以支配客体的安全级，且主体对客体有自主型读权限，主体可以读客体

## ❖ 安全策略

- 简单安全规则（**向下读**）
- \*-规则（**向上写**）

当客体的安全级可以支配主体的安全级，且主体对客体有自主型读权限，主体可以读客体

❖ 根据Bell-LaPadula模型安全策略，下图中写和读操作正确的是（）

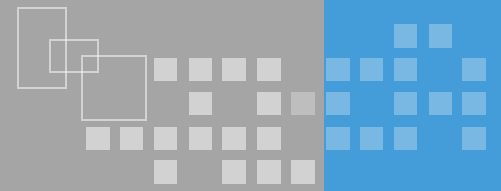


- ❖ A. 可读可写
- ❖ B. 可读不可写
- ❖ C. 可写不可读
- ❖ D. 不可读不可写

❖ 根据 Bell-LaPiedula 模型安全策略，下图中写和读操作正确的是（ ）



- ❖ A. 可读可写
- ❖ B. 可读不可写
- ❖ C. 可写不可读
- ❖ D. 不可读不可写

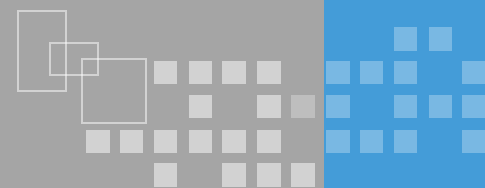


## ❖ Biba模型概念

- 1977年由Biba提出，与BLP模型数学上对偶的完整性保护模型
- 多级访问控制模型，保护数据完整性

## ❖ Biba模型的访问控制策略

- 强制安全策略为每一个主体和客体都分配了**完整级**，根据**完整级**进行访问控制



- ❖ 完整级：安全级和范畴
  - 安全级：极为重要，非常重要，重要，.....
  - 范畴：军事，外交，商务.....
- ❖ 完整级存在支配关系
  - 与BLP类似，安全级高于或等于，范畴包含
- ❖ 安全策略
  - 向上读：主体可以读客体，当且仅当客体的完整级别支配主体的完整级
  - 向下写：主体可以写客体，当且仅当主体的完整级别支配客体的完整级



## ❖ Clark-Wilson模型概念

- 由计算机科学家David D. Clark和会计师David R. Wilson发表于1987年
- 确保**商业数据完整性**的访问控制模型，侧重于满足商业应用的安全需求

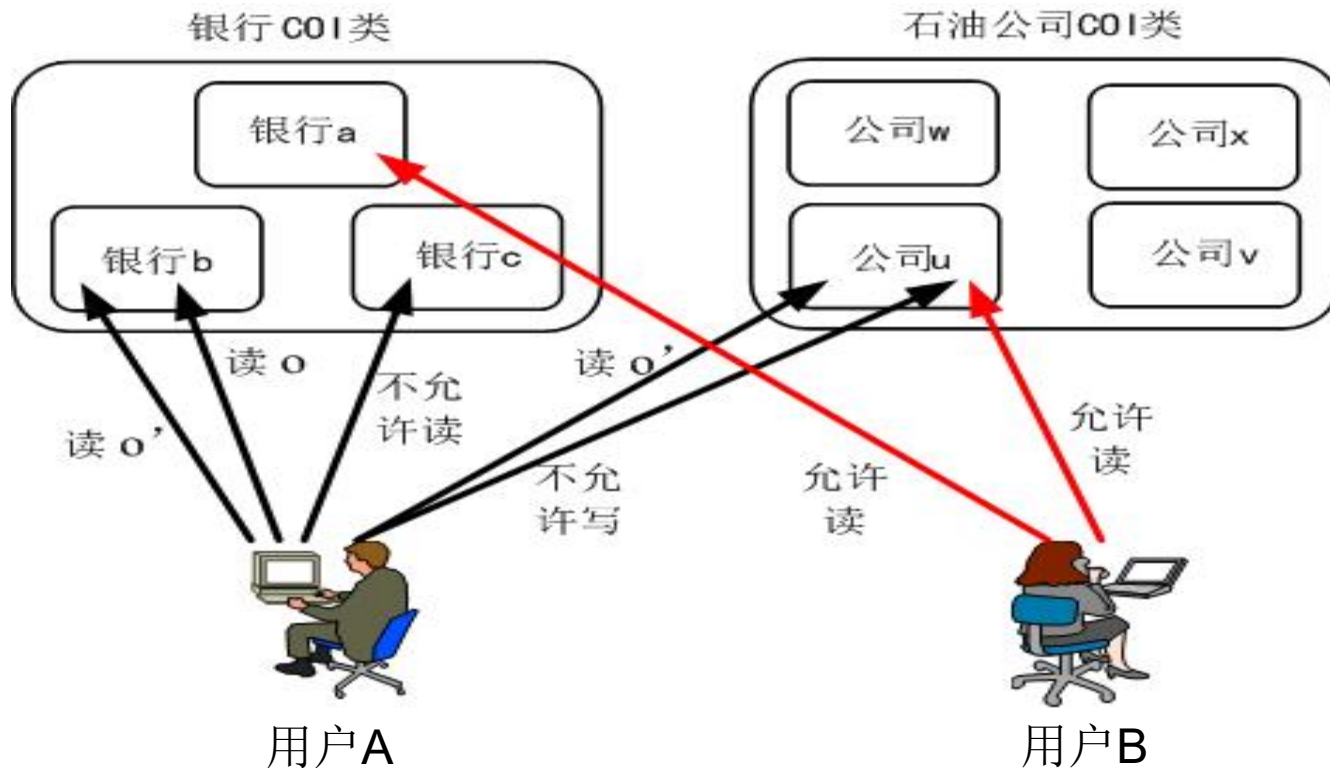
## ❖ Clark-Wilson模型的访问控制策略

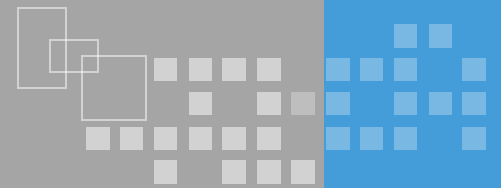
- 每次操作前和操作后，数据都必须满足这个**一致性**条件



# Chinese Wall模型示例

- ❖ 若干有竞争关系数据集构成了利益冲突类
  - 银行COI类（银行a、银行b、银行c）
  - 石油公司COI类（公司w、公司x、公司u、公司v）





## ❖ 基于角色的访问控制模型

- 了解基于角色的访问控制模型基本概念及特点；
- 了解RBAC模型的构成及访问控制规则。

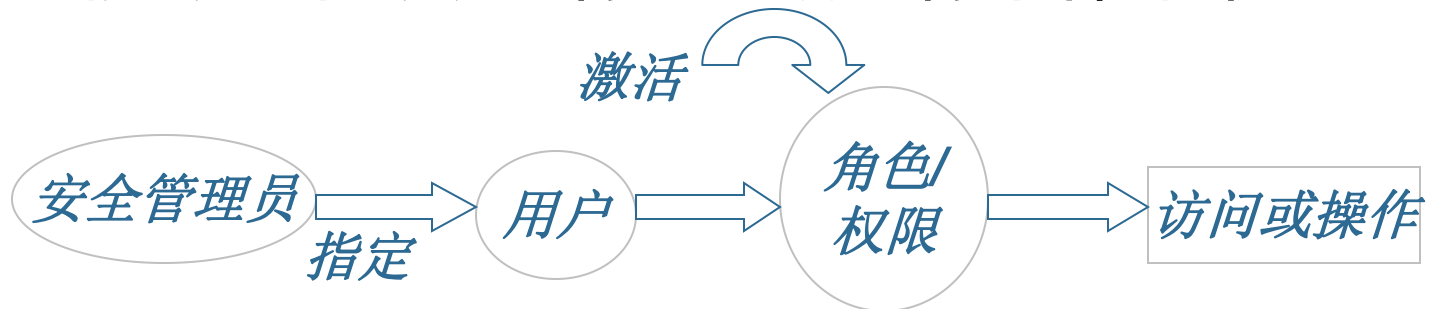
## ❖ 特权管理基础设施

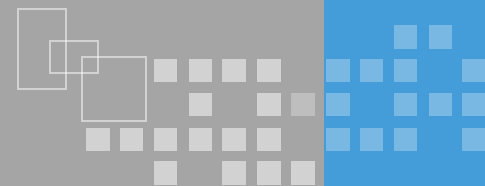
- 理解PMI的主要功能、体系架构及应用。

# 基于角色的访问控制



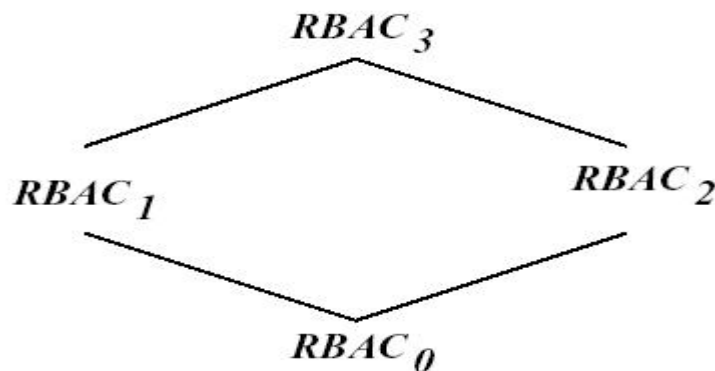
- ❖ 基于角色的访问控制（RBAC）模型
  - 系统内置多个角色，将权限与角色进行关联
  - 用户必须成为某个角色才能获得权限
- ❖ 基于角色访问控制模型访问控制策略
  - 根据用户所担任的角色来决定用户在系统中的访问权限
  - 用户必须成为某个角色，且还必须激活这一角色，才能对一个对象进行访问或执行某种操作





## ❖ RBAC模型四种类型

- RBAC0，基本模型，规定了所有RBAC的基本内容，四种要素，用户(U)、角色(R)、会话(S)和权限(P)
- RBAC1：包含RBAC0，加入安全等级及角色继承关系
- RBAC2：包含RBAC0，加入约束条件，例如财务和会计不能为同一人
- RBAC3：结合了RBAC1、RBAC2





## ❖ PMI是什么

- 与**应用相关的授权服务管理**
- 建立在PKI提供的可信的身份认证服务的基础
- 采用基于属性证书的授权模式

## ❖ PMI的主要功能

- 对权限管理进行了系统的定义和描述
- 系统地建立起对用户身份到应用授权的映射
- 支持访问控制等应用

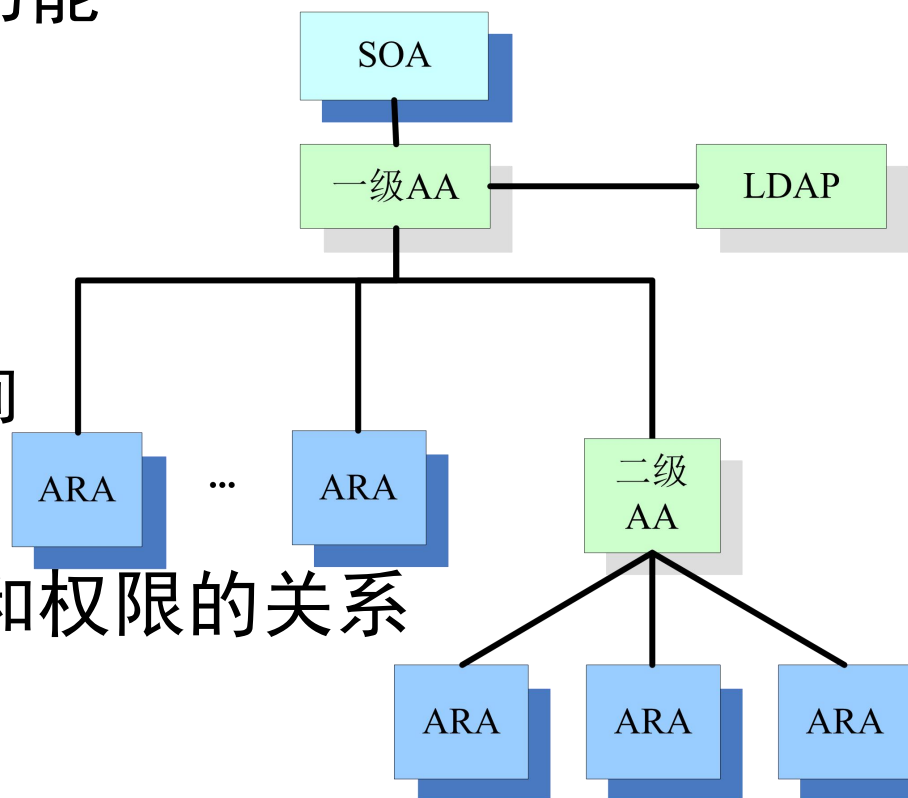
# PMI的体系架构

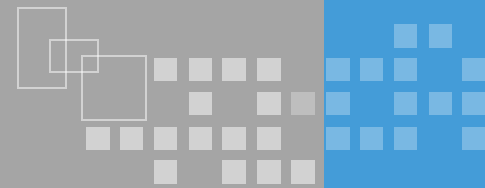
❖ PMI是属性证书、属性权威、属性证书库等部件的集合体，用来实现权限和属性证书的产生、管理、存储、分发和撤销等功能

- SOA:信任源点
- AA:签发属性证书
- ARA:证书签发请求
- LDAP:属性证书发布查询

❖ 属性证书

- 以证书形式给出用户和权限的关系





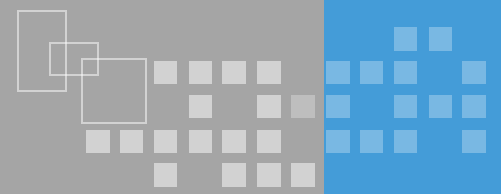
## ❖ PKI

- “你是谁”
- 身份与公钥绑定
- 身份鉴别（护照）
- RCA-CA-RA, LDAP, CRL

## ❖ PMI

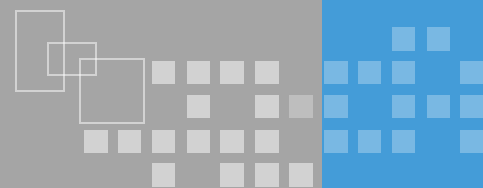
- “你能做什么”
- 身份（角色）与角色（属性、权限）绑定
- 授权管理（签证）
- SOA-AA-ARA, LDAP, ACRL





❖ 访问控制方法可分为自主访问控制、强制访问控制和基于角色的访问控制，他们具有不同的特点和应用场景。如果需要选择一个访问控方法，要求能够支持最小特权原则和职责分离原则，而且在不同的系统配置下可以具有不同的安全控制，那么在下列选项中，能够满足以上要求的选项是（ ）

- ❖ A. 自主访问控制
- ❖ B. 强制访问控制
- ❖ C. 基于角色的访问控制
- ❖ D. 以上选项都可以



## ❖ 密码学

- 密码学基本概念及对信息安全的作用、对称密码算法与非对称密码算法、哈希、消息鉴别、数字签名及PKI

## ❖ 身份鉴别

- 鉴别的三种方式：所知、所有、特征
- Kerberos体系

## ❖ 访问控制模型

- DAC
- MAC (BLP、Biba、Clark-Wilson、Chinese-wall)
- RBAC



**谢谢，请提问题！**