# 系统安全分析与设计

## 信息系统安全属性

安全属性：

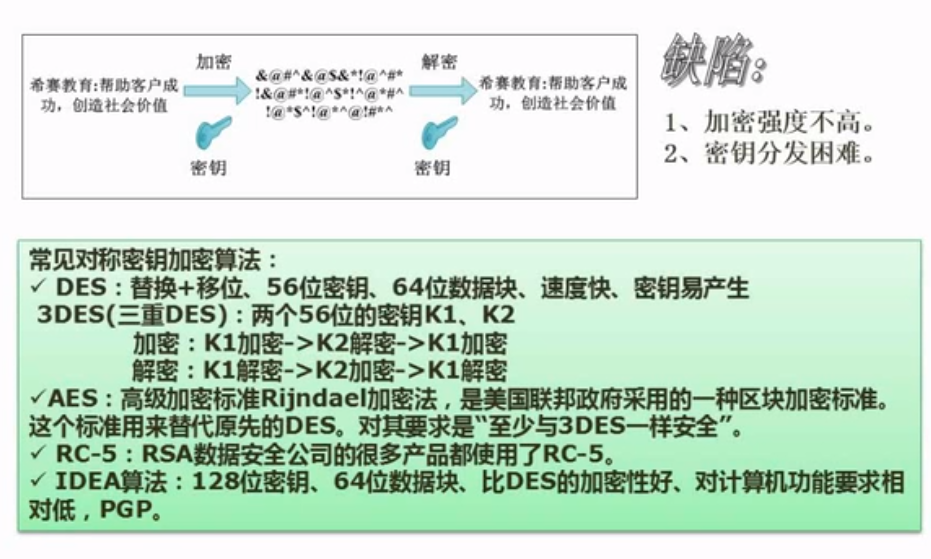
保密性：最小授权原则、防暴露、信息加密、物理保密

完整性：安全协议、校验码、密码校验、数字签名、公证

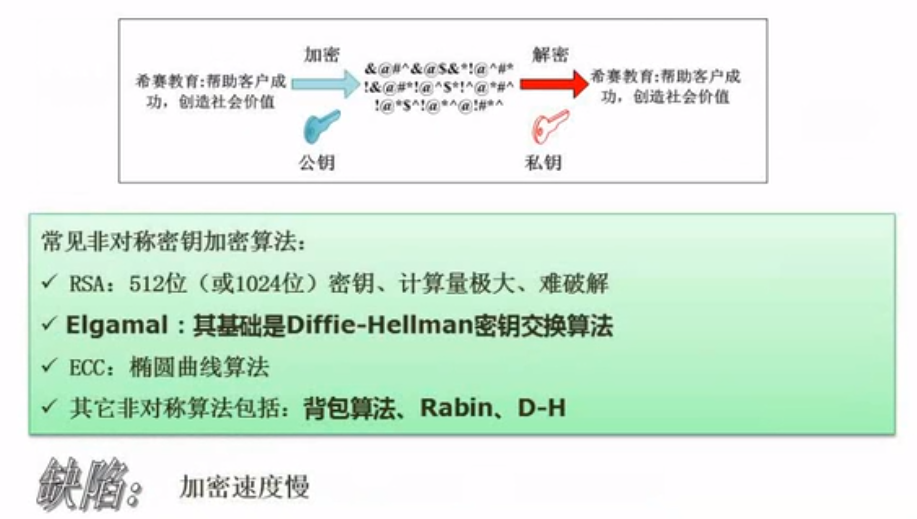
可用性：综合故障（IP过滤、业务流控制、路由选择控制、审计跟踪）

不可抵赖性：数字签名

## 对称加密技术



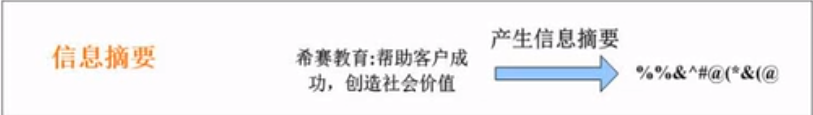
## 非对称加密技术



非对称加密算法需要两个密钥：公开密钥（pubic key）和私有密钥（private key）。公开密钥与私有密钥是一对，如果用公开密钥对数据加密，只有用对应的私钥才能解密。因为加密和解密使用的是两个不同的密钥，所以这种算法叫做非对称加密算法。非对称加密算法实现机密信息交换的基本过程是：甲方生成一对密钥，并将其中的一把作为公开密钥向其他方公开；得到该公用密钥的乙方使用该密钥对机密信息进行加密后再发送给甲方；甲方再用自己保存的另一把专用密钥对加密后的信息进行解密。甲方想要回复乙方正好相反，使用乙方的公钥对数据进行加密，同理，乙方使用自己的私钥来进行解密。

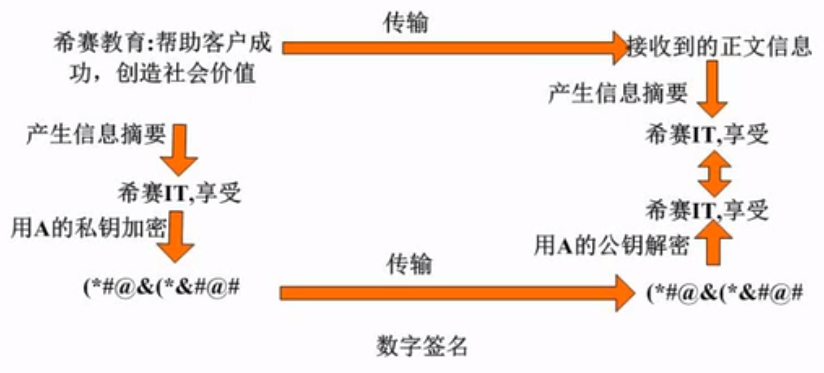
## 信息摘要

单向散列函数（单向hash函数）、固定长度的散列值。



常用的信息摘要算法有MD5，SHA等，市场上广泛使用的MD5，SHA算法的散列值分别为128位和160位，由于SHA通常采用的密钥长度较长，因此安全新高于MD5。

## 数字签名



## 数字信封与PGP

发送方将原文用对称密钥加密传输，而将对称密钥用接收方公钥加密 发送给对方。

接受方收到电子信封用自己的私钥解密信封，取出对称密钥解密得原文。

PGP可用于电子邮件，也可用于文件传输。采用杂合算法，包括IDEA、RSA、MD5、ZIP数据压缩算法。

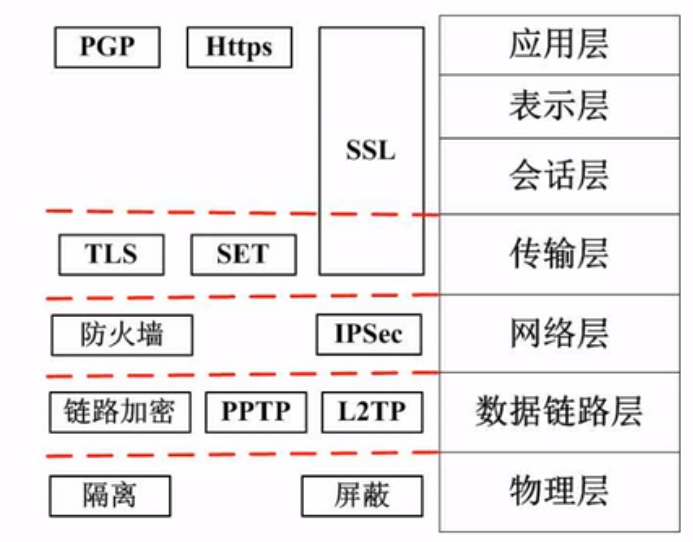
PGP承认两种不同得证书格式：PGP证书和X.509证书。

PGP证书包含PGP版本号、证书持有者得公钥、证书持有者得信息、证书拥有者的数字签名、证书的有效期、密钥首选的对称加密算法。

X.509证书包含证书版本、证书的序列号、签名算法标识、证书有效期、以下数据：证书发行商名字、证书主体名、主体公钥信息、发布者的数字签名。

## 网络安全

### 各个网络层次的安全保障



### 网络威胁与攻击

|  |  |
| --- | --- |
| 威胁名称 | 描述 |
| 重放攻击（ARP） | 所截获的某次合法的通信数据拷贝，出于非法的目的而被重新发送 |
| 拒绝服务（DOS） | 对信息或其他资源的合法访问被无条件的阻止 |
| 窃听 | 用各种可能的合法或非法的手段窃取系统中的信息资源和敏感信息。例如对通信线路中传输的信号进行搭线监听，或者利用通信设备在工作过程中产生的电磁泄漏截取有用的信息等 |
| 业务流分析 | 通过对系统进行长期监听，利用统计分析方法对诸如通信频度、通信的信息流向、通信 总量的变化等参数进行研究，从而发现有价值的信息和规律 |
| 信息泄露 | 信息被泄露或透漏给某个非授权的实体 |
| 破坏信息的完整性 | 数据被非授权的进行增删、修改或破坏而受到损失 |
| 非授权访问 | 某一资源被某非授权的人、或以授权的方式使用 |
| 假冒 | 通过欺骗通信系统（或用户）达到非法用户冒充称为合法用户，或者特权小的用户冒充称为特权大的用户的目的。黑客大多是采用假冒攻击。 |
| 旁路控制 | 攻击者利用系统的安全缺陷或安全性上的脆弱之处获得非授权的权力或特权。例如，攻击者 通过各种攻击手段发现原本应保密，但是却又暴露出来的一些系统“特性”。利用这些“特性”，攻击者可以绕过防线守卫者侵入系统的内部。 |
| 授权侵犯 | 被授权以某一目的使用某一系统或资源的某个人，却将此权限用于其他非授权目的，也称作“内部攻击” |
| 特洛伊木马 | 软件中含有一个察觉不出的或者无害的程序段，当他被执行时，会破坏用户的安全。 |
| 陷阱门 | 在某个系统或某个部件中设置“机关”，使得当提供特定的输入数据时允许违反安全策略 |
| 抵赖 | 这是一种来自用户的攻击，比如：否认自己曾经发布过的某条信息、伪造一份对方来信等。 |

### 防火墙

