



# 信息安全概论

概述

刘亚维

# 主要教材及参考书

- 翟健宏. 信息安全导论. 北京:科学出版社. 2011.7
- Michael Goodrich , Roberto Tamassia,  
Introduction to Computer Security,  
Addison Wesley; 2010.10
- William Stallings. 密码编码学与网络安全—  
原理与实践. 北京: 电子工业出版  
社.2006.11

# 考核方法



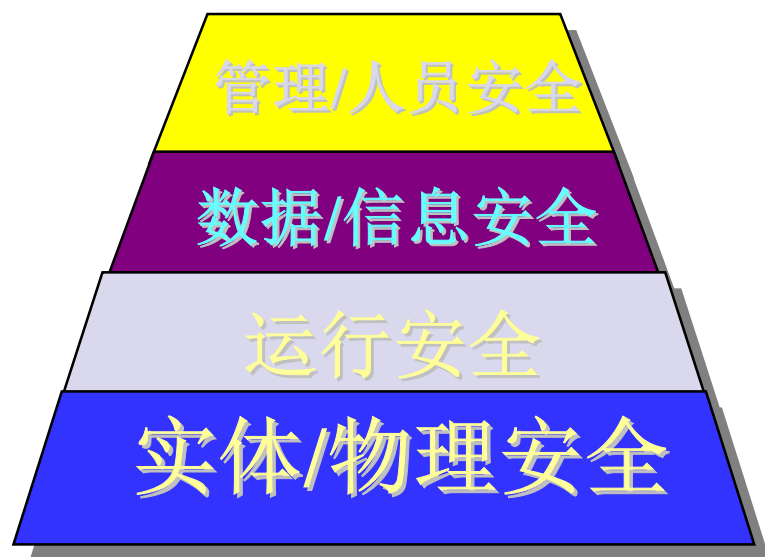
- 平时 10%
- 课后作业 20%
- 实验 10%
- 附加分 5分
- 期末考试 60%

# 主要内容

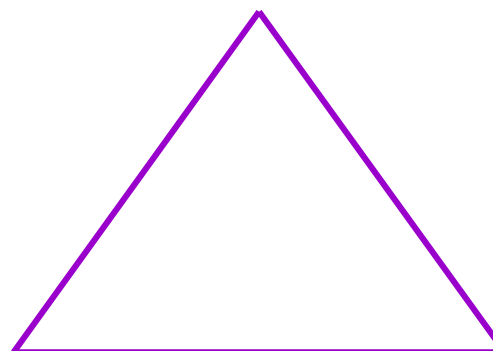


- 信息安全及其关键技术
- 信息安全的理解（1.1）
- 信息安全威胁（1.2）
- 互联网的安全性（1.3）
- 信息安全体系结构（1.4）

# 关于信息安全的两个主要视点



信息安全分层结构  
面向应用的信息安全框架



信息安全金三角（CIA）  
面向属性的信息安全框架

# 两个被忽略的问题之一：内容安全

- 内容安全的本质是什么？

- 内容安全着眼点是依据内容来对安全问题进行判断，但需要通过技术方式来解决。

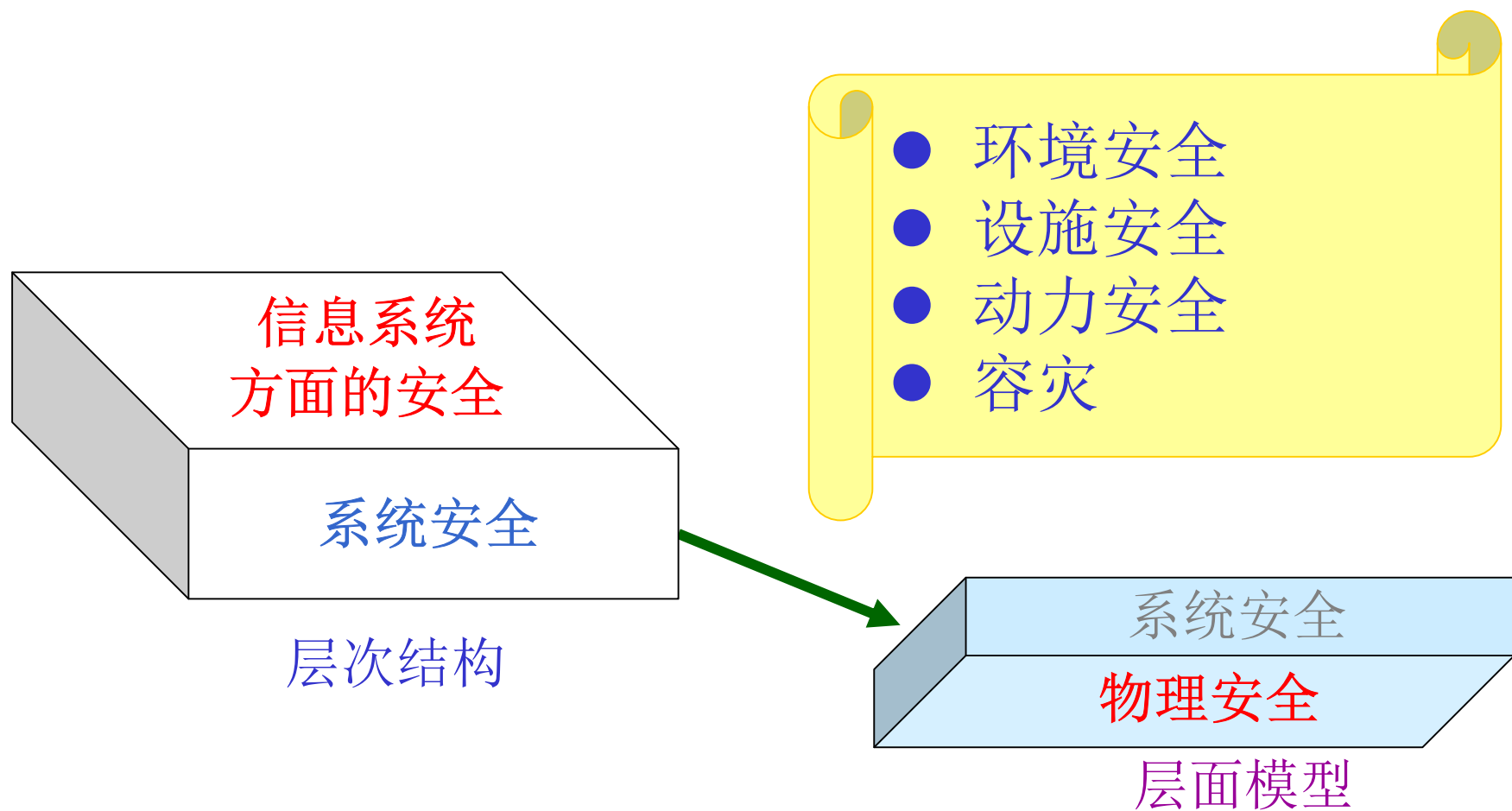
- 内容安全技术的本质是对数据的攻击技术

- 国际社会经常将反网络病毒（**Anti Vandalism**）、反垃圾邮件问题列入内容安全的范畴

## 两个被忽略的问题之二：信息内容对抗

- 一支从事信息安全的队伍研究的是信息对抗的问题，所引发的问题是：
  - 信息对抗与信息安全的关系是什么？
    - 信息对抗自身也存在体系问题，包括不同层次的对抗问题，我们仅选择信息内容对抗来讨论
  - 信息隐藏是典型的信息内容对抗的研究内容
- 站在信息安全的角度考虑这个问题，给出的命题是：
  - 一个客观存在的信息，如何发现？
    - 数据挖掘、情报分析、信息获取
  - 如果我们不能掩盖一个信息，那就淹没这个信息
  - 围绕信息利用的对抗行为(所谓虚虚实实真真假假)

# 信息安全的技术层次视点

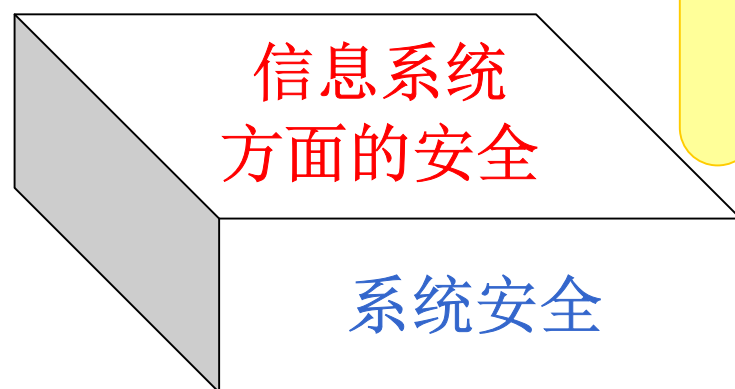




# 关于物理安全

- 指对网络与信息系统物理装备的保护。主要涉及网络与信息系统的机密性、可用性、完整性等属性。
- 所涉及的主要技术：
  - 加扰处理、电磁屏蔽：防范电磁泄露
  - 容错、容灾、冗余备份、生存性技术：防范随机性故障
  - 信息验证：防范信号插入

# 信息安全的技术层次视点



层次结构

- 系统评估-测试评估能力
- 安全策略-信息对抗能力
- 访问控制-安全防护能力
- 入侵检测-安全预警能力
- 应急响应-应急响应能力

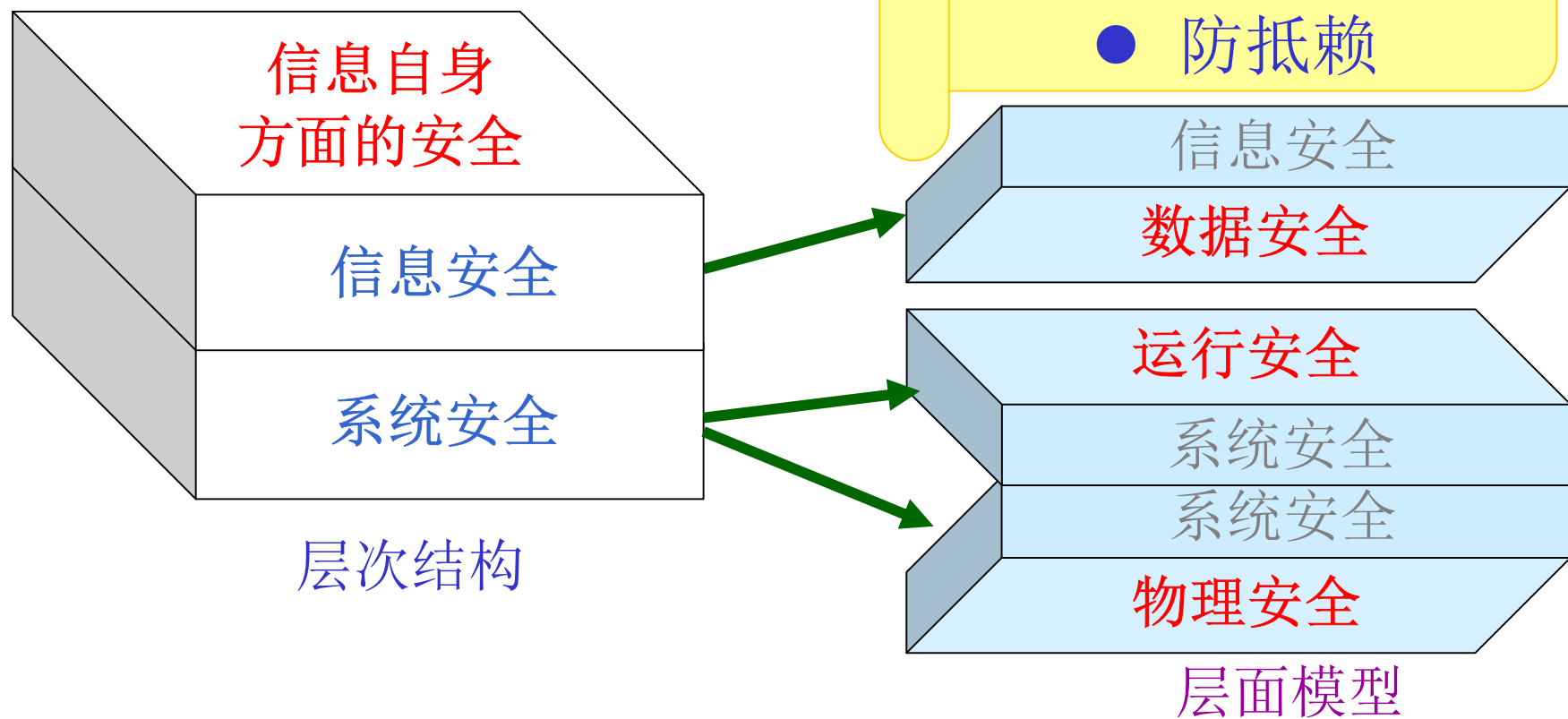


层面模型

# 关于运行安全

- 指对网络与信息系统的运行过程和运行状态的保护。主要涉及网络与信息系统的真实性、可控性、可用性等
- 主要涉及的技术
  - 风险评估体系、安全测评体系：支持系统评估
  - 漏洞扫描、安全协议：支持对安全策略的评估与保障
  - 防火墙、物理隔离系统、访问控制技术、防恶意代码技术：支持访问控制
  - 入侵检测及预警系统、安全审计技术：支持入侵检测
  - 反制系统、容侵技术、审计与追踪技术、取证技术、动态隔离技术：支持应急响应
  - 网络攻击技术，Phishing、Botnet、DDoS、木马等技术

# 信息安全的技术层次视点

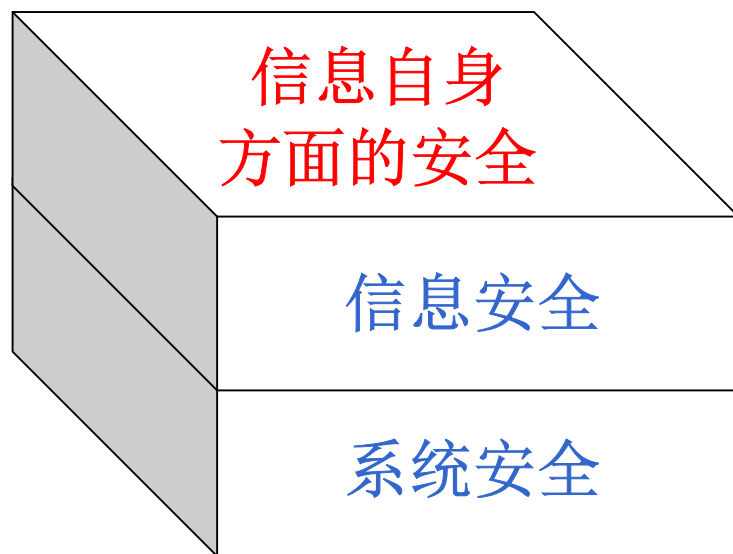


# 关于数据安全

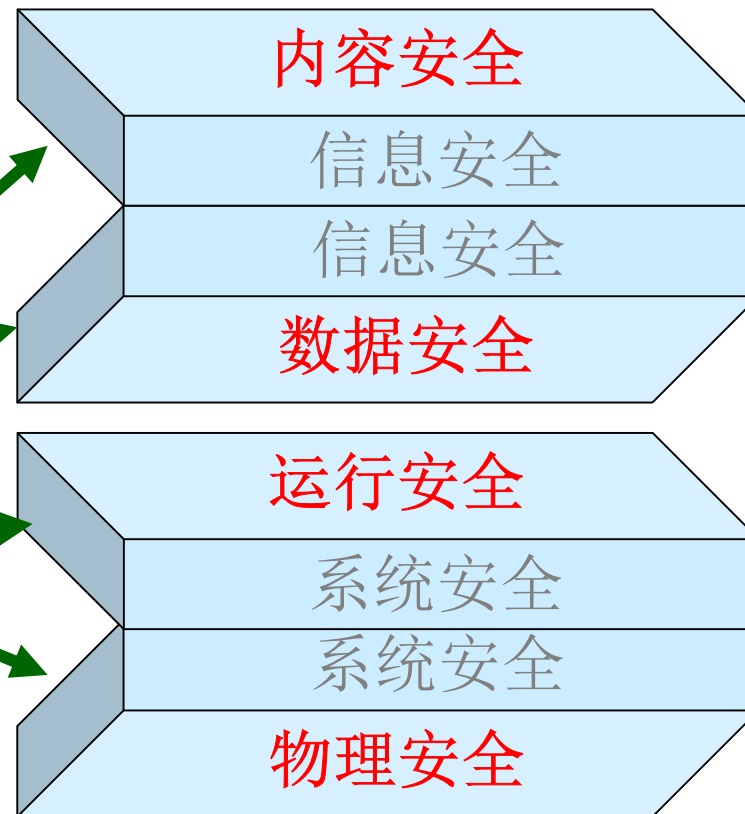
- 指对信息在数据收集、处理、存储、检索、传输、交换、显示、扩散等过程中的保护，使得在数据处理层面保障信息依据授权使用，不被非法冒充、窃取、篡改、抵赖。主要涉及信息的机密性、真实性、完整性、不可否认性等
- 主要涉及的技术
  - 对称与非对称密码技术及其硬化技术、VPN等技术：防范信息泄密
  - 认证、鉴别、PKI等技术：防范信息伪造
  - 完整性验证技术：防范信息篡改
  - 数字签名技术：防范信息抵赖
  - 秘密共享技术：防范信息破坏

# 信息安全的技术层次视点

有害信息的过滤



层次结构

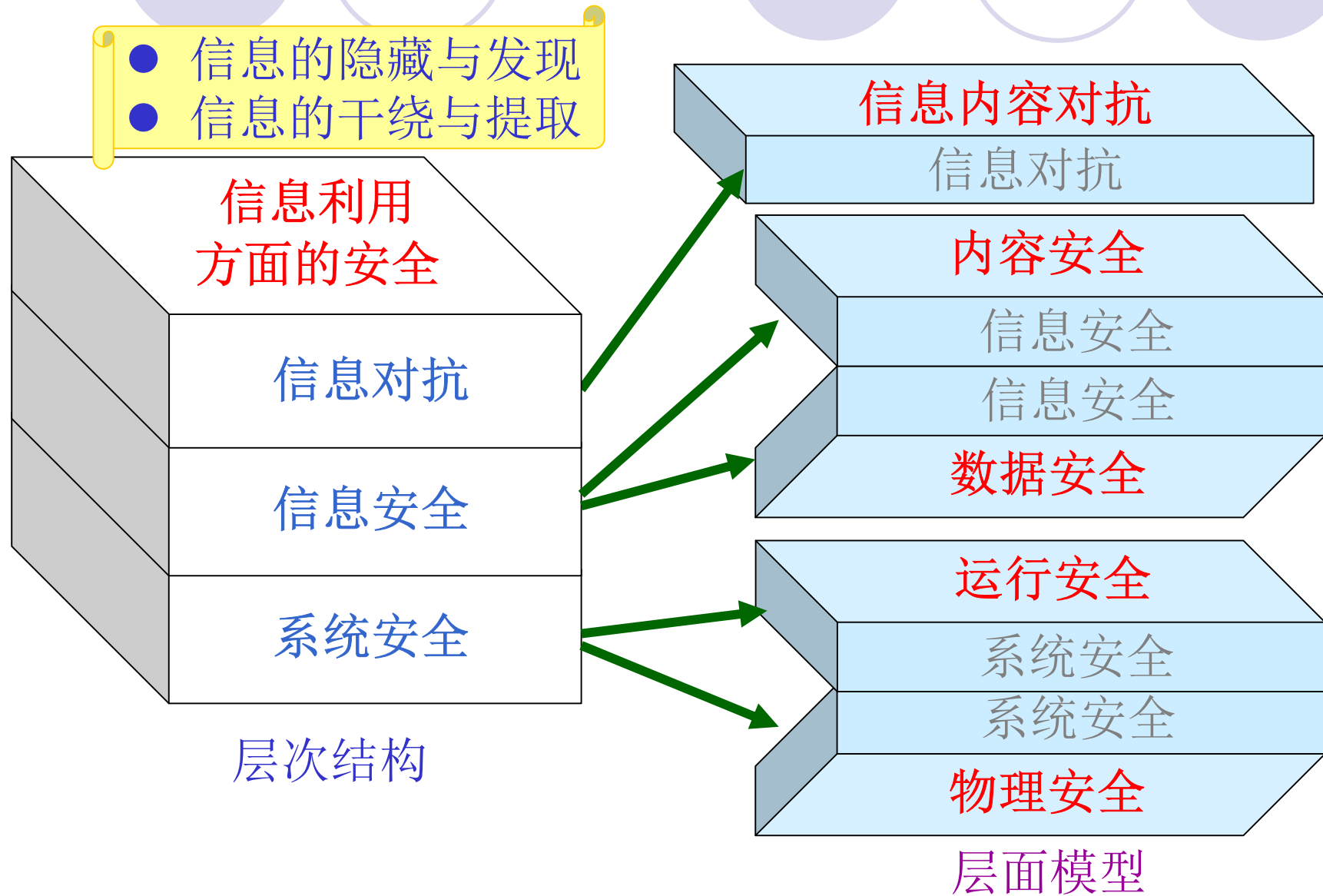


层面模型

# 关于内容安全

- 指对信息在网络内流动中的选择性阻断，以保证信息流动的可控能力。主要涉及信息的机密性、真实性、可控性、可用性等
- 主要涉及的技术：
  - 文本识别、图像识别、流媒体识别、群发邮件识别等：用于对信息的理解与分析；
  - 面向内容的过滤技术（CVP）、面向URL的过滤技术（UFP）、面向DNS的过滤技术等：用于对信息的过滤。

# 信息安全的技术层次视点

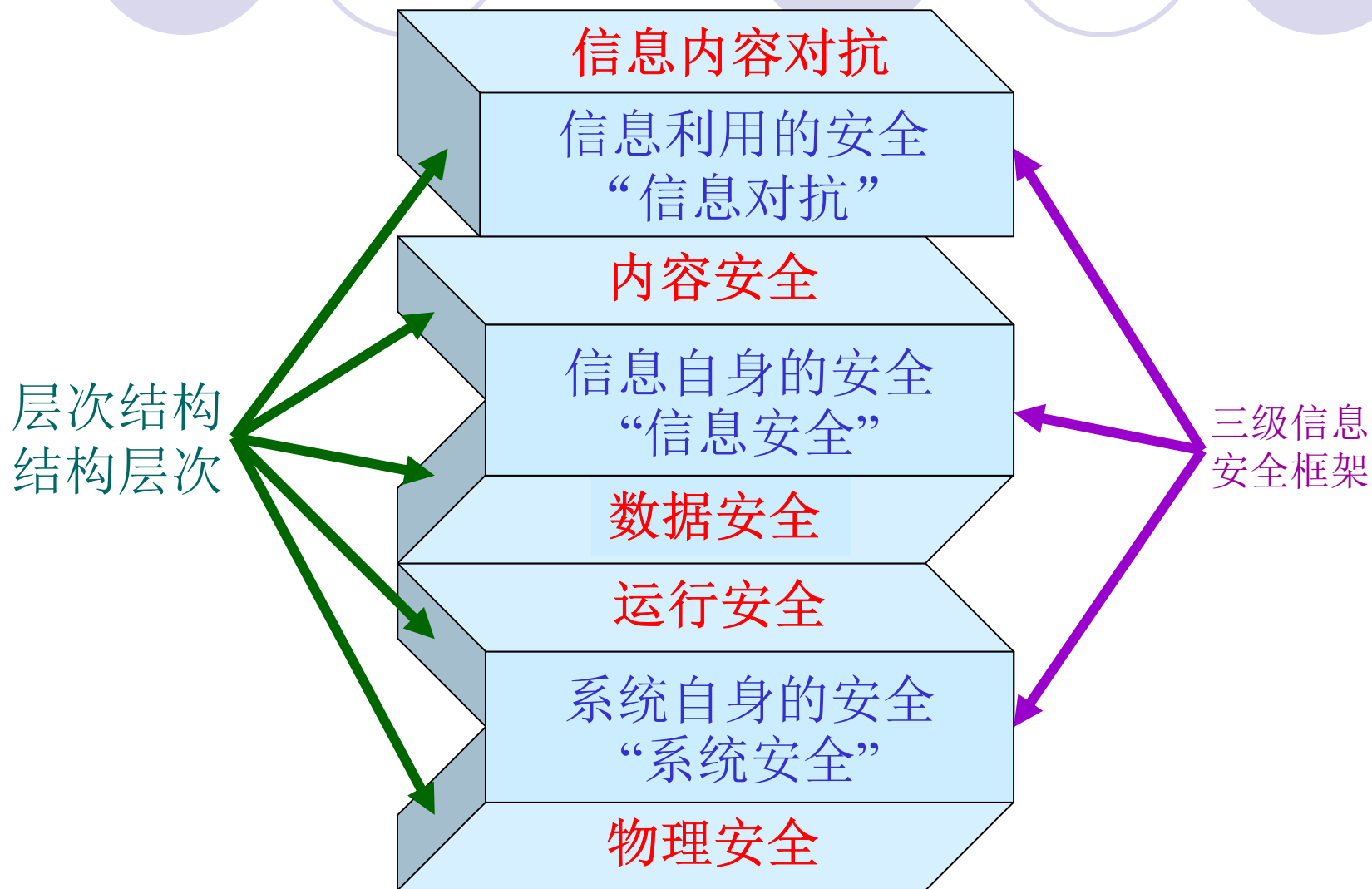




# 关于信息利用的安全

- 指对信息有效内容真实性的隐藏、保护与分析。主要涉及信息有效内容的机密性、完整性等
- 所涉及的主要技术：
  - 数据挖掘技术：发现信息
  - 隐写技术、水印技术：保护信息
  - 即时通、MSN等协议的分析技术：对特定协议的理解，
  - VoIP识别技术：对数字化语音信息的理解
  - 音频识别与按内容匹配：锁定音频目标进行

# 信息安全的技术层次视点



# ITU-X.800给出的相关属性的定义:

- 机密性 (**Confidentiality**) :
  - Prevent unauthorised disclosure of information
- 完整性 (**Integrity**) :
  - assurance that data received are exactly as sent by an authorized sender
- 可用性 (**Availability**) :
  - services should be accessible when needed and without delay
- 真实性 (**Authentication**) :
  - assurance that the communicating entity is the one it claims to be
  - peer entity authentication
  - Data-origin authentication
- 不可抵赖性 (**Non-Repudiation**) :
  - protection against denial by one of the parties in a communication
    - Origin non-repudiation: proof that the message was sent by the specified party
    - Destination non-repudiation: proof that the message was received by the specified party

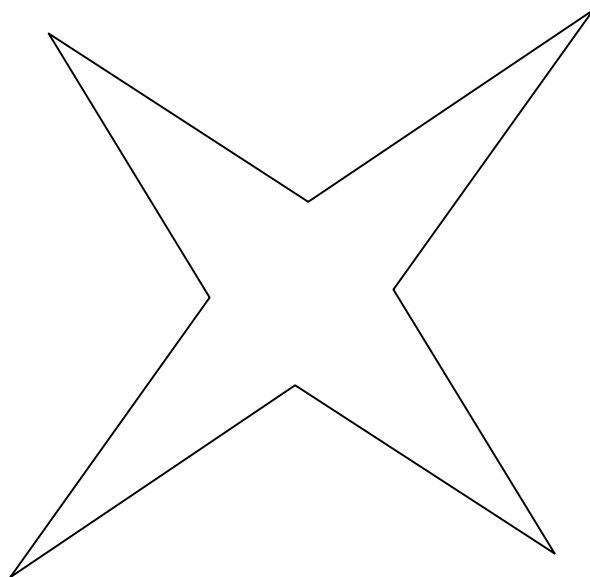
# 关于信息安全的基本属性

- 机密性（**Confidentiality**）：反映了信息与信息系统的不可被非授权者所利用
- 真实性（**Authentication**）：反映了信息与信息系统的行为不被伪造、篡改、冒充
- 可控性（**controllability**）：反映了信息的流动与信息系统可被控制者所监控
- 可用性（**Availability**）：反映了信息与信息系统可被授权者所正常使用

# 信息安全的基本属性视点

机密性 (**Cf**)

真实性 (**Au**)



可控性 (**Ct**)

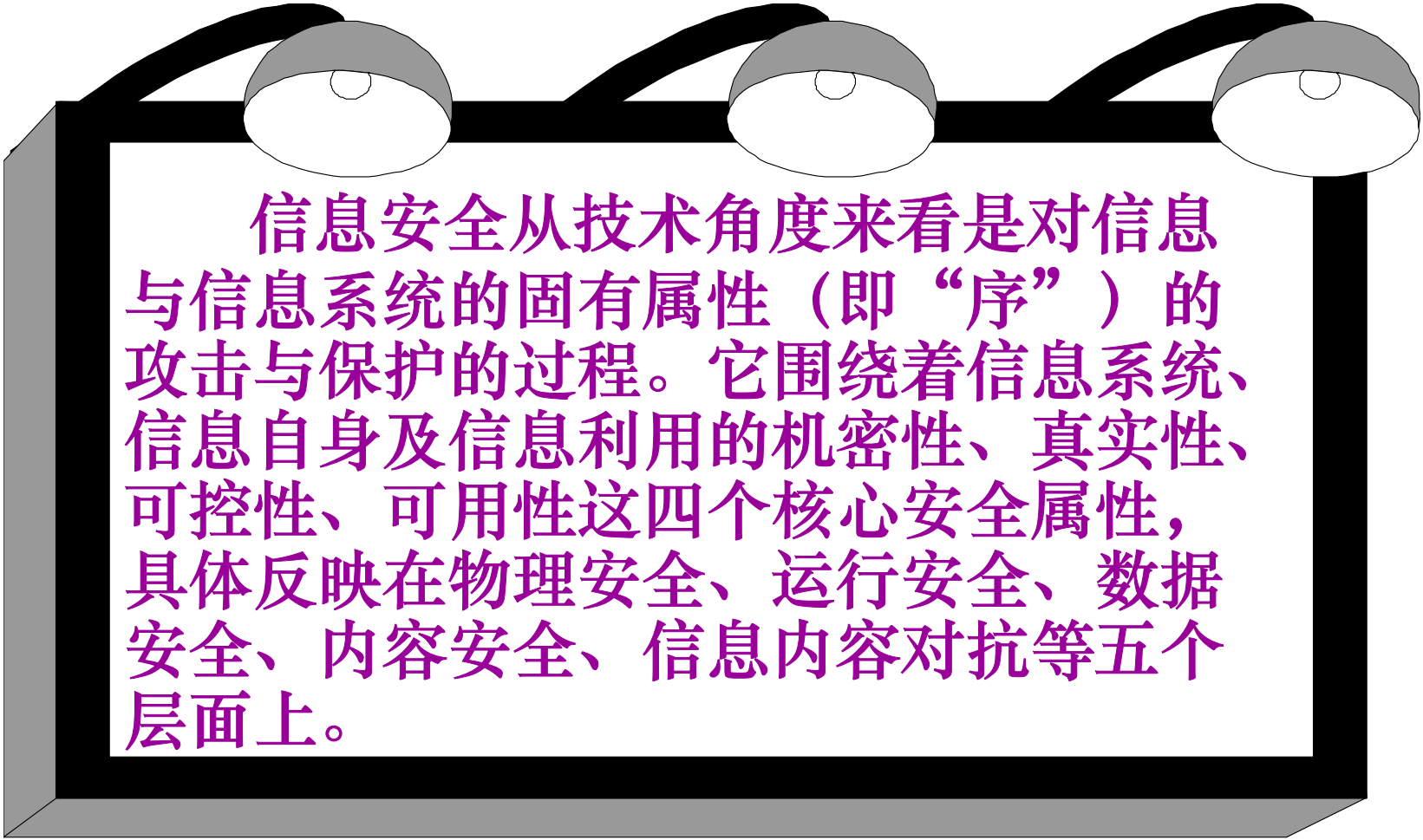
可用性 (**Av**)

信息安全四要素: **CACA**

# 信息安全经纬线—— 层次模型与要素模型的结合

	机密性	真实性	可控性	可用性
物理安全	✓	✓		✓
运行安全		✓	✓	✓
数据安全	✓	✓		✓
内容安全	✓	✓	✓	✓
信息内容 对抗	✓	✓		

# 结论：什么是信息安全？



信息安全从技术角度来看是对信息与信息系统的固有属性（即“序”）的攻击与保护的过程。它围绕着信息系统、信息自身及信息利用的机密性、真实性、可控性、可用性这四个核心安全属性，具体反映在物理安全、运行安全、数据安全、内容安全、信息内容对抗等五个层面上。

# 主要内容



- 信息安全及其关键技术
- 信息安全的理解（1.1）
- 信息安全威胁（1.2）
- 互联网的安全性（1.3）
- 信息安全体系结构（1.4）



# 1.1 信息的理解

## 1.1.1 信息与信息安全

### ○ 信息：事物运动的状态与方式

- ISO给出的解释：“信息是通过施加于数据上的某些约定而赋予这些数据的特定含义”。

- 通常我们可以把消息、信号、数据、情报和知识等都看作信息。信息本身是无形的，借助信息介质以多种形式存在或传播。

### ○ 信息安全

- ISO给出的定义：“在技术和管理上为数据处理系统建立的安全保护，保护信息系统的硬件、软件及相关数据不因偶然或者恶意的原因遭到破坏、更改及泄露”。

- 信息安全的目的是：“确保以电磁信号为主要形式的、在计算机网络化系统中进行获取、处理、存储、传输和应用的信  
息内容在各个物理及逻辑区域中的安全存在，并不发生任何侵害行为”。

# 1.1 信息的理解

## 1.1.2 信息的安全的发展阶段


- 信息安全发展：

- 通信安全→ 信息安全→信息保障

- 通信安全（COMSEC）


- 20世纪90年代以前，这一阶段的信息安全可以简单称为通信安全，主要目的是保障传递的信息安全，防止信源、信宿以外的对象查看信息。

# 通信安全



- 早期，所有的资产都是物理的，重要的信息也是物理的。
  - 如古代刻在石头上，到后来写在纸上。
- 为了保护这些资产，只需要用墙、护城河、警卫等物理安全措施。
  - 信息传递通常由信使完成，需要时可带有警卫。
- 除非用物理的掠夺，否则就无法得到信息。

# 通信安全



- 物理安全存在缺陷


- 如果报文在传递中被截获，则报文的信息就会被敌人知悉。因此就产生了通信安全的问题。
- 早在公元前600年Julius Caesar生成了Caesar密码，以使报文即使被截获也无法读出。

# 通信安全

- 第二次世界大战，德国人使用一种称为**Enigma**的机器来加密报文，用于军队，当时他们认为**Enigma**是不可破译的。确实是这样，如果使用恰当，要破译它非常困难。
- 但经过一段时间发现，由于某些操作员的使用差错，**Enigma**被破译了。



# 通信安全



- Navaho码的步话机

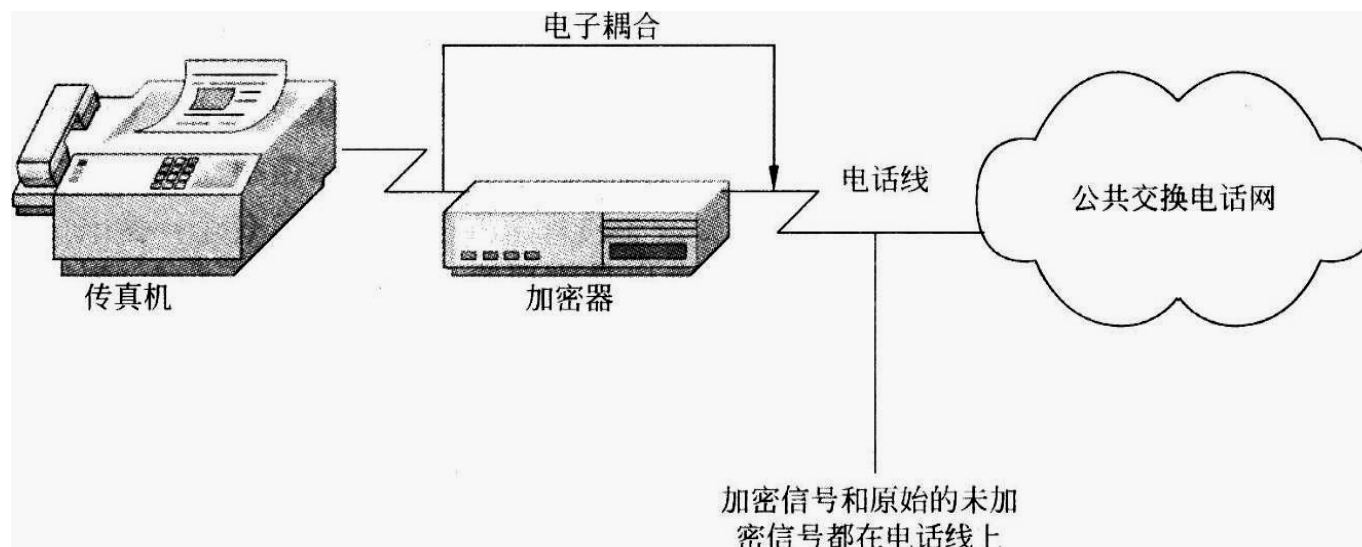
- 为了防止敌人窃听语音报文，美国军队曾使用一种Navaho码的步话机
- Navaho用本土语言传送报文，敌人即使收听到无线电通信，也无法懂得报文的意思。

# 通信安全

- 通信安全的主要目的是解决数据传输的安全问题，主要的措施是密码技术。
  - 除非不正确的使用密码系统，一般来说，好的密码难以破译。

# 通信安全

- 在20世纪50年代发现了寻找在电话线上的信号来达到获取报文的目的。



旁路密码的电子信号



# 1.1 信息的理解

## 1.1.2 信息的安全的发展阶段

### ○ 信息安全（INFOSEC）

- 20世纪90年代以后，主要保证信息的机密性、完整性、可用性、可控性、不可否认性。
  - 机密性（**Confidentiality**）指信息只能为授权者使用而不泄漏给未经授权者的特性。
  - 完整性（**Integrity**）指保证信息在存储和传输过程中未经授权不能被改变的特性。
  - 可用性（**Availability**）指保证信息和信息系统随时为授权者提供服务的有效特性。
  - 可控性（**Controllability**）指授权实体可以控制信息系统和信息使用的特性。
  - 不可否认性（**Non-Repudiation**）指任何实体均无法否认其实施过的信息行为的特性，也称为抗抵赖性。

# 1.1 信息的理解

## 1.1.2 信息安全的发展阶段

### ○ 信息保障(IA, Information Assurance)

#### ● 1996年美国人提出了信息保障:

- 保护 (Protect)、检测 (Detect)、反应 (React)、恢复 (Restore) 四个方面。

#### ● 我国也对信息保障给出了相关解释:

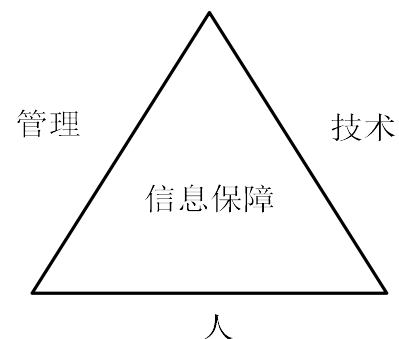
- “信息保障是对信息和信息系统的安全属性及功能、效率进行保障的**动态行为**过程。它运用源于**人、管理、技术**等因素所形成的**预警能力、保护能力、检测能力、反应能力、恢复能力**和**反击能力**，在信息和系统生命周期全过程的各个状态下，保证**信息内容、计算环境、边界与连接、网络基础设施**的**真实性、可用性、完整性、保密性、可控性、不可否认性**等安全属性，从而保障应用服务的效率和效益，促进信息化的可持续健康发展。”。

# 1.1 信息的理解

## 1.1.2 信息安全的发展阶段

- 信息保障三大要素。

- 人是信息保障的基础
- 技术是信息保障的核心
- 管理是信息保障的关键



- 信息安全不是一个孤立静止的概念，具有系统性、相对性和动态性。

## 1.2 信息安全威胁

### 1.2.1 信息安全威胁的基本类型

- 信息泄露:信息被有意或无意泄露给某个非授权的实体。
- 信息伪造:某个未授权的实体冒充其他实体发布信息，或者从事其他网络行为。
- 完整性破坏:非法手段窃取信息的控制权，未经授权对信息进行修改、插入、删除等操作，使信息内容发生不应有的变化。
- 业务否决或拒绝服务:攻击者通过对信息系统进行过量的、非法的访问操作使信息系统超载或崩溃，从而无法正常进行业务或提供服务。
- 未经授权访问:某个未经授权的实体非法访问信息资源，或者授权实体超越其权限访问信息资源。

# 1.2 信息安全威胁

## 1.2.2 信息安全威胁的主要表现形式

- 攻击原始资料
  - 人员泄露,废弃的介质,窃取
- 破坏基础设施
  - 破坏电力系统,破坏通讯网络,破坏信息系统场所
- 攻击信息系统
  - 物理侵入,特洛伊木马,恶意访问,服务干扰,旁路控制,计算机病毒,
- 攻击信息传输
  - 窃听,业务流分析,重放,
- 恶意伪造
  - 业务欺骗,假冒,抵赖
- 自身失误
- 内部攻击

## 1.3 互联网的安全性

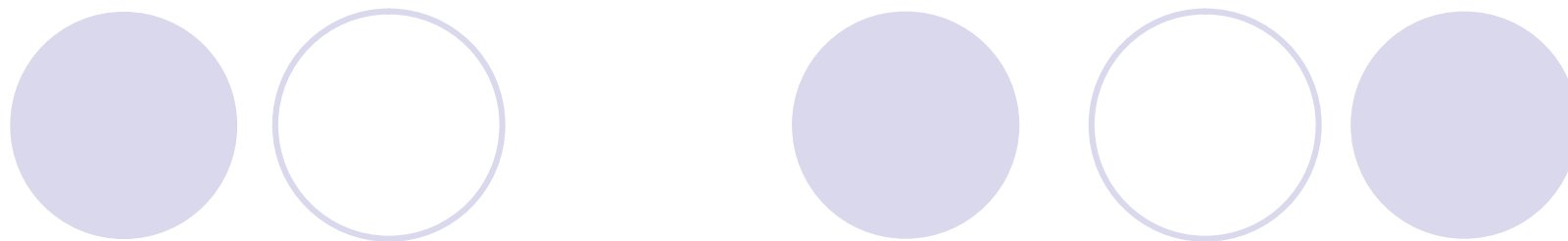
### 1.3.1 互联网的发展现状

- 1983年，ARPA和美国国防部通信局研制TCP/IP协议，该协议被做为其BSD UNIX的一部分。
- 1986年，NSF 利用Internet Protocol，连接5个科研教育服务机构，建立了NSFnet广域网。
- 1987年开始，中国四大网络CSTnet、CERNET、Chinanet、GBnet与Internet直连。
- 2007年底，我国互联网用户1.62亿，其中宽带上网用户达到1.22亿，中文网站89.8万个，IPv4地址总数9800多万个，国际出口带宽总量为368927 Mbps。

## 1.3 互联网的安全性

### 1.3.2 互联网的安全现状

- 2000年开始，病毒制造产业化操作，黑色产业链每年的整体利润预计高达数亿元。
- 窃取的个人资料
  - QQ密码、网游密码、银行账号、信用卡帐号,任何可以直接或间接转换成金钱的东西，都成为不法分子窃取的对象。
- CERT统计，
  - 在1988年安全事件6件，2001年5万件，2003年为13万7千多件，在2003年以后发生呈线性增长。
  - 据CCERT统计，2006年26476件，是2005年9112件的三倍。



○ 互联网安全不仅影响普通网民的信息和数据的安全性，而且严重的影响国家的健康发展。

- 网络安全与政治
- 网络安全与经济
- 网络安全与军事
- 网络安全与社会稳定

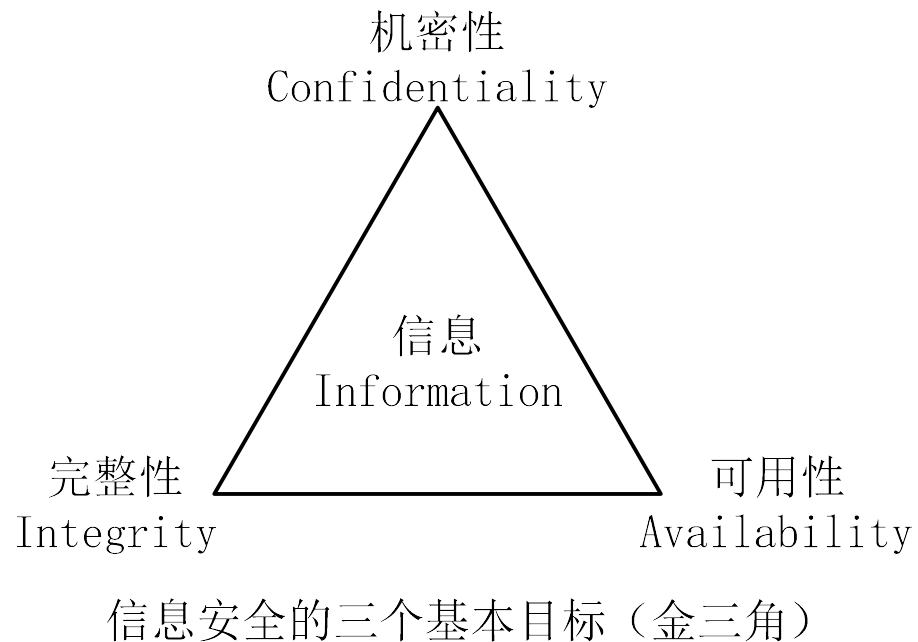


### 1.3.3 互联网的安全性分析

- 互联网的设计原始背景
- 网络传输的安全性
- 信息系统的安全性
  - 基础网络应用成为黑客及病毒的攻击重点。
  - 系统漏洞带来的安全问题异常突出。
  - Web程序安全漏洞愈演愈烈。
- 社会工程学攻击越来越多

## 1.4 信息安全体系结构

### ● 1.4.1 面向目标的知识体系结构

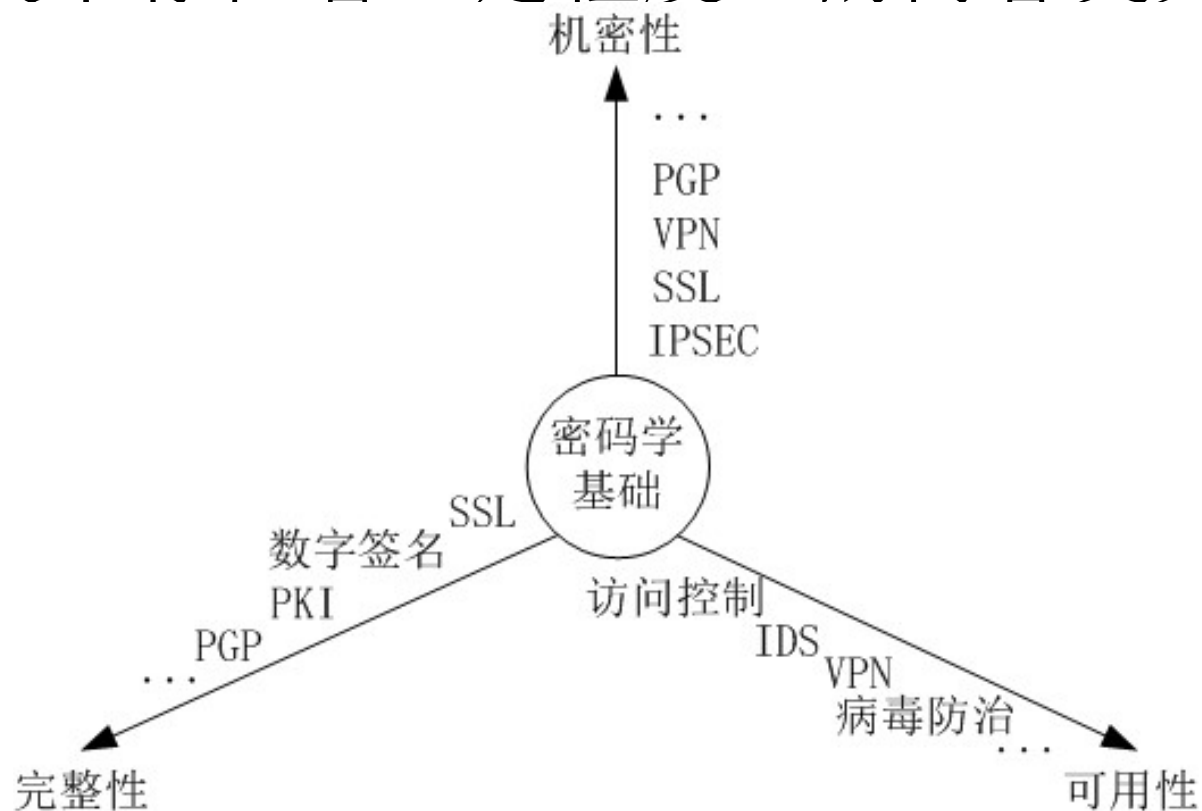


# CIA三元组

- CIA三元组是信息安全的三个最基本的目标
  - 机密性**Confidentiality**: 指信息在存储、传输、使用过程中，不会泄漏给非授权用户或实体；
  - 完整性**Integrity**: 指信息在存储、使用、传输过程中，不会被非授权用户篡改或防止授权用户对信息进行不恰当的篡改；
  - 可用性**Availability**: 指确保授权用户或实体对信息资源的正常使用不会被异常拒绝，允许其可靠而及时地访问信息资源。
- DAD（**Disclosure**、**Alteration**、**Destruction**）是最普遍的三类风险

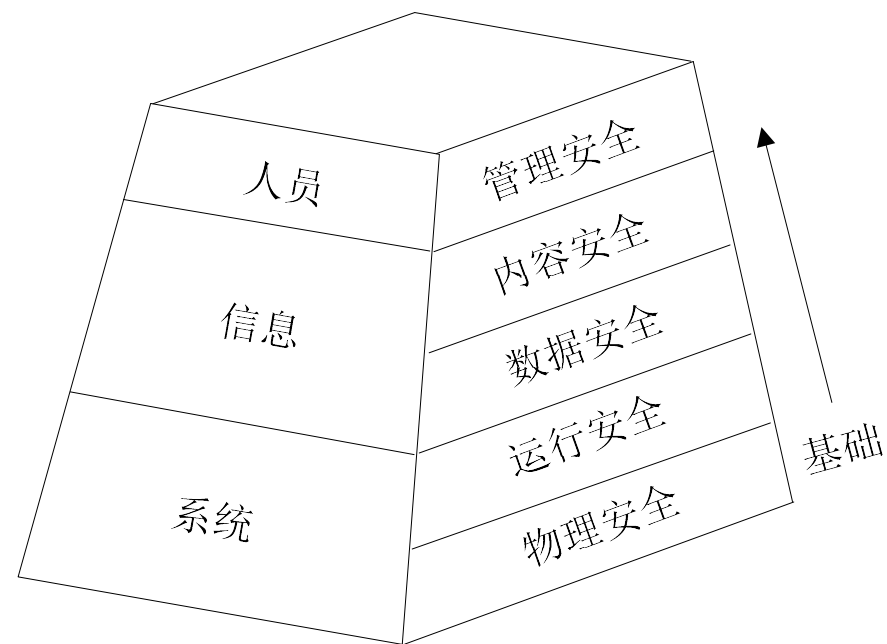
# 围绕CIA三元组展开的知识体系

- 密码学是三个信息安全目标的技术基础
- CIA技术存在着一定程度上的内容交叉



## 1.4.2 面向应用的层次型技术体系架构

- 信息系统基本要素
  - 人员、信息、系统
- 安全层次
  - 三个不同部分存在五个的安全层次与之对应
  - 每个层次均为其上层提供基础安全保证



面向应用的层次型信息安全技术体系结构



# 安全层次

## ● 物理安全

- 指对网络及信息系统物理装备的保护。

## ● 运行安全

- 指对网络及信息系统的运行过程和运行状态的保护。

## ● 数据安全

- 指对数据收集、存储、检索、传输等过程提供的保护，不被非法冒充、窃取、篡改、抵赖。

## ● 内容安全

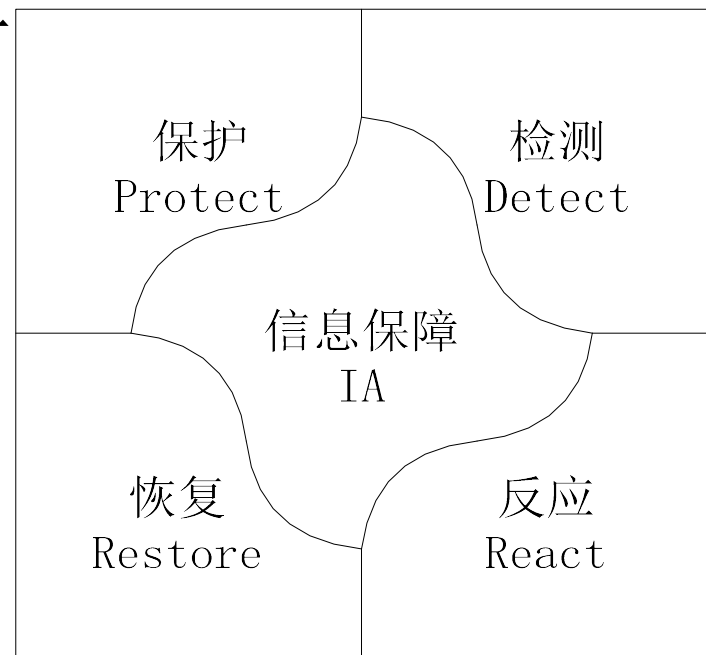
- 指依据信息内涵判断是否违反特定安全策略，采取相应的安全措施。

## ● 管理安全

- 指通过针对人的信息行为的规范和约束，提供对信息的机密性、完整性、可用性以及可控性的保护。

### 1.4.3 面向过程的信息安全保障体系

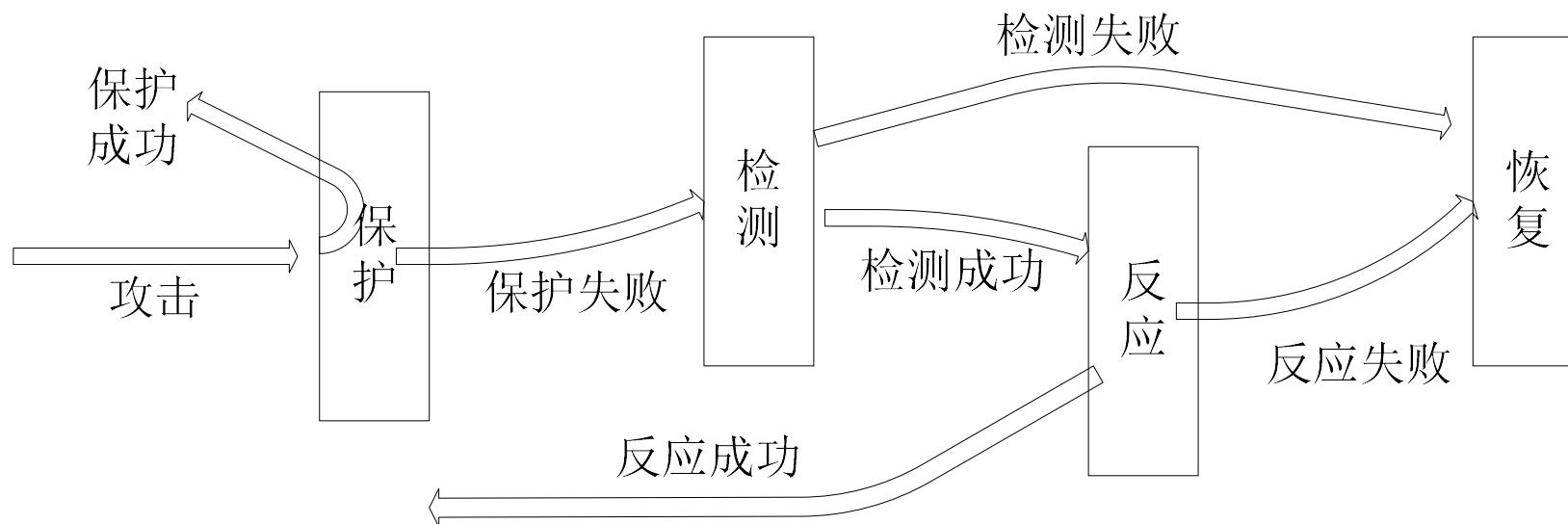
- 美国国防部提出的“信息安全保障体系”为诠释了安全保障的内涵。
- 信息安全保障体系包括四个部分内容，即PDRR。
  - 保护（Protect）
  - 检测（Detect）
  - 反应（React）
  - 恢复（Restore）



信息保障体系

### 1.4.3 面向过程的信息安全保障体系

- 信息安全保障是一个完整的动态过程，而保护、检测、反应和恢复可以看作信息安全保障四个子过程。



PDRR 模型安全保障动态过程示意图



# PDRR

- 这四个部分组成了一个动态的信息安全周期。



# 安全策略



- 防御

- 根据系统已知的所有的安全问题做出防御的措施。
- 如打补丁、访问控制、数据加密等等。

- 检测

- 攻击者如果穿过了防御系统，检测系统就会检测出来。
- 检测的功能就是检测出入侵者的身份，包括攻击源、系统损失等。

- 响应

- 一旦检测出入侵，响应系统开始响应包括事件处理和其他业务。

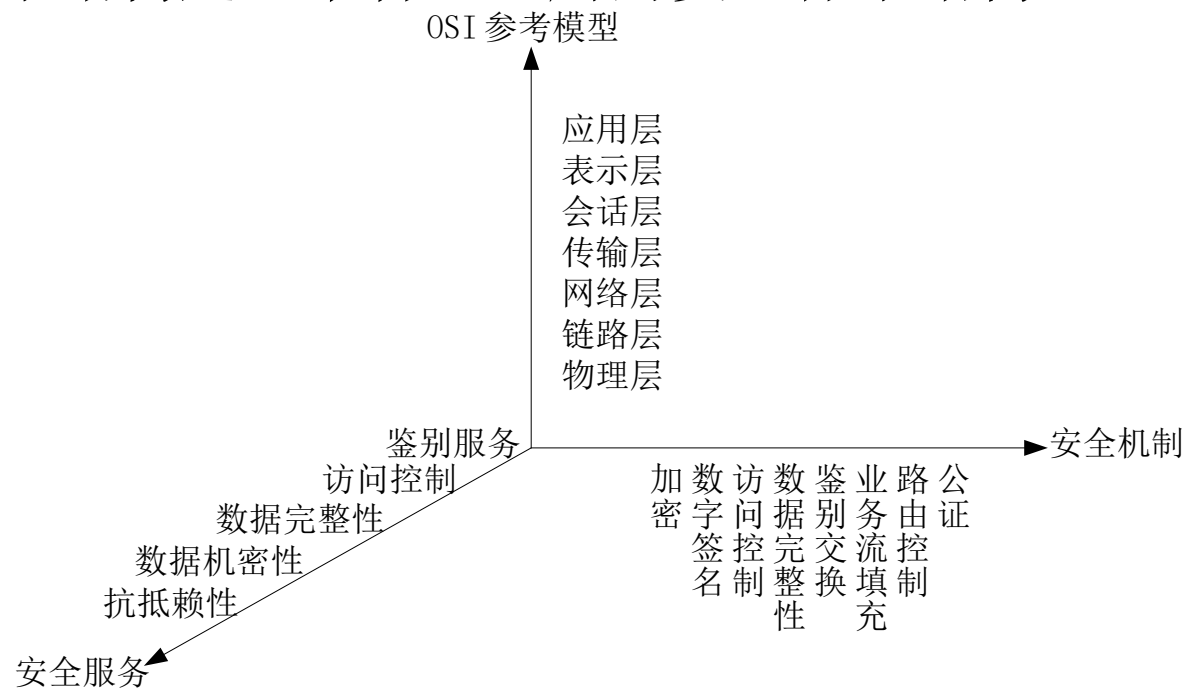
- 恢复。

- 在入侵事件发生后，把系统恢复到原来的状态。

## 1.4.4 OSI开放系统互连安全体系结构

### ○ ISO7498-2 (1989)

- 《信息处理系统、开放系统互连、基本参考模型—第2部分：安全体系结构》。描述的开放系统互联安全体系结构是一个普遍适用的安全体系结构



ISO7498-2 安全体系结构三维图

# 安全服务（Security Service）

- 鉴别服务 确保某个实体身份的可靠性。
- 访问控制 确保只有经过授权的实体才能访问受保护的资源。
- 数据机密性 确保只有经过授权的实体才能理解受保护的信息。
- 数据完整性 防止对数据的未授权修改和破坏。
- 抗抵赖性 用于防止对数据源以及数据提交的否认。

# 对付典型网络威胁的安全服务

安全威胁	安全服务
假冒攻击	鉴别服务
非授权侵犯	访问控制服务
窃听攻击	数据机密性服务
完整性破坏	数据完整性服务
服务否认	抗抵赖服务
拒绝服务	鉴别服务、访问控制服务、数据完整性服务等

# 安全机制（Security Mechanism）

- 加密 用于保护数据的机密性。
- 数字签名 保证数据完整性及不可否认性的一种重要手段。
- 访问控制 访问实体成功通过认证，访问控制对访问请求进行处理，查看是否具有访问所请求资源的权限，并做出相应的处理。
- 数据完整性 用于保护数据免受未经授权的修改。
- 鉴别交换 用于实现通信双方实体的身份鉴别。
- 业务流填充 针对的是对网络流量进行分析攻击。
- 路由控制 可以指定数据报文通过网络的路径。路径上的节点都是可信任的
- 公证机制 由第三方来确保数据完整性、数据源、时间及目的地的正确。

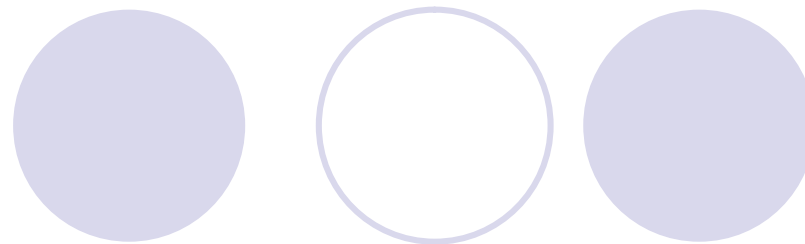
# OSI安全服务与安全机制的关系

服务	机制							
	加密	数字 签名	访问 控制	数据 完整性	鉴别 交换	通信业 务填充	路由 控制	公证
对等实体鉴别	Y	Y			Y			
数据原发鉴别	Y	Y						
访问控制服务			Y					
连接机密性	Y						Y	
无连接机密性	Y						Y	
选择字段机密性	Y							
通信业务流机密性	Y					Y	Y	
带恢复的连接完整性	Y			Y				
不带恢复的连接完整性	Y			Y				
选择字段连接完整性	Y			Y				
无连接完整性	Y	Y		Y				
选择字段无连接完整性	Y	Y		Y				
有数据原发证明的抗抵赖		Y		Y				Y
有交付证明的抗抵赖		Y		Y				Y

说明：Y表示机制适合提供该种服务，空格表示机制不适合提供该种服务。

# 密码学基础

- 对称密码
- 非对称密码





# Symmetric Encryption

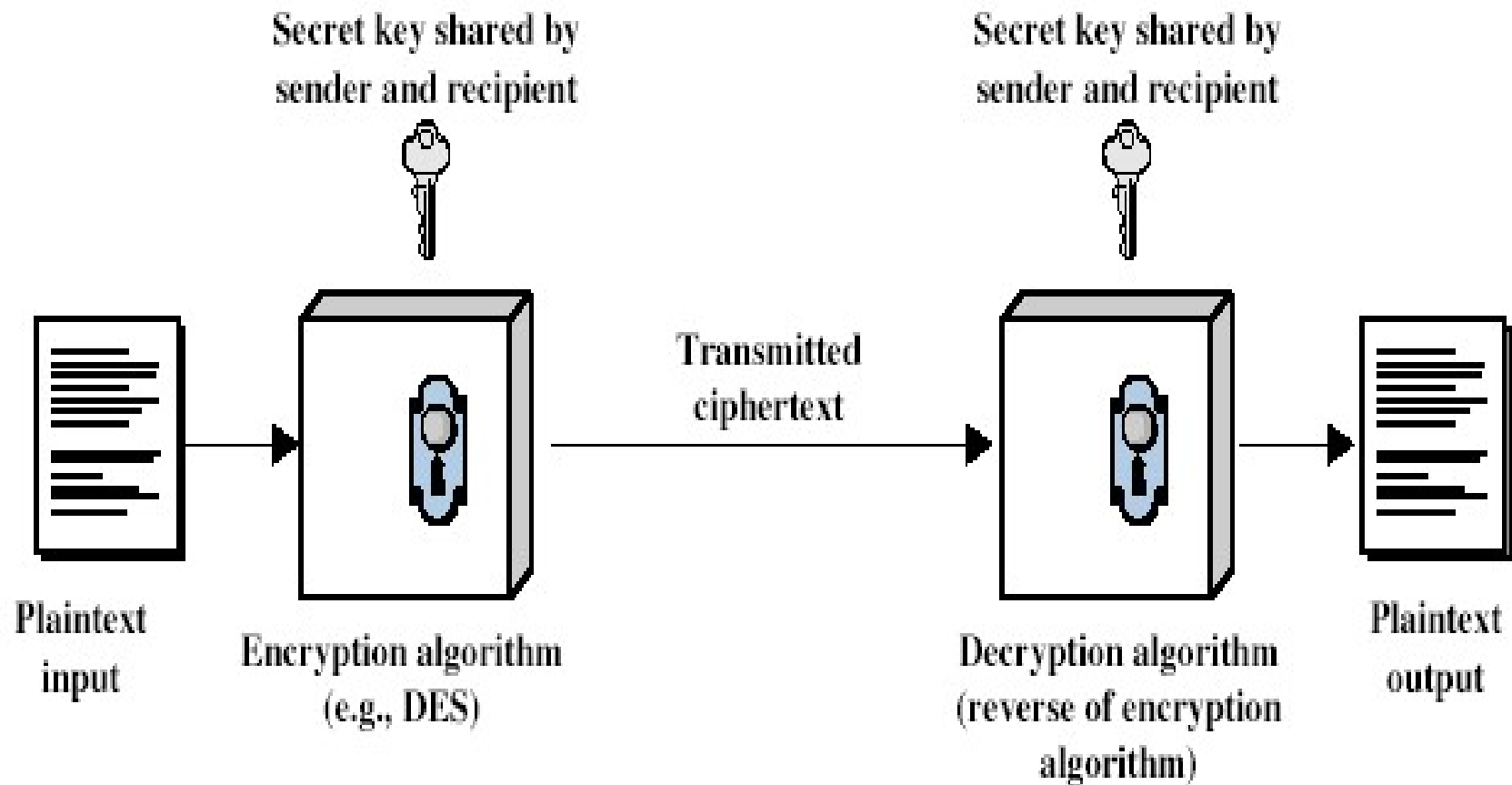
- or conventional / private-key / single-key
- sender and recipient share a common key
- all classical encryption algorithms are private-key (私钥)
- was only type prior to invention of public-key in 1970's
- and by far most widely used



# Some Basic Terminology

- **plaintext** (明文)- original message
- **Ciphertext** (密文) - coded message
- **cipher** (加密算法)- algorithm for transforming plaintext to ciphertext
- **Key** (密钥)- info used in cipher known only to sender/receiver
- **encipher (encrypt)** (加密)- converting plaintext to ciphertext
- **decipher (decrypt)** (解密)- recovering ciphertext from plaintext
- **cryptography** (密码编码学)- study of encryption principles/methods
- **cryptanalysis (codebreaking)** (密码分析学)- study of principles/ methods of deciphering ciphertext *without* knowing key
- **cryptology** (密码学)- field of both cryptography and cryptanalysis

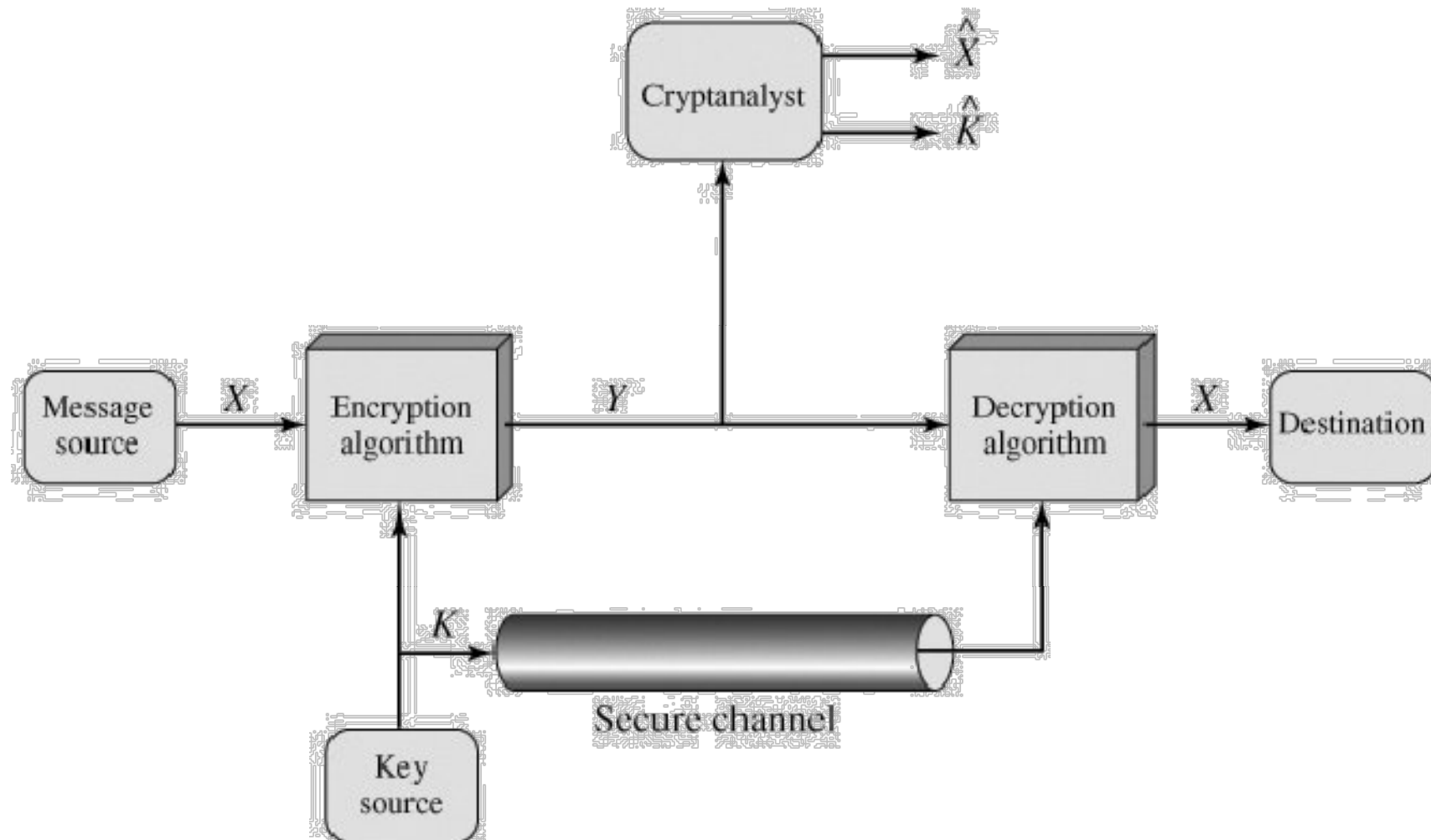
# Symmetric Cipher Model



# Requirements

- two requirements for secure use of symmetric encryption:
  - a strong encryption algorithm
  - a secret key known only to sender / receiver
- mathematically have:
$$Y = E_K(X)$$
$$X = D_K(Y)$$
- assume encryption algorithm is known
- implies a secure channel to distribute key

# Model of Conventional Cryptosystem



# Cryptography

- characterize cryptographic system by:
  - type of encryption operations used
    - Substitution(代換) / transposition(置換) / product(乗積)
  - number of keys used
    - single-key or private / two-key or public
  - way in which plaintext is processed
    - block / stream

# Cryptanalysis



- objective to recover key not just message
- general approaches:
  - cryptanalytic attack
  - brute-force attack(穷举攻击)



# Cryptanalytic Attacks

- **ciphertext only**

- only know algorithm & ciphertext, is statistical, know or can identify plaintext

- **known plaintext**

- know/suspect plaintext & ciphertext

- **chosen plaintext**

- select plaintext and obtain ciphertext

- **chosen ciphertext**

- select ciphertext and obtain plaintext

- **chosen text**

- select plaintext or ciphertext to en/decrypt



# More Definitions



- **unconditional security**

- no matter how much computer power or time is available, the cipher cannot be broken since the ciphertext provides insufficient information to uniquely determine the corresponding plaintext

- **computational security**

- given limited computing resources (eg time needed for calculations is greater than age of universe), the cipher cannot be broken

# Brute Force Search

- always possible to simply try every key
- most basic attack, proportional to key size
- assume either know / recognise plaintext

Key Size (bits)	Number of Alternative Keys	Time required at 1 decryption/ $\mu$ s	Time required at $10^6$ decryptions/ $\mu$ s
32	$2^{32} = 4.3 \times 10^9$	$2^{31} \mu$ s = 35.8 minutes	2.15 milliseconds
56	$2^{56} = 7.2 \times 10^{16}$	$2^{55} \mu$ s = 1142 years	10.01 hours
128	$2^{128} = 3.4 \times 10^{38}$	$2^{127} \mu$ s = $5.4 \times 10^{24}$ years	$5.4 \times 10^{18}$ years
168	$2^{168} = 3.7 \times 10^{50}$	$2^{167} \mu$ s = $5.9 \times 10^{36}$ years	$5.9 \times 10^{30}$ years
26 characters (permutation)	$26! = 4 \times 10^{26}$	$2 \times 10^{26} \mu$ s = $6.4 \times 10^{12}$ years	$6.4 \times 10^6$ years

## 密码学重要进步

- 从Rotor到DES

- New Directions in Cryptography

*Whitfield Diffie, Hellman 1976*

- 提出了公钥密码算法的概念和思路
- 提出了鉴别和签名问题
- 提出了D-H密钥协商协议

- 其他

Bobby Inman/NSA, James Ellis, Clifford Cocks

# 公钥密码算法的思路

- 对称算法的缺陷

- 为事先协商密钥，需另外的安全信道或KDC
- 不能满足签名的需求

- 非对称算法

密钥  $K = (K_d, K_e)$ ， $K_d$ 即私钥  $K_e$ 即公钥

加密： $E(P, K_e) = C$

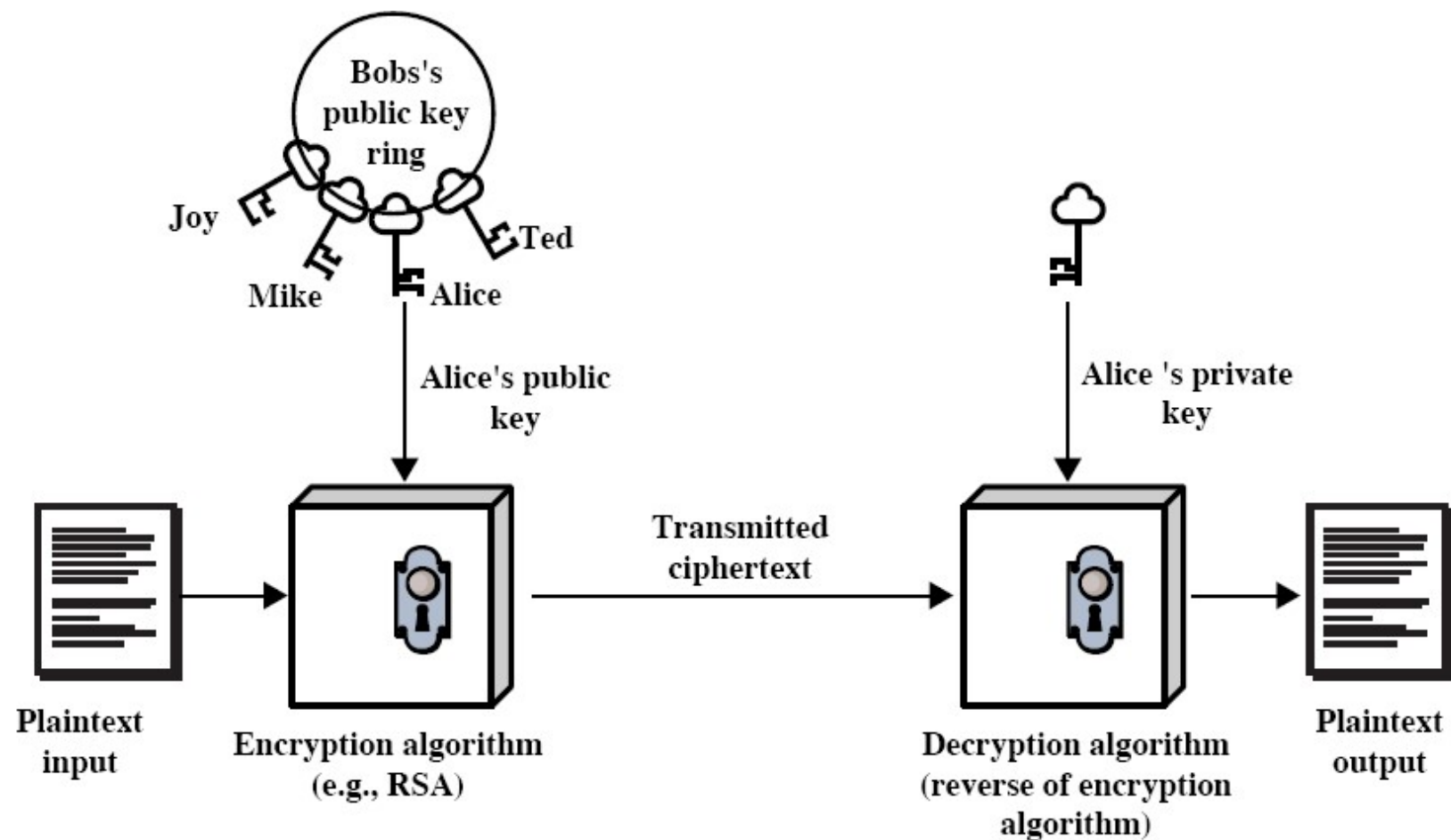
解密： $D(C, K_d) = P$

要求从 $K_e$  

- 理论上能够

实际上需要计算量太大因而很难

# 公开密钥加密过程



(a) Encryption

# 公开密钥认证过程

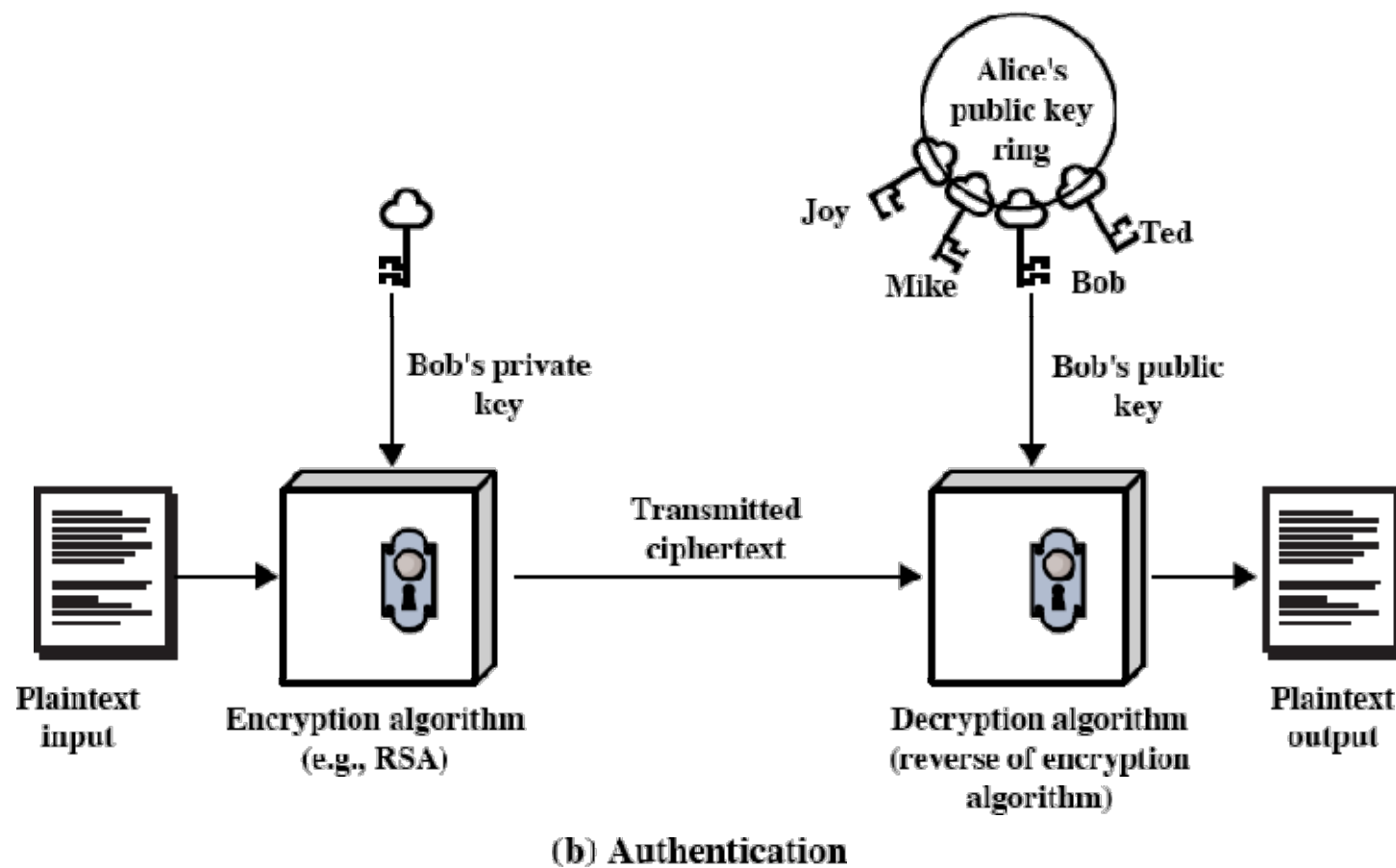


Figure 9.1 Public-Key Cryptography

# 常规和公开密钥加密的重要特征

TABLE 6.1 CONVENTIONAL AND PUBLIC-KEY ENCRYPTION

## Conventional Encryption

### *Needed to Work:*

1. The same algorithm with the same key is used for encryption and decryption.
2. The sender and receiver must share the algorithm and the key.

### *Needed for Security:*

1. The key must be kept secret.
2. It must be impossible or at least impractical to decipher a message if no other information is available.
3. Knowledge of the algorithm plus samples of ciphertext must be insufficient to determine the key.

## Public-Key Encryption

### *Needed to Work:*

1. One algorithm is used for encryption and decryption with a pair of keys, one for encryption and one for decryption.
2. The sender and receiver must each have one of the matched pair of keys (not the same one).

### *Needed for Security:*

1. One of the two keys must be kept secret.
2. It must be impossible or at least impractical to decipher a message if no other information is available.
3. Knowledge of the algorithm plus one of the keys plus samples of ciphertext must be insufficient to determine the other key.



# 公开密钥密码系统的应用

- 加密/解密：发送方用接收方的公开密钥加密报文
- 数字签名：发送方用自己的私有密钥“签署”报文
- 密钥交换：两方合作以交换会话密钥



# Applications for Public-Key Cryptosystems

Algorith m	Encryption /Decryption	Digital Signature	Key Exchang e
RSA	Yes	Yes	Yes
Elliptic Curve	Yes	Yes	Yes
Diffie- Hellman	No	No	Yes
DSS	No	Yes	No

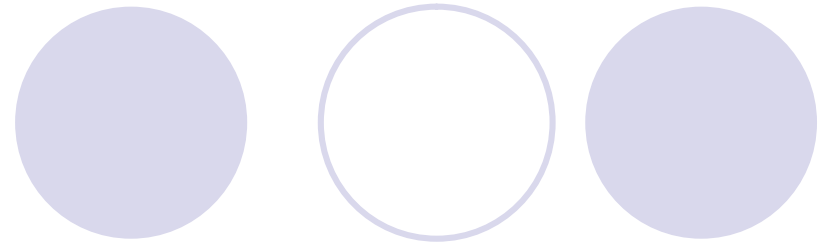
# 对公开密钥密码编码系统的要求

- 容易计算公开密钥 $k_e$ 和私有密钥 $k_d$
- 不难计算 $C=E(k_e, m)$ 和 $m=D(k_d, c)$
- 不知道 $k_d$ ，即使知道 $k_e, E, D$ 及 $c$ ，计算 $m$ 也不可行
- 即使知道 $k_e, E, D$ 及 $c$ ，计算 $k_d$ 也不可行
- $D(k_d, E(k_e, m))=m$ ，且 $E(k_e, D(k_d, c))=c$
- 加密变换和解密变换可以互换顺序，即 $D(E(m))=E(D(m))$

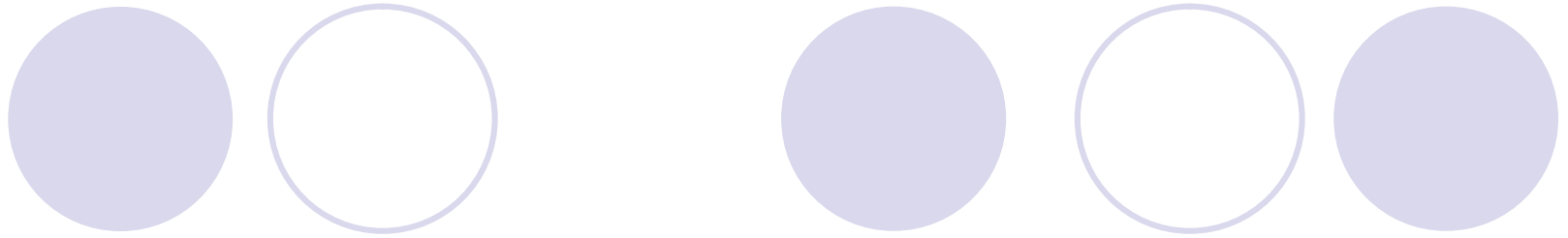
# 对公开密钥密码编码系统的要求

- 1976年，Whitfield Diffie和Martin Hellman提出这样的设想：
  - 每个用户A有一加密密钥 $k_a$ ，不同于解密密钥 $k_a'$ ，可将加密密钥 $k_a$ 公开， $k_a'$ 保密，要求 $k_a$ 的公开不影响 $k_a'$ 的安全。若B要向A秘密发送明文 $m$ ，可查A的公开密钥 $k_a$ ，加密得密文 $C = E_{k_a}(m)$
  - A收到C后用只有A才拥有的解密密钥 $k_a'$ 对C进行解密得 $m = D_{k_a'}(C)$ .

# 公钥密码算法的实现



- 对称算法
  - 替换
  - 混乱
- 基于某些数学特性
  - 从公钥推导私钥理论可能，但计算困难  
(从私钥到公钥容易)
  - 实用方案的发展依赖于单向陷井函数
- 单向函数(one-way function)



***Any question?***