大学计算机基础

教学课件

北京航空航天大学

第7章 信息安全

7.1 怎样才算信息安全

7.2 关于计算机病毒

7.3要保证信息安全可以采用哪些技术

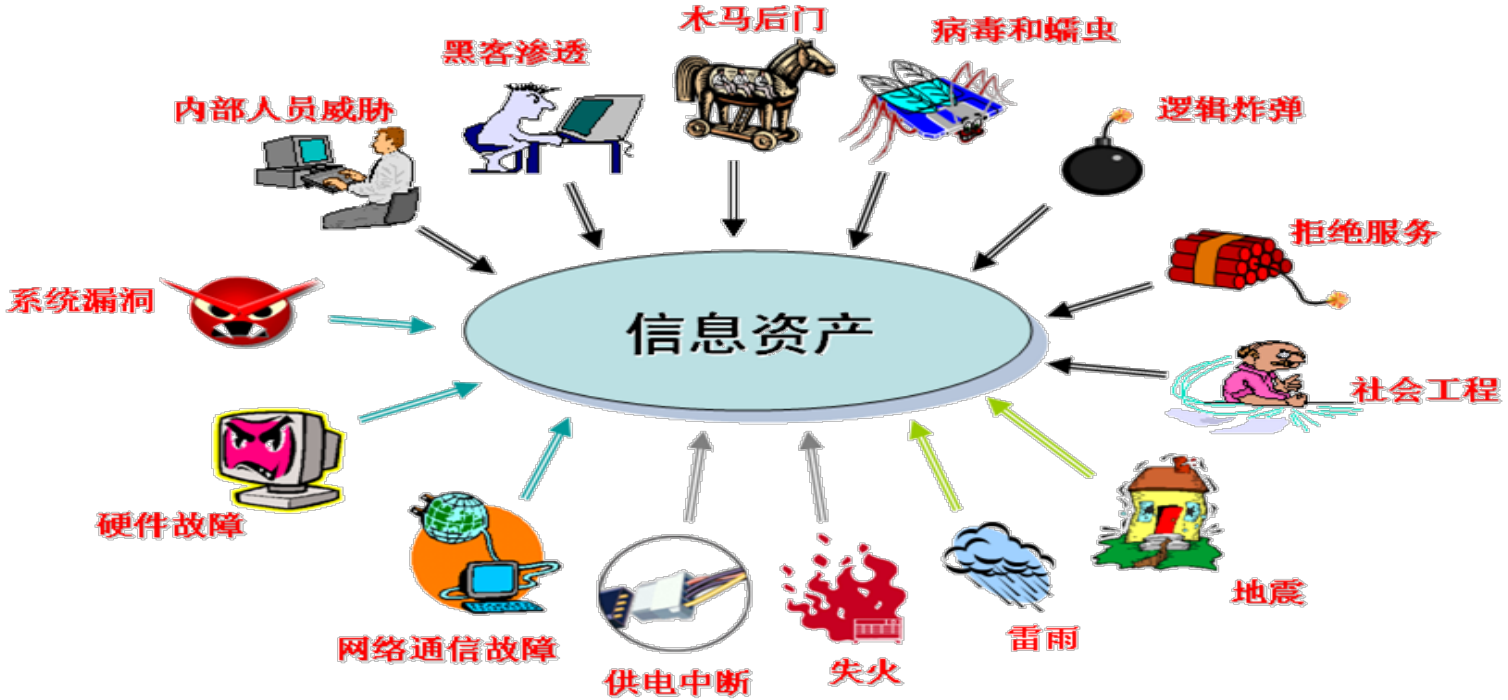
本章重点

- 什么是信息安全？
- 怎样保障信息安全？有哪些信息安全技术？
- 密码学的原理与应用
- 什么是计算机病毒？计算机病毒如何分类和防范？

什么是信息？

- ISO 13335《信息技术安全管理指南》定义：信息是通过在数据上施加某项约定而赋予这些数据的特殊含义。

信息面临哪些安全威胁？

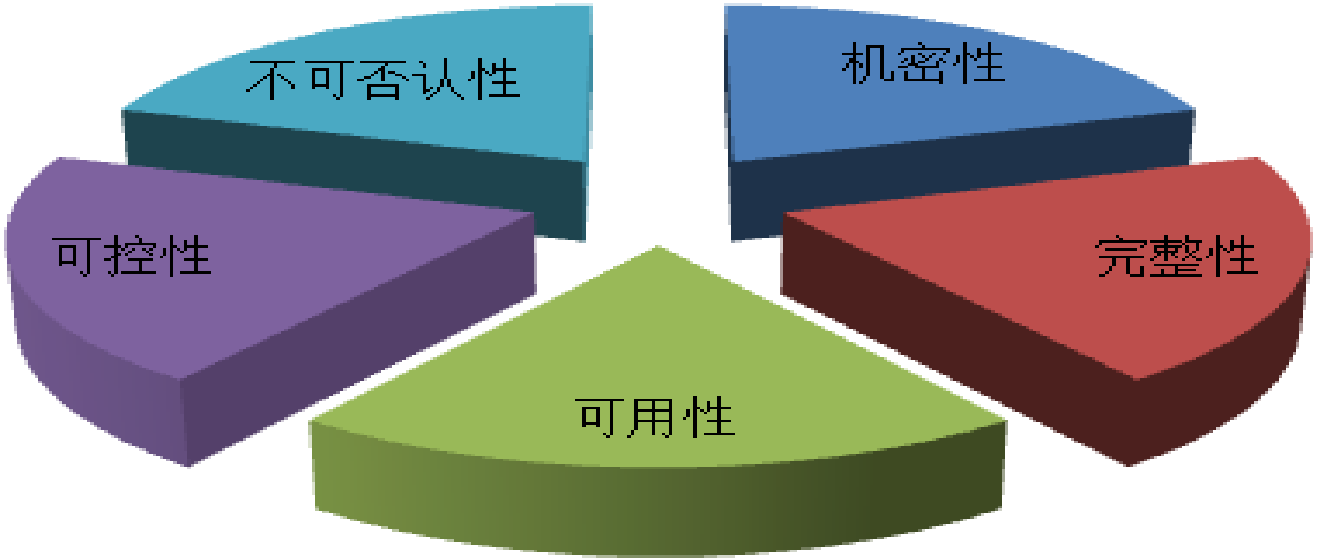


如何保障信息的安全？

信息的价值在哪些情况下会丧失？

- 机密性（泄密…）
- 可用性（被盗、损坏…）
- 完整性（被恶意修改…）
- 不可否认性（赖账…）
- …

信息安全目标

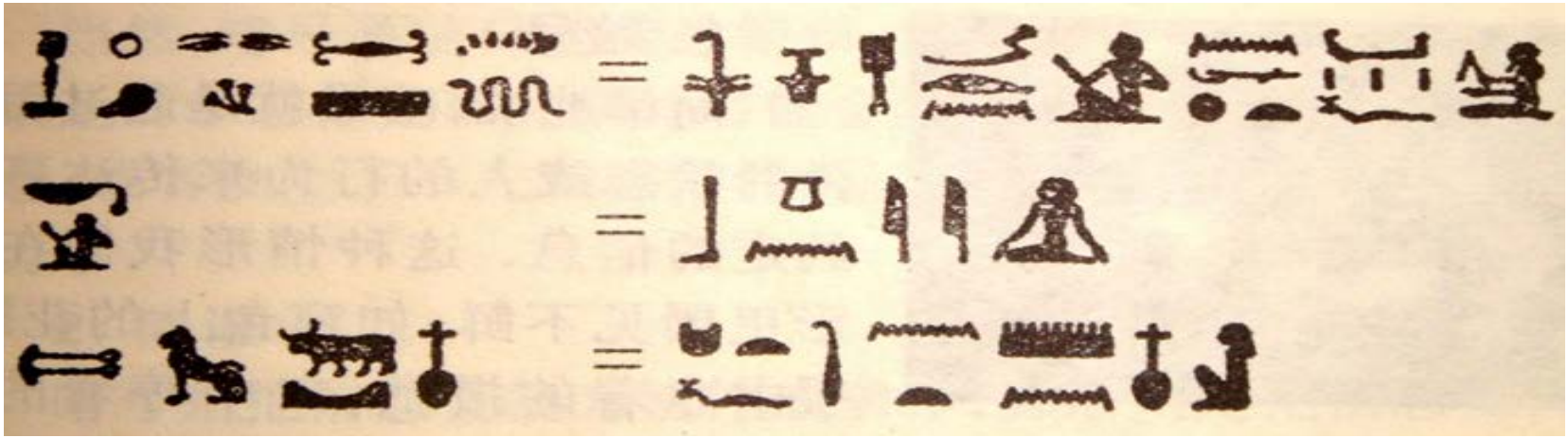


密码学概述

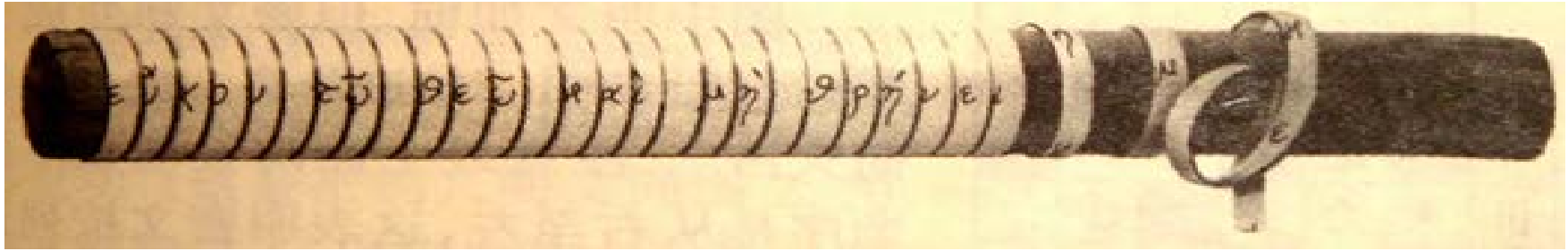
- 生活中的问题
  - 银行卡里的钱被盗取
    - ——丢失的卡上直接写着密码“123456”
  - 古代的保密意识

古埃及的原始密码

- 公元前19世纪，古埃及第十二王朝，祭司用一些奇怪的符号来代替常用的象形文字，撰写碑文



斯巴达人的“天书”密码

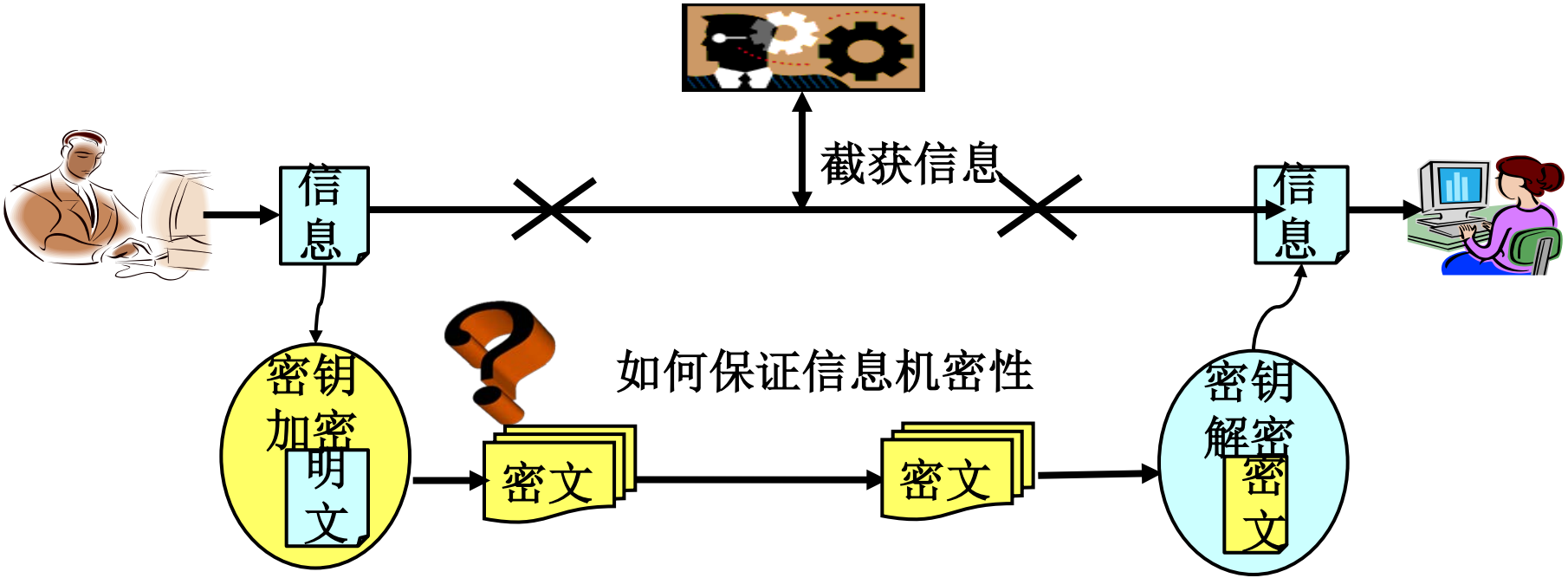


战争时期的密码

密码学领域

- 密码学
  - 对己方信息进行保护，对敌方信息进行破译的科学
  - 密码学(Cryptology) =密码编码学(Cryptography) + 密码分析学(Cryptoanalysis)

保障信息的机密性



几个基本概念

- 明文、密文
- 加密、解密

密码系统

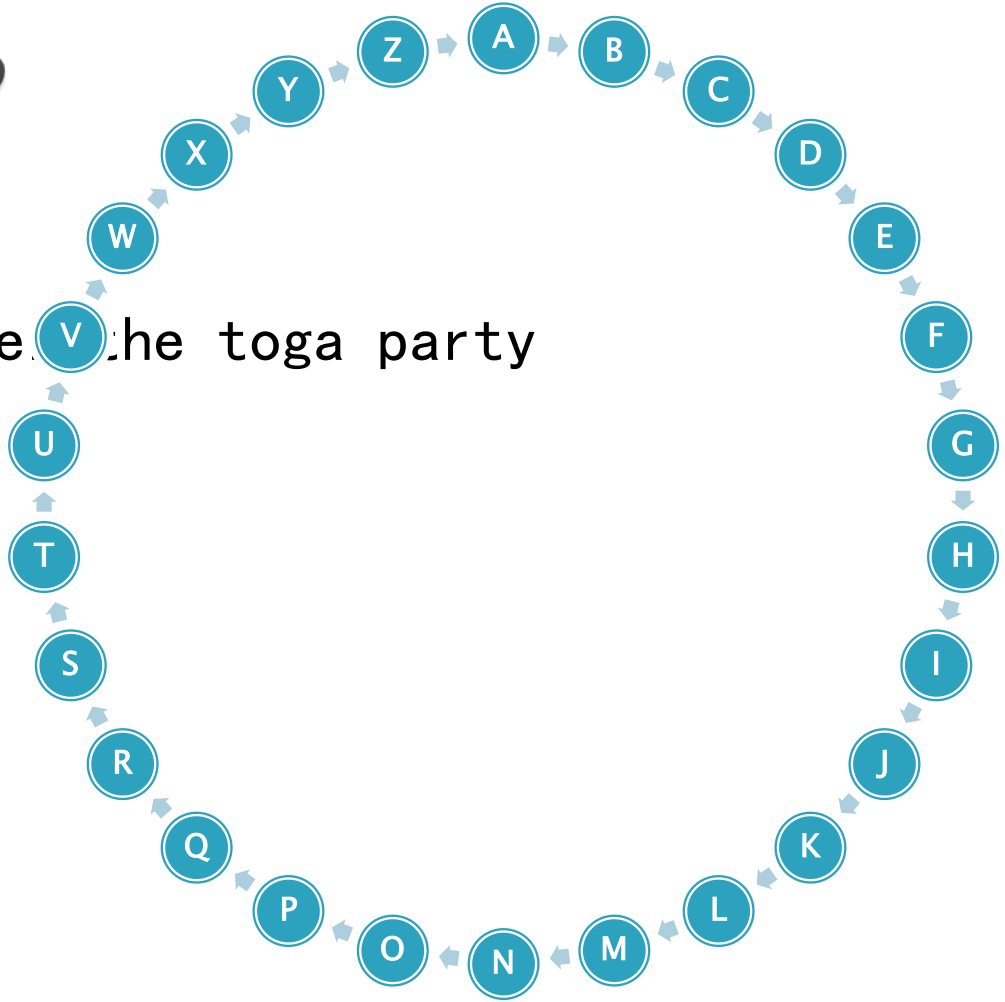
- 密码体制：密码系统采用的基本工作方式（加密方案）。
- 密码体制的基本要素：密码算法和密钥。

密码体制的安全性

- 无条件安全 unconditional security
- 可证明安全 provable security
- 计算上安全 computational security

明文怎样加密？

- 已知：
  - 明文：meet me after the toga party
- 怎样加密？



代换密码（替代密码）

- 代换：将明文字母替换成其他字母、数字或符号
- 凯撒密码Caesar密码
  - 最早的代换密码
- 例：
  - 明文：meet me after the toga party
  - 密文：PHHW PH DIWHU WKH WRJD SDUWB
- 改进：将每个字母用字母表中它之后的第k个字母替代

凯撒密码加密程序

```
void main()
 { char c;
    while((c=getchar())!='\n')
       {   if((c>='a' && c<='z') || (c>='A' && c<='Z'))
             { c=c+3;
               if (c>'Z' && c<='Z'+3 || c>'z')
                    c=c-26;
             }
         printf("%c",c);
         }
```

凯撒密码解密程序

```
void main()
 { char c;
    while((c=getchar())!='\n')
      {   if((c>='a' && c<='z') || (c>='A' && c<='Z'))
            { c=c-3;
              if (c<'A' ||  c<'a' && c>='a'-3)
                    c=c+26;
              }
           printf("%c",c);
       }
```

凯撒密码的安全性

- 安全性：
  - 密钥只有25个可用
  - 可以使用穷举攻击，依次尝试便可
    - 最坏情况需要尝试25次
    - 平均需要尝试25/2=12.5次
  - 破译结果需要人为辨别对错
    - 明文可以理解
    - 编码或压缩会使得明文难以辨别，增加破译工作量

凯撒密码的改进——单表代换密码

- 每个明文字母按照密钥替换为一个新的字母
- 密钥长度26个字母，例：

  明文：a b c d e f g h i j k l m n o p q r s t u v w x y z

  加密：D K V Q F I B J W P E S C X H T M Y A U O L R G Z N

  明文：i f w e w i s h t o r e p l a c e l e t t e r s

  密文：W I R F R W A J U H Y F T S D V F S F U U F Y A
- 密钥空间大小：$26! \approx 4 \times 10^{26}$

单表代换的改进——多表代换密码

- 为了减少明文结构在密文中的残留程度
- 几种典型的多表代换密码
  - Playfair密码
  - Hill密码Vigen è re密码
- 杰斐逊的轮子密码机M-94

置换密码

- 换位（重新排列消息中的字母）
- 最简单的置换密码是把明文中字母顺序倒过来
  - 如：　　cryptography
  - 加密为：yhpargotpyrc

典型置换密码

- 明文：cryptography is an applied science
- 密钥：encry

密钥	2	3	1	4	5
	c	r	y	p	t
	o	g	r	a	p
	h	y	i	s	a
	n	a	p	p	l
	i	e	d	s	c
	i	e	n	c	e

- ✓ 密文：yripdn cohnii rgyaee paspsc tpalce

古典密码特点

- 密码学还不是科学，而是艺术；
- 出现一些简单的密码算法和加密设备；
- 密码算法的基本手段出现，针对的是字符；
- 简单的密码分析手段出现；

主要特点：

数据的安全基于算法的保密

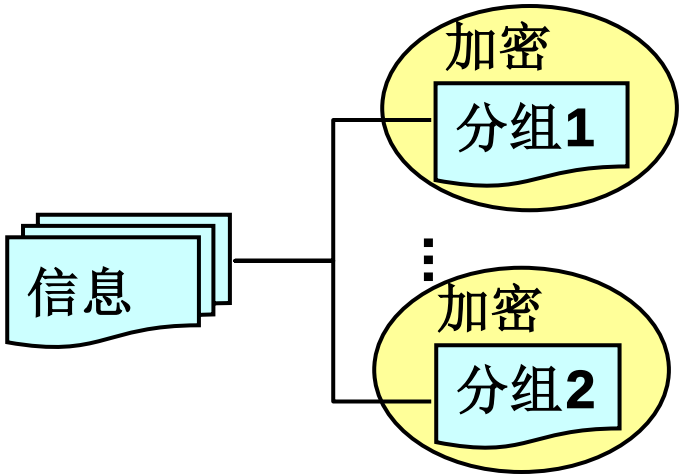
现代密码特点

计算机使得基于复杂计算的密码成为可能。

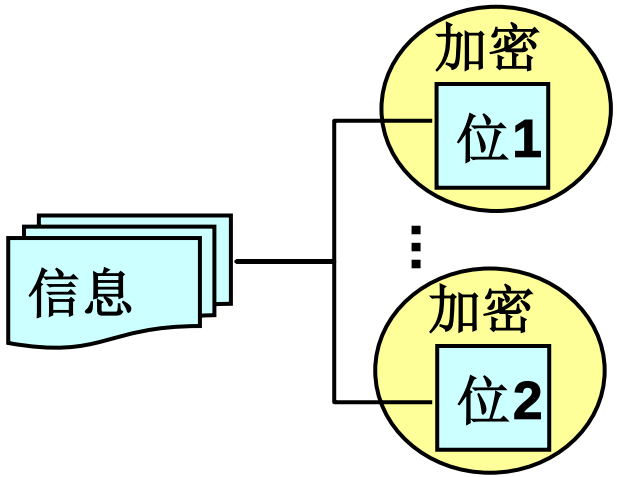
主要特点

- 数据的安全**基于密钥**而不是算法的保密

分组加密和序列加密



分组加密



序列加密

典型算法：DES、IDEA、AES等。

对称密钥标准DES

- DES：由IBM公司研制的，1977年被美国政府采纳作为非绝密信息的正式标准
- 56比特对称密钥，64比特明文输入
- 初始置换
- 16轮相同的“迭代”操作，每一轮都使用不同的48比特密钥
- 最终置换

DES初始置换IP

M_1	M_2	M_3	M_4	M_5	M_6	M_7	M_8
M_9	M_{10}	M_{11}	M_{12}	M_{13}	M_{14}	M_{15}	M_{16}
M_{17}	M_{18}	M_{19}	M_{20}	M_{21}	M_{22}	M_{23}	M_{24}
M_{25}	M_{26}	M_{27}	M_{28}	M_{29}	M_{30}	M_{31}	M_{32}
M_{33}	M_{34}	M_{35}	M_{36}	M_{37}	M_{38}	M_{39}	M_{40}
M_{41}	M_{42}	M_{43}	M_{44}	M_{45}	M_{46}	M_{47}	M_{48}
M_{49}	M_{50}	M_{51}	M_{52}	M_{53}	M_{54}	M_{55}	M_{56}
M_{57}	M_{58}	M_{59}	M_{60}	M_{61}	M_{62}	M_{63}	M_{64}

M_{58}	M_{50}	M_{42}	M_{34}	M_{26}	M_{18}	M_{10}	M_2
M_{60}	M_{52}	M_{44}	M_{36}	M_{28}	M_{20}	M_{12}	M_4
M_{62}	M_{54}	M_{46}	M_{38}	M_{30}	M_{22}	M_{14}	M_6
M_{64}	M_{56}	M_{48}	M_{40}	M_{32}	M_{24}	M_{16}	M_8
M_{57}	M_{49}	M_{41}	M_{33}	M_{25}	M_{17}	M_9	M_1
M_{59}	M_{51}	M_{43}	M_{35}	M_{27}	M_{19}	M_{11}	M_3
M_{61}	M_{53}	M_{45}	M_{37}	M_{29}	M_{21}	M_{13}	M_5
M_{63}	M_{55}	M_{47}	M_{39}	M_{31}	M_{23}	M_{15}	M_7

初始置换前后

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

DES安全性问题

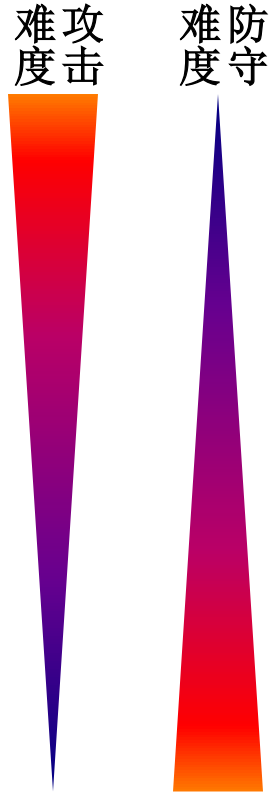
- 安全性问题：1999年，DES挑战赛被志愿者以22小时多一点儿的时间赢得
- 如何获得更高的安全性？
  - 使用三重DES
  - 使用AES

AES:高级加密标准

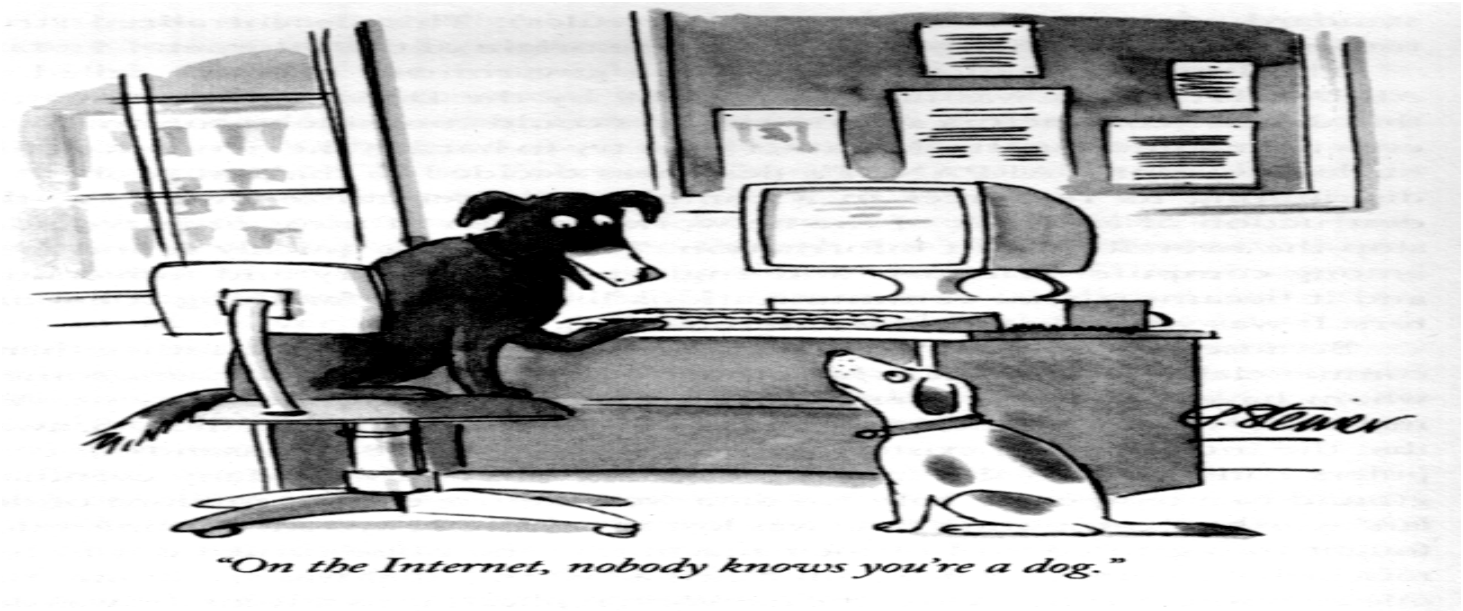
- 2001年11月，NIST选择了Rijndael作为DES的后继算法高级加密标准AES
- 其数据块及密钥的长度都可以分别是128比特、192比特和256比特的密钥加密

密码分析的基本类型

攻击类型	密码分析员的资源
唯密文攻击	加密算法 待分析密文
已知明文攻击	加密算法 待分析密文 用同一密钥加密的一个或多个明文－密文对
选择密文攻击	加密算法 待分析密文 密码分析员可选择特定密文，并获得对应的明文
选择明文攻击	加密算法 待分析密文 密码分析员可选择特定明文，并获得对应的密文
选择文本攻击	加密算法 待分析密文 密码分析员可选择特定密文，并获得对应的明文 密码分析员可选择特定明文，并获得对应的密文



Who are you?



网络中，我如何能相信你

传统的对称密钥体制的弱点

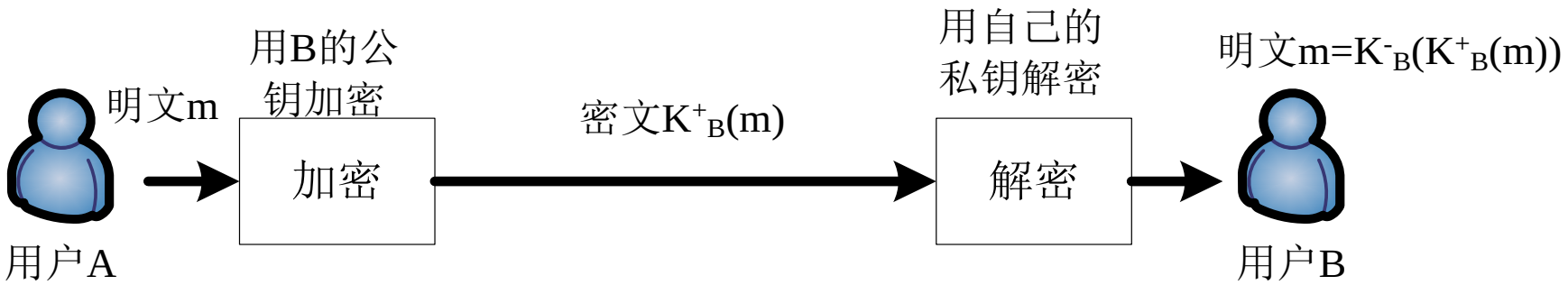
- 密钥管理
  - 如何安全的共享秘密密钥
  - 每对通信者间都需要一个不同的密钥。n个人通信需要n(n−1)/2个密钥。
  - 不可能与你未曾谋面的人加密通信
- 没有解决抵赖问题
  - 文档不能被签名
  - 通信双方都可以否认发送或接收过的信息

公钥密码体制

- 产生原因
  - 对称密码体制的密钥分配问题
  - 对数字签名的需求
- 公钥密码体制
  - 公钥K^+
  - 私钥K^-
  - 加密和解密的运算可以互逆，即
    - $K^-(K^+(m)) = K^+(K^-(m)) = m$
- 算法公开
- 无密钥传输的保密通信成为可能

公钥加密与私钥解密

- K_B^+和K_B^-分别表示用户B的公钥和私钥



公钥标准RSA

- 基于数论的非对称 (公钥) 密码体制
- RSA算法 发明者：Ron Rivest、Adi Shamir 和 Leonard Adleman

RSA公开密钥算法的发明人
（从左到右Ron Rivest, Adi Shamir, Leonard Adleman. 照片摄于1978年）

对RSA的攻击方法

1. 能否从公钥PK={e,n}推出秘密密钥SK={d,n}？

$ed = 1 \bmod \phi(n)$ ⟶ 需要 $\phi(n)$ ？

$\Phi(n) = (p-1)(q-1)$ ⟶ 需要p, q?

p, q ⟶ 需要分解n

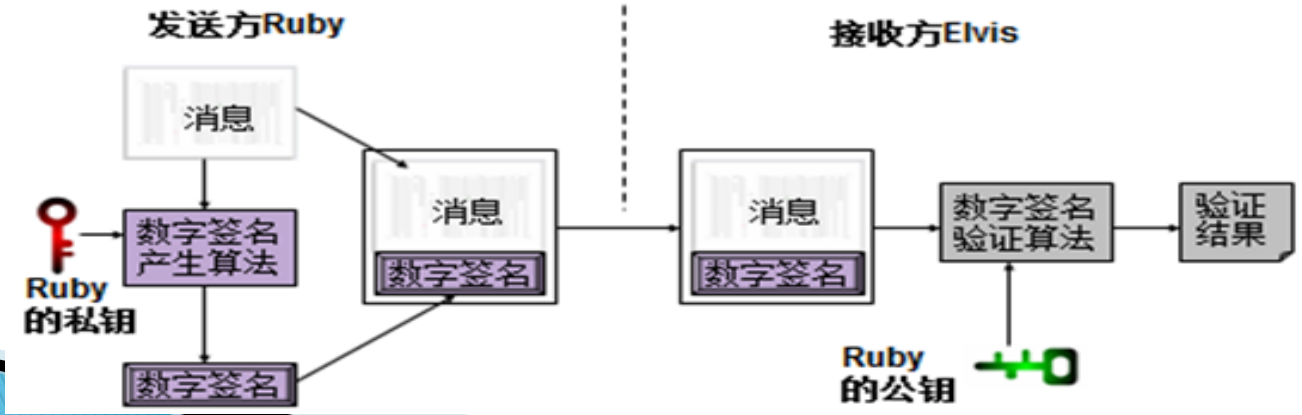
整数n的十进制位数	因子分解的运算次数	所需计算时间（每微秒一次）
50	1.4×10^{10}	3.9小时
75	9.0×10^{12}	104天
100	2.3×10^{15}	74年
200	1.2×10^{23}	3.8×10^{9}年
300	1.5×10^{29}	4.0×10^{15}年
500	1.3×10^{39}	4.2×10^{25}年

Hash函数

- 散列函数对任意长度报文M，产生定长的散列码h=H(M)，亦称作报文摘要Message Digest
- 散列函数算法
  - MD5 (Ronald Rivest，1992)
  - SHA-1 (NIST，1993)
  - 其他优秀的散列算法

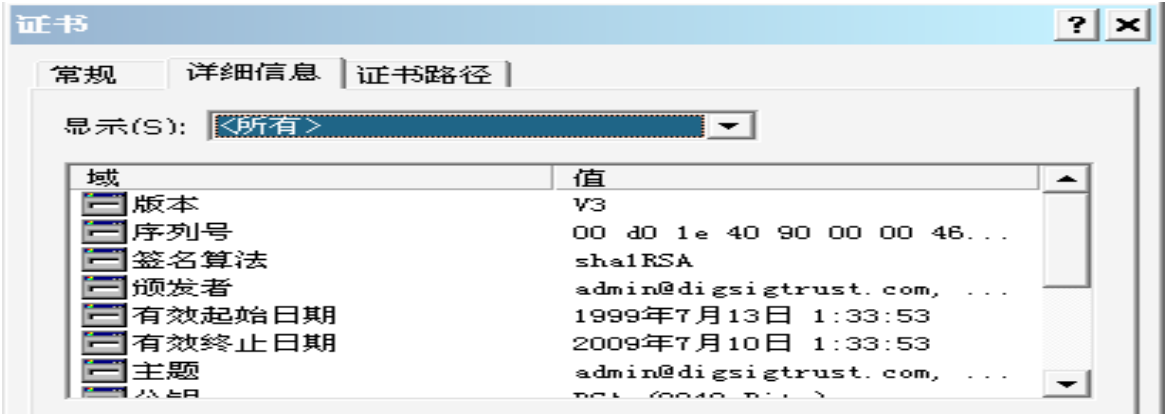
数字签名简介

- 数字签名： Ⅰ必须能够证明由某个人在一个文档上的签名确实是由该人签署的 (签名具有可鉴别性)， Ⅱ能证明只有那个人签署了那个文件 (签名具有不可伪造性、不可否认性)。
- 通常，使用公钥技术来实现数字签名。



数字证书

- 证书是由权威的、公正的认证机构来颁发和管理的。
- 一个典型的证书示例



数字证书的使用

证书授权中心（CA，Certificate Authority ）

数字证书

公开密钥2
名称2

数字证书

公开密钥1
名称1

公钥1加密

信息

私钥2签名

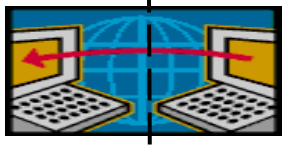
私钥1解密

信息

公钥2验证签名

客户

商家



？

私钥2解密

信息

公钥1验证签名

如何保证双方信息安全

公钥2加密

信息

私钥1签名

密码体制小结

- 对称密码体制
  - 古典对称密码体制
    - 代换密码（替代密码）
    - 置换密码
  - 现代对称密码体制
    - 数据加密标准DES
    - 高级加密算法AES
    - …
- 公钥密码体制
  - 公钥标准RSA
  - …
- 散列函数

对抗各种威胁

增强信息系统的物理安全。

自然威胁

防止对信息的非法攻击（主动攻击和被动攻击）。

通信传输威胁、存储攻击威胁

主动攻击和被动攻击

主动攻击

通过伪造、篡改或中断等技术改变原始消息来进行攻击的。

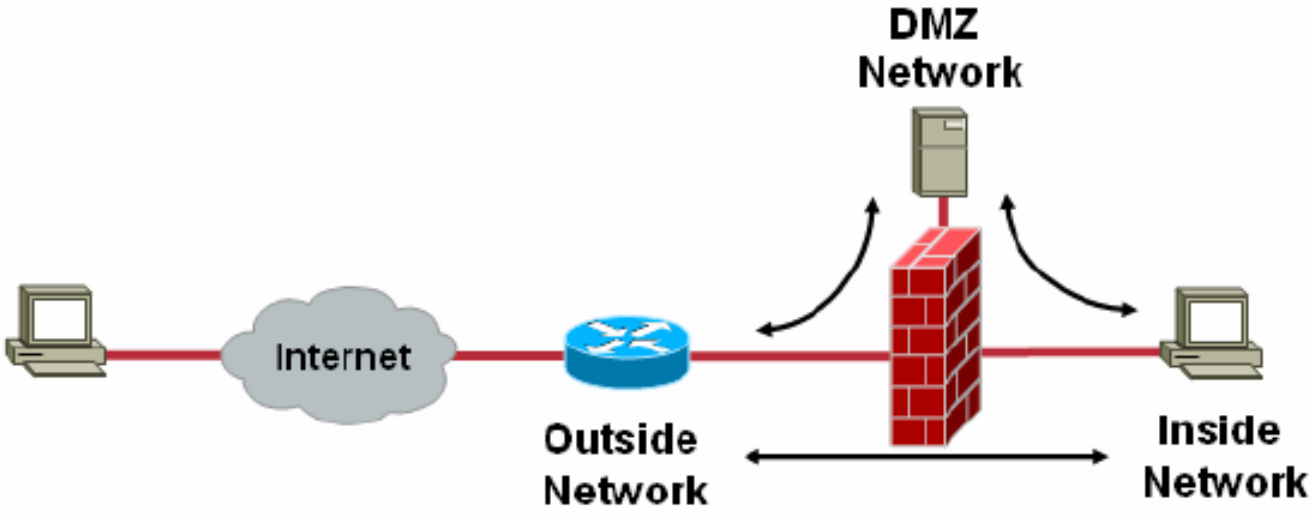
对抗主动攻击的常用技术有：认证、访问控制与入侵检测等。

被动攻击

通过窃取的方法，如：在网上截获消息等方法，非法获得信息。

被动攻击通常不改变消息而很难检测到，因此往往采用加密技术来对抗被动攻击，保护信息安全。

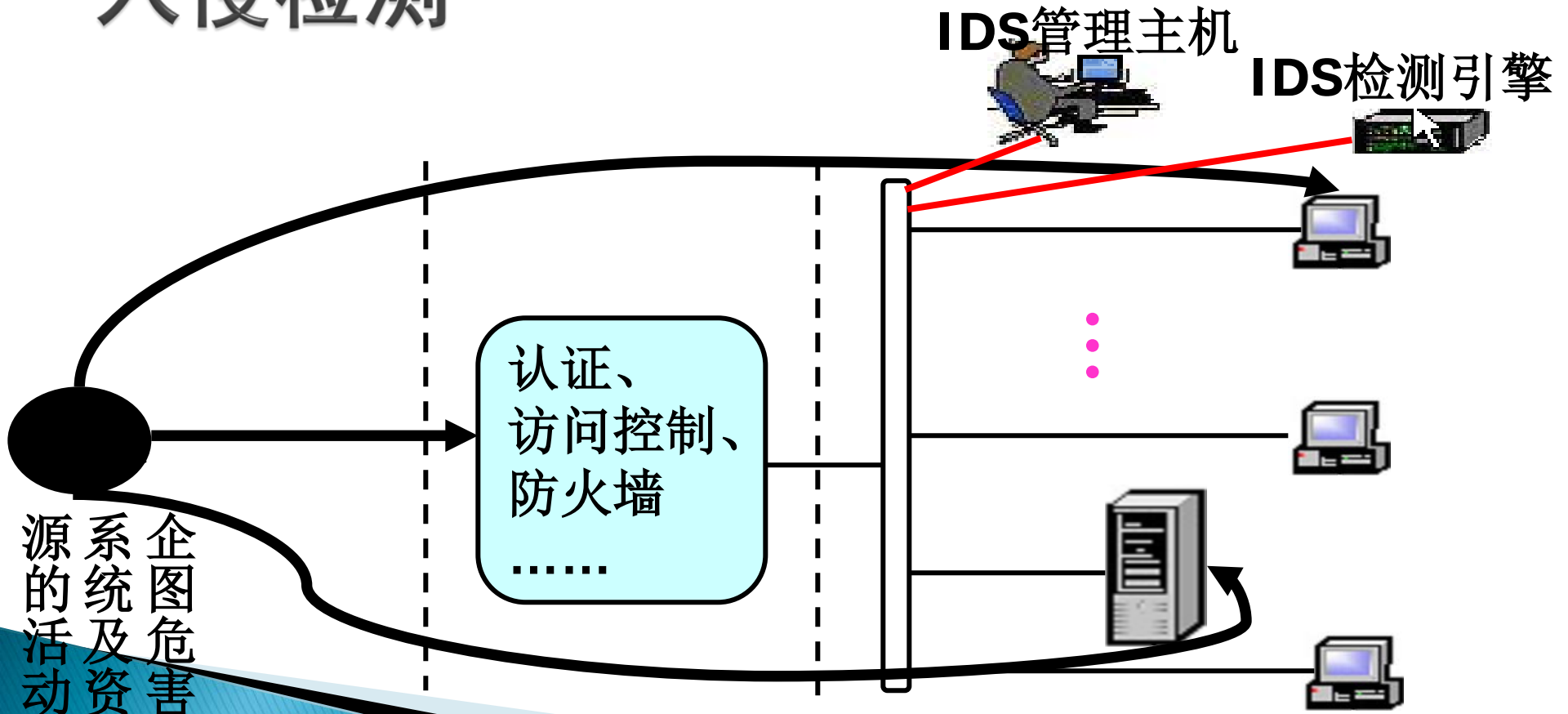
防火墙



黑客

- 黑客的含义
  - 利用计算机技术非法闯入到其它计算机或系统的人。
- 常用的黑客攻击方法
  - 端口扫描
  - 网络窃听
  - 拒绝服务
  - TCP/IP劫持

入侵检测



入侵检测系统不是万能的，也存在许多不足

- 不能在没有用户参与的情况下对攻击行为展开调查；
- 不能克服网络协议方面的缺陷；
- 不能克服设计原理方面的缺陷；
- 入侵检测系统可以检测到全部入侵行为吗？
  - 存在漏报与误报。

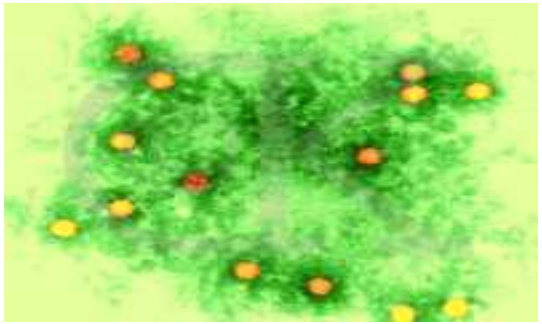
安全审计

- 怎样发现成功突破入侵检测系统的入侵行为？
  - 安全审计
    - 对与安全有关的活动及相关信息进行识别、记录、存储和分析。
    - 审计的记录用于检查网络上发生了哪些与安全有关的活动，谁（哪个用户）对这个活动负责。

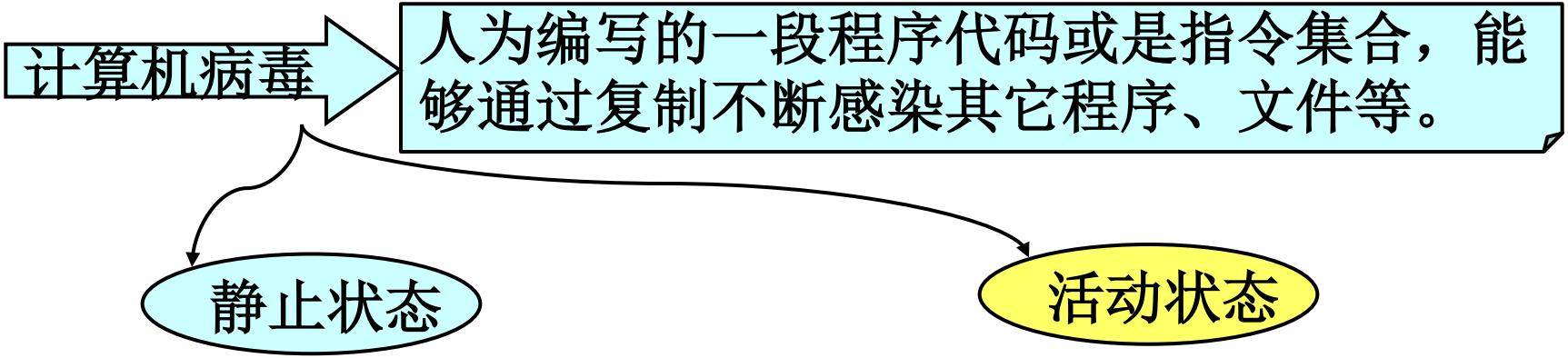
计算机病毒

计算机病毒

生物病毒



计算机病毒（续）



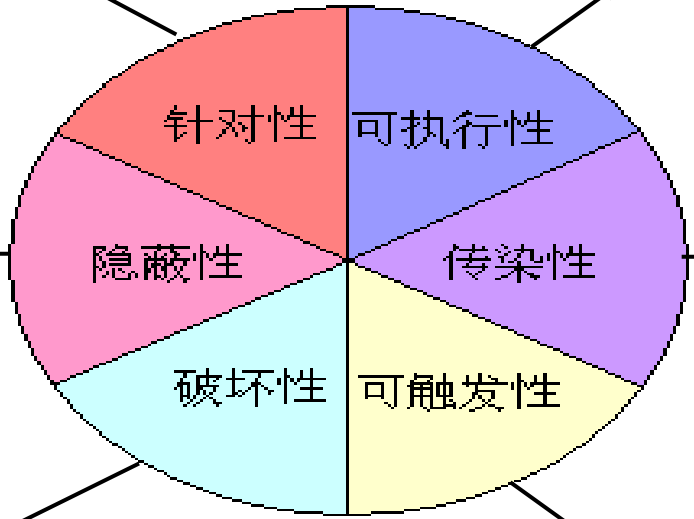
存在于外部存储介质，不具有传染和破坏能力。

被加载到内存后，此时如果病毒获得系统控制权就可以破坏系统或是传播病毒。

计算机病毒的特性

计算机病毒是针对特定的操作系统的。

计算机病毒执行的关键是获得系统的控制权。



计算机病毒是一段寄生在其它程序上的可执行程序，具有很强的隐蔽性。

计算机病毒只有运行时，才具有传染性。

取决于病毒开发者的本意。

病毒满足触发条件时发作。

计算机病毒的分类

- 计算机病毒的分类方法很多。
- 按照寄生方式分类
- 按照病毒的传播途径分类
- 按照破坏性分类
- 几种常见的病毒

计算机病毒的防范

- 计算机应定期安装系统补丁、安装有效的杀毒软件并根据实际需求进行安全设置。同时，定期升级杀毒软件并经常查毒、杀毒。
- 未经检测过是否感染病毒的文件、软盘、光盘及优盘等移动存储设备在使用前应首先用杀毒软件查毒后再使用。
- 尽量使用具有查毒功能的电子邮箱，尽量不要打开陌生的可疑邮件。
- 浏览网页、下载文件时要选择正规的网站。
- 关注目前流行病毒的感染途径、发作形式及防范方法，做到预先防范、感染后及时查毒，避免遭受更大损失。

本章小结

- 信息安全的有关概念，建立信息安全的整体框架
- 密码学
  - 密码编码学和密码分析学
  - 对称加密技术和非对称加密技术（公钥加密）
- 网络安全技术
- 计算机病毒的原理、特性与分类。