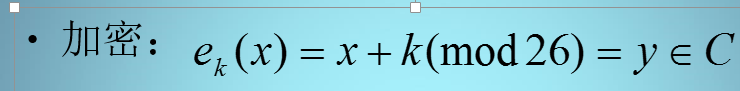
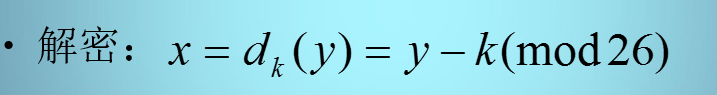
# 古典密码

代替

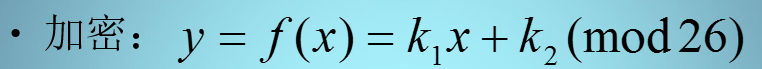
单表：

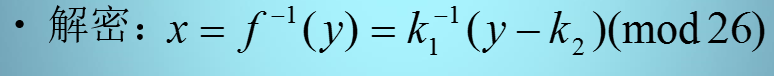
## 凯撒密码

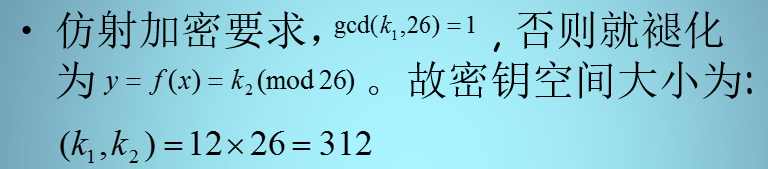




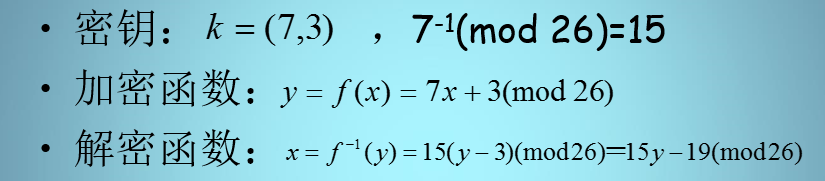
仿射加密







例子：



7\*15 mod 26 =1

多表：

Palyfir 双字母

Hill 字母数组\*矩阵密钥

## 维吉尼亚

换位：



密钥干什么用的?

# 现代密码

现代密码学对加密算法要求：

（1）必须提供高度的安全性；

（2）具有相当高的复杂性，使得破译的开销超过可能获得的利益，同时又便于理解和掌握；

（3）安全性应不依赖于算法的保密，其加密的安全性仅以加密密钥的保密为基础；

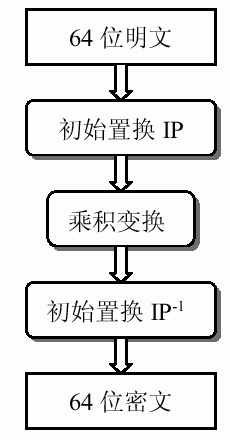
（4）必须适用于不同的用户和不同的场合；

（5）实现算法的电子器件必须很经济、运行有效；

（6）必须能够验证。

## 对称加密

### DES的加密处理略图



3DES

优点：

密钥长度增加到112位或168位，可以有效克服穷举搜索攻击；

相对于DES，增强了抗差分分析和线性分析的能力；

具备继续使用现有的DES实现的可能。

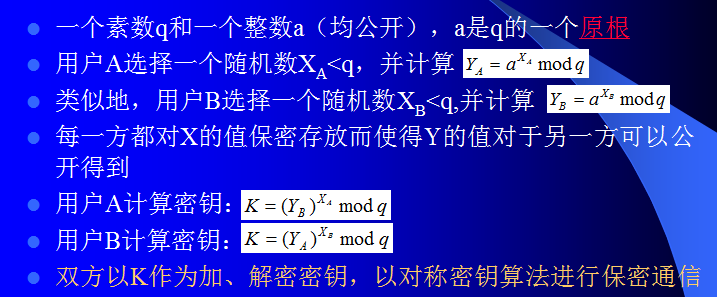
缺点：

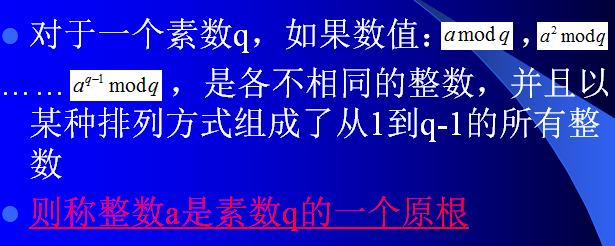
处理速度相对较慢，特别是对于软件实现。

明文分组的长度仍为64位，就效率和安全性而言，与密钥的增长不相匹配。

## 公钥算法

### Diffie-Hellman密钥交换算法







### RSA

明文空间P＝密文空间C=Zn

密钥的生成

选择互异素数p,q，则n=p\*q,ⱷ(n)=(p-1)(q-1), 选择整数e使(ⱷ(n),e)=1,1<e<ⱷ(n),计算d,使d=e-1mod ⱷ (n)

公钥Pk={e,n}

私钥Sk={d,n}

加密 (用e,n)

明文：M<n 密文：C=Me(mod n)

解密 (用d,n)

密文：C 明文：M=Cd（mod n)

Bob寻找出两个大素数p和q

Bob计算出n=pq和 ⱷ (n)=(p-1)(q-1).

Bob选择一个随机数e(0<e< ⱷ (n))，满足（e，ⱷ (n)）＝1

Bob使用辗转相除法计算d=e-1(mod ⱷ (n))

Bob在目录中公开n和e作为她的公开钥

RSA算法归纳

选择两个大素数p和q，通常要求每个均大于10100。

1.计算n＝pｘq和z＝(p－1)(q－1)。

2.选择一与z互素的数，令其为d 。

3.找到一个e满足e×d＝1 (mod z)。

选好这些参数后，将明文划分成块，使得每个明文报文P长度m满足0<m<n。加密P时，计算C＝Pe(mod n)，解密C时计算P＝Cd(mod n)。由于模运算的对称性，可以证明，

在确定的范围内，加密和解密函数是互逆的。

为实现加密，需要公开(e, n)，为实现解密需要(d, n)。

安全性：密码分析者攻击RSA体制的关键点在于如何分解n。若分解成功使n=pq，则可以算出φ(n)＝（p-1)(q-1)，然后由公开的e，解出秘密的d。

**RSA在使用时达到安全效果要求**：若使RSA安全，p与q必为足够大的素数，使分析者没有办法在有效时间内将n分解出来。建议选择p和q大约是100位的十进制素数。 模n的长度要求至少是512比特。

为了抵抗现有的整数分解算法，对RSA模n的素因子

p和q还有如下要求：

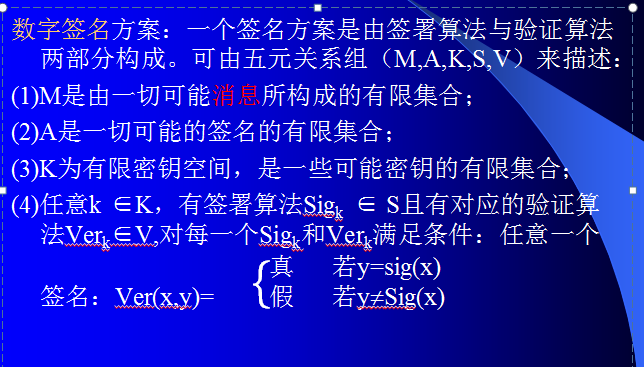
(1)|p-q|很小，通常 p和q的长度相同或仅相差几位；

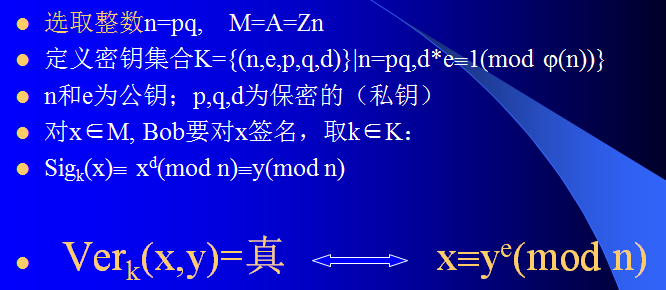
(2)p-1 和q-1分别含有大素因子p1和q1

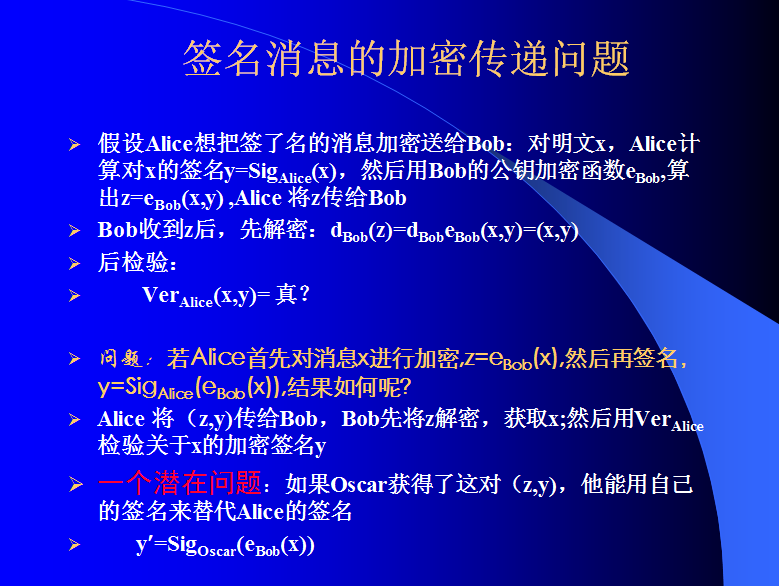
(3)gcd(p-1,q-1)应该很小。

　　　为了提高加密速度，通常取e为特定的小整数，如EDI国际标准中规定 e＝216＋1，ISO/IEC9796中甚至允许取e＝3。这时加密速度一般比解密速度快10倍以上。

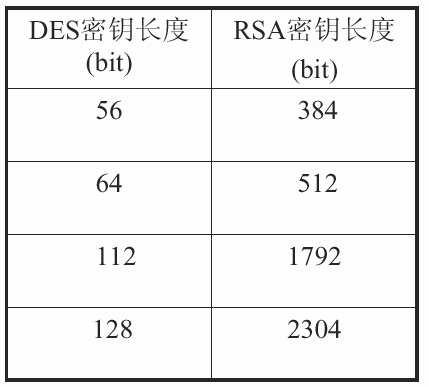
#### RSA的数字签名应用







DES和RSA性能比较（同等强度）



### 哈希函数

Hash算法是把任意长度的输入数据经过算法压缩，输出一个尺寸小了很多的固定长度的数据，即哈希值。哈希值也称为输入数据的数字指纹（Digital Fingerprint）或消息摘要（Message Digest）等。Hash函数具备以下的性质：

　　1、给定输入数据，很容易计算出它的哈希值；

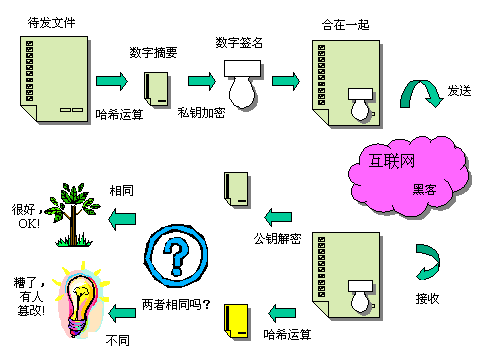
　　2、反过来，给定哈希值，倒推出输入数据则很难，计算上不可行。这就是哈希函数的单向性，在技术上称为抗原像攻击性；

　　3、给定哈希值，想要找出能够产生同样的哈希值的两个不同的输入数据，（这种情况称为碰撞，Collision），这很难，计算上不可行，在技术上称为抗碰撞攻击性；

4、哈希值不表达任何关于输入数据的信息。

发信者在发信前使用哈希算法求出待发信息的数字摘要，然后用私钥对这个数字摘要，而不是待发信息本身，进行加密而形成一段信息，这段信息称为数字签名。发信时将这个数字签名信息附在待发信息后面，一起发送过去。收信者收到信息后，一方面用发信者的公钥对数字签名解密，得到一个摘要H；另一方面把收到的信息本身用哈希算法求出另一个摘要H’，再把H和H’相比较，看看两者是否相同。根据哈希函数的特性，我们可以让简短的摘要来“代表”信息本身，如果两个摘要H和H’完全符合，证明信息是完整的；如果不符合，就说明信息被人篡改了。

由于摘要一般只有128位或160位比特，比信息本身要短许多倍，USB Key或IC卡中的微处理器对摘要进行加密就变得很容易，数字签名的过程一般在一秒钟内即可完成。



<http://www.cfca.com.cn/20150811/101230821.html>

## 序列密码：

具有实现简单、便于硬件实现、加解密处理速度快、没有或只有有限的错误传播等特点

特点：

同步流密码：

同步要求，无错误传播 ，如果密钥流为无限随机序列，则成为一次一密

自同步流密码：

自同步，有限的错误传播

### 流密码和分组密码

流密码的优点:转换速度快，低错误传播

流密码的缺点:低扩散，有意插入及修改的不敏感性

分组密码的优点:扩散性，插入的敏感性

分组密码的缺点:加密速度慢，错误传播

### 密钥的分发

是保密通信中的一方生成并选择秘密密钥，然后把该密钥发送给通信参与的其他一方或多方的机制

密钥分发协议：

分类：网外分发、网内分发

　　　　秘密密钥的分发、公开密钥的分发

1. 秘密密钥的分发

用一个密钥加密密钥加密多个会话密钥

使用密钥分发中心

1. 公开密钥的分发

公钥的公开发布

建立公钥目录

带认证的公钥分发（在线服务器方式）

使用数字证书的分钥分发（离线服务器方式）

# 模运算

估计结合rsa一类的

带余除法：  
a∈z,>0，可找出两个唯一确定的整数q和r,  
使a=qm+r, 0<=r< m,q和r这两个数分别称为以m去除a所得到的商数和余数。 (若r=0则m∣a）

整数同余：

定义：如果a mod m =b mod m，则称整数a模正整数m同余于整数b，并写a≡b（mod m）是指m∣（a－b）, m称为模数。  
注：1\*.m∣a-ba=q1m+r,b=q2m+r即a和b分别 除以m有相同的余数。“同余”二字的来源就在于此。

2\*.相对于某个固定模数m的同余关系，是整数间的一种等价关系。具有等价关系的三点基本性质：

自反性：对任意整数a有：a≡a（mod m）

对称性：如果a≡b(mod m)，则b≡a（mod m）

传递性：如果a≡b (mod m）b≡c（mod m），则a≡c(mod m)

于是，全体整数集合z可按模m（m>1）分成一些两两不交的等价类。

3\*. 对于某个固定模m的同余式可以象普通的等式那样相加、相减和相乘，可结合：

(1)[a(mod m)±b(mod m)]mod m=(a±b)(mod m)

(2)[a(mod m)\*b(mod m)]mod m=(a\*b)(mod m)

(3)[(a\*b)modm+(a\*c)modm]=[a\*(b+c)]modm

例子.通过同余式演算证明：

（1）560－1是56的倍数

（2）223－1是47的倍数。

解：

注意53=125≡13(mod56)

于是有56≡169≡1(mod56)

对同余式的两边同时升到10次幂，

即有56∣560-1。

定理：(消去律)对于ab≡ac（mod m）来说，若gcd(a,m)＝1则b≡c(mod m)

# 安全专题

## 物理安全技术

1.物理安全又叫实体安全（Physical Security），是保护计算机设备、设施（网络及通信线路）免遭地震、水灾、火灾、有害气体和其他环境事故（如电磁污染等）破坏的措施和过程。

实体安全技术主要是指对计算机及网络系统的环境、场地、设备和通信线路等采取的安全技术措施

2. 影响物理安全的因素

1）计算机及其网络系统自身存在的脆弱性因素。

2）各种自然灾害导致的安全问题。

3）由于人为的错误操作及各种计算机犯罪导致的安全问题。

3. 物理安全包括：环境安全、电源系统安全、设备安全和通信线路安全。

1)环境安全：应具备消防报警、安全照明、不间断供电、温湿度控制系统和防盗报警。

2)电源系统安全：电源安全主要包括电力能源供应、输电线路安全、保持电源的稳定性等。

3)设备安全：要保证硬件设备随时处于良好的工作状态，建立健全使用管理规章制度，建立设备运行日志。同时要注意保护存储媒体的安全性，包括存储媒体自身和数据的安全。

4)通信线路安全：包括防止电磁信息的泄漏、线路截获，以及抗电磁干扰。

4.物理安全包括以下主要内容:

1）计算机机房的场地、环境及各种因素对计算机设备的影响。

2）计算机机房的安全技术要求。

3）计算机的实体访问控制。

4）计算机设备及场地的防火与防水。

5）计算机系统的静电防护。

6）计算机设备及软件、数据的防盗防破坏措施。

7）计算机中重要信息的磁介质的处理、存储和处理手续的有关问题。

5.环境安全

安全保卫技术是环境安全技术的重要一环，主要的安全技术措施包括：防盗报警、实时监控、安全门禁等。

计算机机房的温度、湿度等环境条件保持技术可以通过加装通风设备、排烟设备、专业空调设备来实现。

计算机机房的用电安全技术主要包括不同用途电源分离技术、电源和设备有效接地技术、电源过载保护技术和防雷击技术等。

计算机机房安全管理技术是指制定严格的计算机机房工作管理制度，并要求所有入机房的人员严格遵守管理制度，将制度落到实处。

6. 计算机网络系统设备安全应采取的主要手段有计算机网络系统设备的安全管理和维护、信息存储媒体的管理和计算机网络系统设备的电磁兼容技术。通信线路安全主要注重介绍加压电缆和光纤等通信线路的防窃听技术。

## 专题2数据链路层安全

1.计算机网络通信线路屏蔽

屏蔽：

用金属网或金属板将信号源包围，利用金属层来阻止内部信号向外发射，同时也可以阻止外部信号进入金属层内部。

通信线路的屏蔽：

采用屏蔽性能好的传输介质

把传输介质、网络设备、机房等整个通信线路安装在屏蔽的环境中

2.物理线路隔离

物理隔离的指导思想与防火墙绝然不同：防火墙的思路是在保障互联互通的前提下，尽可能安全，而物理隔离的思路是在保证必须安全的前提下，尽可能互联互通。

主要物理隔离产品：

物理隔离卡

物理隔离集线器/交换机

物理隔离网闸

案例：电子政务

一般划分为3个安全等级不同的部分

内部保密专用网络，传送保密信息

业务网络，传送政府业务管理信息

Internet连接网络，建设网站或对外访问

保密网络要求跟其它部分物理隔离

其它部分可以在保证安全性情况下互连

案例：证劵交易网

一般划分为3个安全等级不同的部分

证券交易业务专用网络，传送证券业务信息

企业内综合管理网络，传送办公、财务、VoIP等企业内部管理信息

Internet连接网络，建设网站或对外访问

交易网络首先要保证可靠性和安全性，跟其它部分物理隔离，必要时可以采用逻辑隔离方式连接

其它可以在保证安全性情况下互连

未完待续

## 专题三 防火墙技术

1.定义：

防火墙是位于两个或多个网络之间，执行访问控制策略的一个或一组系统，是一类防范措施的总称 .

一个好的防火墙具备:

内部和外部之间的所有网络数据流必须经过防火墙

只有符合安全政策的数据流才能通过防火墙

防火墙自身应对渗透免疫

2.控制能力

服务控制，确定哪些服务可以被访问

方向控制，对于特定的服务，可以确定允许哪个方向能够通过防火墙

用户控制，根据用户来控制对服务的访问

行为控制，控制一个特定的服务的行为

3.作用

防火墙对企业内部网实现了集中的安全管理

防火墙能防止非授权用户进入内部网络。

防火墙可以方便地监视网络的安全性并报警。

可以作为部署网络地址转换NAT的地点

可以实现重点网段的分离

防火墙是审计和记录网络的访问和使用的最佳地方。

4.局限性

限制或关闭了一些有用但存在安全缺陷的网络服务，给用户带来使用的不便。

目前防火墙对于来自网络内部的攻击还无能为力。

防火墙不能防范不经过防火墙的攻击。

可能带来传输延迟、瓶颈及单点失效。

防火墙不能有效地防范数据驱动式攻击。

作为一种被动的防护手段，防火墙不能防范因特网上不断出现的新的威胁和攻击。

5.安全策略

在构筑防火墙之前，需要制定一套完整有效的安全策略

网络服务访问策略

一种高层次的具体到事件的策略，主要用于定义在网络中允许或禁止的服务。

防火墙设计策略

一切未被允许的就是禁止的

一切未被禁止的都是允许的

6. 包过滤防火墙

往往用一台路由器来实现

基本的思想很简单

对所接收的每个数据包进行检查，根据过滤规则，然后决定转发或者丢弃该包

往往配置成双向的

如何过滤

过滤规则基于IP报头信息。IP源地址、目的地址、TCP/UDP端口、ICMP消息类型、TCP头中的ACK位。

过滤器往往建立一组规则，根据IP包是否匹配规则中指定的条件来作出决定。

如果有匹配按规则执行，没有匹配，则按缺省策略。

重要规定：

访问规则要使用IP地址，而不使用主机名或域名

不要回应所有经过外部网络接口来的ICMP包。

要丢弃所有通过外部网络适配器流入，且其源地址是来自受保护网络的包。

7. 其他防火墙技术

网络地址转换

热恢复策略

流量控制

IP和MAC绑定

身份鉴别

负载均衡

内容安全

加密

审计

防火墙的免疫设计

分布式防火墙

8.防火墙的发展趋势

高速

应用ASIC、FPGA和网络处理器是实现高速防火墙的主要方法，算法也是关键。

多功能化

比如NAT、VPN(IPSec)、IDS，以及一些鉴别和访问控制技术

安全

防火墙自身的安全性和稳定性

## 专题4 入侵检测系统

1. 黑客攻击策略

入侵步骤：

信息获取实施攻击掩盖痕迹，预留后门

入侵造成的破坏：

保密性、完整性、可用性、可控性、

2. 入侵检测的方式：

被动、非在线地发现

主动、在线地发现

3. 入侵检测系统必须具备的特点：

经济性

时效性

安全性

可扩展性

4. 通用入侵检测系统流程图：

5. 入侵检测系统的主要功能有：

　　●监测并分析用户和系统的活动；

　　●核查系统配置和漏洞；

　　●评估系统关键资源和数据文件的完整性；

　　●识别已知的攻击行为；

　　●统计分析异常行为；

●操作系统日志管理，并识别违反安全策略的用户活动。

6.异常检测原理：根据非正常行为和使用计算机资源非正常情况检测出入侵行为。

7. 误用检测原理：根据已经知道的入侵方式来检测入侵。

8. 入侵检测系统的分类

按数据源和系统结构：

(1) 基于网络的入侵检测系统(NIDS)

(2) 基于主机的入侵检测系统(HIDS)

(3) 分布式入侵检测系统(DIDS)

按数据分析方法：

(1) 异常检测模型

(2) 误用检测模型

按数据分析发生的时效：

(1) 离线检测系统

(2) 在线检测系统

按系统模块运行分布方式：

(1) 集中式检测系统

(2) 分布式检测系统

9. 入侵响应

当检测到入侵或攻击时,采取适当的措施阻止入侵和攻击的进行.

针对入侵的建议步骤:

●估计形势并决定需要做出那些响应.

●如有必要就断开连接或关闭资源.

●事故分析和响应.

●根据响应策略向其他人报警.

●保存系统状态.

●恢复遭到攻击的系统.

●记录所发生的一切.

10. 现代安全审计技术

安全审计现状

目前的安全审计类产品：

(1) 网络设备及防火墙日志

(2) 操作系统日志

(3) Sniff、Snoop类工具

## 专题5邮件系统安全

反垃圾邮件技术：

1.垃圾邮件:

(1)收件人无法拒收的电子邮件;

(2)收件人事先没有提出要求或同意接收的宣传性质的邮件;

(3)含有不良或有害信息的邮件;

(4)隐藏发件人身份、地址、标题等信息的邮件;

(5)含有虚假的信息源、发件人、路由等信息的电子邮件;

2. 邮件过滤技术:

(1)黑名单

(2)白名单

(3)简单的关键字过滤

(4)简单的DNS测试

(5)实时黑名单

(6)指纹识别技术

(7)基于规则的过滤技术

(8)贝叶斯过滤技术

(9)分布式适应性黑名单

3. SMTP协议的改进:

(1)反向查询

(2)SenderID检查技术

(3)DKIM技术

(4)FairUCE技术

(5)密码技术

4. 邮件服务器的安全管理:

(1)SMTP身份认证(ip spoofing)

(2)病毒过滤

(3)安全审计

5. 邮件客户端的安全管理:

(1)邮件客户端的选择

(2)邮件客户端的使用

## 专题7 DNS

1.DNS服务的安全性

DDoS隐患

缺省设置: 一个域名服务器允许远程主机向它查询其他域(它本身并不管理这些域)的域名，即允许递归查询.

2. 利用递归查询实施DDoS攻击

建议:禁止来自其它主机的递归查询，只允许从信任主机或网络查询，避免成为攻击的工具。

3. FTP服务的安全性

帐户管理(匿名)

权限管理(下载/上传)

主动模式/被动模式与防火墙规则

●主动：客户端从一个任意的非特权端口N(N>=1024)连接到FTP服务器的命令端口21; 客户端开始监听端口N1，并发送FTP命令“port N1”到FTP服务器。服务器从它自己的数据端口(20)连接到客户端指定的数据端口N1。

●被动：开启一个FTP连接时，客户端打开两个任意的非特权本地端口(N>=1024和N1)。第一个端口连接服务器的21端口，但与主动方式的FTP不同，客户端不会提交PORT命令并允许服务器来回连它的数据端口，而是提交PASV命令。这样做的结果是服务器会开启一个任意的非特权端口(P>=1024)，并发送PORT P命令给客户端。然后客户端发起从本地端口N1到服务器的端口P的连接用来传送数据。

4. telnet服务的安全性

用途

安全隐患(监听演示)

SSH

5. Ipv6及其安全性

ipv6的特点

Ipv6的部署情况

Ipv6的安全特性

## 专题8 病毒

1.发作前，发作时，发作后的表现

2.特征：

传染性，寄生性，隐蔽性，潜伏性，破坏性，触发性

3. 蠕虫病毒与一般病毒的异同



4.蠕虫特点：利用操作系统和应用程序的漏洞主动进行攻击。此类病毒主要是“红色代码”和“尼姆达”，以及至今依然肆虐的”求职信”等

传播方式多样。如“尼姆达”病毒和”求职信”病毒，可利用的传播途径包括文件、电子邮件、Web服务器、网络共享等等.

5.防范蠕虫病毒措施

需要考虑几个问题：

病毒的查杀能力

病毒的监控能力

新病毒的反应能力

a.对于局域网而言，可以采用以下一些主要手段：

在因特网接入口处安装防火墙或防杀计算机病毒产品，将病毒隔离在局域网之外。

对邮件服务器进行监控，防止带毒邮件进行传播。

对局域网用户进行安全培训。

建立局域网内部的升级系统，包括各种操作系统的补丁升级，各种常用的应用软件升级，各种杀毒软件病毒库的升级等等。

b.对于个人用户而言，威胁大的蠕虫病毒采取的传播方式一般为电子邮件(Email)以及恶意网页等等。

对于利用email传播得蠕虫病毒来说，通常利用的是社会工程学(Social Engineering)，即以各种各样的欺骗手段那诱惑用户点击的方式进行传播。

恶意网页确切的讲是一段黑客破坏代码程序，它内嵌在网页中，当用户在不知情的情况下打开含有病毒的网页时，病毒就会发作。

网络蠕虫病毒对个人用户的攻击主要还是通过社会工程学，而不是利用系统漏洞。所以防范此类病毒需要注意以下几点

购买合适的杀毒软件

经常升级病毒库

提高防杀毒意识，不要轻易去点击陌生的站点，有可能里面就含有恶意代码。

不随意查看陌生邮件，尤其是带有附件的邮件

6. 宏病毒的特点：

以数据文件方式传播，隐蔽性好，传播速度快，难于杀除

制作宏病毒以及在原型病毒上变种非常方便

破坏可能性极大

宏病毒会感染DOC文档文件和DOT模板文件

7.处理方法

1、首选方法：用最新版的反病毒软件清除宏病毒。

2、应急处理方法：用写字板或WORD 6.0文档作为清除宏病毒的桥梁

8.脚本病毒

脚本病毒具有如下几个特点：

1．编写简单。

2．破坏力大。

3．感染力强。

4．传播范围大。

5．病毒源码容易被获取，变种多。

6．欺骗性强。

7．使得病毒生产机实现起来非常容易。

9. 邮件型病毒也是脚本病毒的一种，主要是通过利用 Outlook 的可编程特性来完成的

10。病毒检测  
1、比较法

2、加总比对法

3、搜索法

4、分析法

5、人工智能陷阱技术和宏病毒陷阱技术

6、软件仿真扫描法

7、先知扫描法

11.病毒防治

1、新购置的计算机硬软件系统的测试

2、计算机系统的启动

3、单台计算机系统的安全使用

4、重要数据文件要有备份

5、不要随便直接运行或直接打开电子函件中夹带的附件文件，不要随意下载软件，尤其是一些可执行文件和Office文档。

6、计算机网络的安全使用

（1）安装网络服务器时，应保证没有计算机病毒存在

（2）在安装网络服务器时，应将文件系统划分成多个文件卷系统，至少划分成操作系统卷、共享的应用程序卷和各个网络用户可以独占的用户数据卷。

（3）一定要用硬盘启动网络服务器，否则在受到引导型计算机病毒感染和破坏后，遭受损失的将不是一个人的机器，而会影响到整个网络的中枢。

（4）为各个卷分配不同的用户权限。

（5）在网络服务器上必须安装真正有效的防杀计算机病毒软件，并经常进行升级。

（6）系统管理员的职责

12计算机病毒感染后的一般修复处理方法：

1）首先必须对系统破坏程度有一个全面的了解，并根据破坏的程度来决定采用有效的计算机病毒清除方法和对策。

2）修复前，尽可能再次备份重要的数据文件。

3）启动防杀计算机病毒软件，并对整个硬盘进行扫描。

4）发现计算机病毒后，我们一般应利用防杀计算机病毒软件清除文件中的计算机病毒，如果可执行文件中的计算机病毒不能被清除，一般应将其删除，然后重新安装相应的应用程序。5）杀毒完成后，重启计算机，再次用防杀计算机病毒软件检查系统中是否还存在计算机病毒，并确定被感染破坏的数据确实被完全恢复。

6）此外，对于杀毒软件无法杀除的计算机病毒，还应将计算机病毒样本送交防杀计算机病毒软件厂商的研究中心，以供详细分析。

13计算机系统修复

计算机系统修复应急计划

1）人员准备

2）应急计划的实施步骤

3）善后工作

4）此外，在应急计划中还必需包括救援物质、计算机软硬件备件的准备，以及参加人员的联络表等，以便使得发生计算机病毒疫情后能够迅速地召集人手，备件到位，快速进入应急状态。

## 专题9 操作系统安全

1.操作系统的安全配置：

　操作系统访问权限的恰当设置

　操作系统的及时更新

　对外界攻击的防范

2. 操作系统安全性的设计方法及原则

　通用操作系统的安全性设计原则：

　隔离性

内核机制

分层结构