计算机网络信息安全

第一章 网络安全概述

一、 信息安全概述：

信息安全：研究信息获取、存储、传输以及处理领域的信息安全保障问题的一门新兴学科，是防止信息被非授权使用、误用、篡改和拒绝使用而采取的措施和手段。

信息安全是综合学科、包括：物理、生物、电子、通信、计算机、系统工程、语言学、统计学、心理学（蜜罐）、法律、管理、教育等学科演绎而成的交叉学科。

二、 信息安全研究层次

总体分为五个层次：安全的密码算法、安全协议、网络安全、系统安全、应用安全。密码安全是安全研究的关键点

三、 信息安全的常见威胁

信息安全的风险来自于以下方面：

1.物理因素：计算机本身和外部设备乃至网络和通信线路面临各种风险，如各种自然灾害、设备故障、电磁干扰、被盗等。

2.系统因素：组件的脆弱性和TCP/IP协议簇先天不足，各种未知的漏洞。

3.网络因素：各种类型的人为攻击

4.应用因素：内部操作不当，使用中的信息泄露。如：人为破坏、操作失误。

5.管理因素：没有完整的安全管理制度。单纯依靠安全设备。

四、 信息安全的目标

信息安全的**基本目标**应该是**保护信息的机密性、完整性、可用性、可控性和不可抵赖性。**

1.真实性：对信息的来源进行判断，能对伪造来源的信息予以鉴别。

2.保密性：保证机密信息不被窃听，或窃听者不能了解信息的真实含义。

3.完整性：保证数据的一致性，防止数据被非法用户篡改。

4.可用性：保证合法用户对信息和资源的使用不会被不正当地拒绝。

5.不可抵赖性：建立有效的责任机制，防止用户否认其行为，这一点在电子商务中是极其重要的。

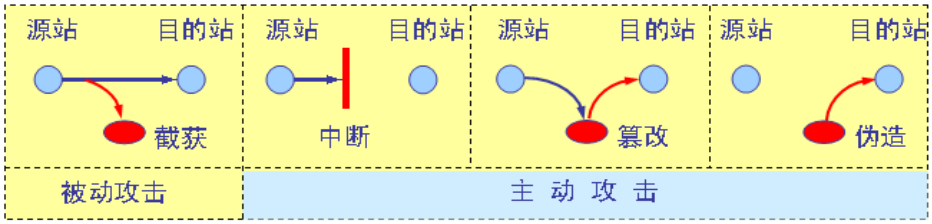
6.可控制性：对信息的传播及内容具有控制能力

五、 网络安全：网络安全是信息安全的重要分支

网络安全的定义：网络安全是指网络系统的硬件、软件及其系统中的数据的安全，它体现于网络信息的存储、传输和使用过程。

所谓的网络安全性就是网络系统的硬件、软件及其系统中的数据受到保护不会由于偶然的或者恶意的原因而遭到破坏、更改、泄露，系统连续、可靠、正常地运行，网络服务不中断

1．1 计算机网络上的通信面临以下的四种威胁：



(1) **截获**——从网络上窃听他人的通信内容。

(2) **中断**——有意中断他人在网络上的通信。

(3) **篡改**——故意篡改网络上传送的报文。

(4) **伪造**——伪造信息在网络上传送。

保证网络信息传输安全需要注意哪些问题

(1) **截获** (2) **中断** (3) **篡改** (4) **伪造**（5）**重发-----** 即攻击者截获网络上的密文信息后，并不将其破译，而是把这些数据包再次向有关服务器（如银行的交易服务器）发送，以实现恶意的目的。

截获信息的攻击是属于被动攻击，而更改信息和拒绝用户使用资源的攻击是属于主动攻击。

1.2 网络安全的攻防体系

- **攻击技术：**

1、 **网络监听：**监听目标主机的通讯。
2、 **网络扫描：**扫描目标主机的开放端口，目的是发现漏洞，为入侵做准备。
3、 **网络入侵：**非授权进入目标系统。
4、 **网络后门：**为实现长期控制，种植木马等后门程序。
5、 **网络隐身：**清除入侵留下的痕迹。

- **防卸技术：**

1、 **安全的操作系统和操作系统安全配置**
2、 **加密技术：**对数据加密
3、 **防火墙技术：**构建网络安全边界
4、 **入侵检测：**及时发现入侵，并作出反应

六、 可信计算机评价标准（了解）

- 我国，计算机信息系统安全保护等级划分

第一级：用户自主保护级（TCSEC 的 C1 级）：用户自己决定
第二级：系统审计保护级（TCSEC 的 C2 级）：按标记的安全级别限制使用者的访问权限
第三级：安全标记保护级（TCSEC 的 B1 级）：将安全保护分为关键和非关键，关键部分强制保护
第四级：结构化保护级（TCSEC 的 B2 级）：将安全保护分为关键和非关键，关键部分强制保护
第五级：访问验证保护级（TCSEC 的 B3 级）：增加了访问验证机制” 负责仲裁访问者对访问对象的所有访问活动。

- 美国,可信计算机标准评价准则（TCSEC）

TCSEC（习惯上称橘皮书）。TCSEC 将系统分成 ABCD 四类 7 个安全级别。但是一般上说是 4 级
D 级是安全级别最低的级别，C 类为自主保护级别；
B 类为强制保护级别；A 类为验证保护类
当前主流的操作系统安全性远远不够，**如 UNIX 系统，Windows NT 都只能达到 C2 级，**安全性均有待提高。
1、D 级，最低安全性；
2、C1 级，自主安全控制；
3、C2 级，受控存储控制；单独的可查性，安全标识。
4、B1 级，标识的安全保护；强制存取控制。安全标识
5、B2 级，良好的结构化设计；面向安全的体系结构、安全模型；
6、B3 级，安全区域；全面的访问控制、可信恢复；高抗渗透能力
7、A1 级，验证设计；符合形式化的最高级描述和认证。

例题：
TCSEC 系统把计算机安全的等级分为__4__级。

ok 判断：
1. 网络系统的安全性取决于网络系统中最薄弱的环节。
2. 审计是记录用户使用计算机网络系统进行所有活动的过程，它是提高安全性的重要工具。
3. 备份不仅在网络系统硬件故障或人为失误时起到保护作用，也在入侵者非授权访问或对网络攻击及破坏数据完整性时起到保护作用，同时亦是系统灾难恢复的前提之一。
4. 鉴别是对网络中的主体进行验证的过程，通常有三种方法验证主体身份，1、口令、密码 2、智能卡、令牌卡、3、只有该主体具有的独一无二的特征或能

力，如指纹、声音、视网膜或签字等。

5. 网络安全完整性方面的特征指数据未经授权不能进行改变的特性，即信息在存储或传输过程中保持不被修改、不被破坏和丢失的特性。
6. 拒绝服务攻击是指以非法手段窃得对数据的使用权，删除、修改、插入或重发某些重要信息，以取得有益于攻击者的响应；恶意添加，修改数据，以干扰用户的正常使用。

ok 简答：

1. 根据网络安全的定义，网络安全应具有哪些个方面的特征？

网络安全应具有保密性、完整性、可用性、可控性、可审查性、可保护性六个方面的特征。

2. 什么是拒绝服务攻击？

拒绝服务攻击是指不断对网络服务系统进行干扰，改变其正常的作业流程，执行无关程序使系统响应减慢甚至瘫痪，影响正常用户的使用，甚至使合法用户被排斥而不能进入计算机网络系统或不能得到相应的服务。

3. 什么是信息重发的攻击方式？

信息重发的攻击方式，即攻击者截获网络上的密文信息后，并不将其破译，而是把这些数据包再次向有关服务器（如银行的交易服务器）发送，以实现恶意的目的。

4. 为确保网络信息的传输安全，尤其需要防止如下 5 个问题。

（1）截获

对网上传输的信息，攻击者只需在网络的传输链路上通过物理或逻辑的手段，就能对数据进行非法的截获（Interception）与监听，进而得到用户或服务方的敏感信息。

（2）伪造

对用户身份伪造（Fabrication）这一常见的网络攻击方式，传统的对策一般采用身份认证方式来进行防护，但是，用于用户身份认证的密码在登录时常常是以明文的方式在网络上进行传输的，很容易被攻击者在网络上截获，进而可以对用户的身份进行仿冒，使身份认证机制被攻破。身份认证的密码 90％以上是用代码形式传输的。

（3）篡改

攻击者有可能对网络上的信息进行截获并且篡改（Modification）其内容

（增加、截去或改写），使用户无法获得准确、有用的信息或落入攻击者的陷阱。

（4）中断

攻击者通过各种方法，中断（Interruption）用户的正常通信，达到自己的目的。

（5）重发

信息重发（Repeat）的攻击方式，即攻击者截获网络上的密文信息后，并不将其破译，而是把这些数据包再次向有关服务器（如银行的交易服务器）发送，以实现恶意的目的。

安全体系结构与模型

一、选择题

1. 信息安全的基本属性是（D）。

A. 机密性　B. 可用性

C. 完整性　D. 上面 3 项都是

2. “会话侦听和劫持技术”是属于（B）的技术。

A. 密码分析还原　B. 协议漏洞渗透

C. 应用漏洞分析与渗透　D. DOS 攻击

3. 对攻击可能性的分析在很大程度上带有（B）。

A. 客观性　B. 主观性

C. 盲目性　D. 上面 3 项都不是

4. 从安全属性对各种网络攻击进行分类，阻断攻击是针对（B）的攻击。

A. 机密性　B. 可用性　C. 完整性　D. 真实性

5. 从安全属性对各种网络攻击进行分类，截获攻击是针对（A）的攻击。

A. 机密性　B. 可用性　C. 完整性　D. 真实性

6. 从攻击方式区分攻击类型，可分为被动攻击和主动攻击。被动攻击难以（C），然而（C）这些攻击是可行的；主动攻击难以（C），然而（C）这些攻击是可行的。

A. 阻止,检测,阻止,检测　B. 检测,阻止,检测,阻止

C. 检测,阻止,阻止,检测　D. 上面 3 项都不是

7. 窃听是一种（A）攻击，攻击者（A）将自己的系统插入到发送站和接收站之间。截获是一种（A）攻击，攻击者（A）将自己的系统插入到发送站和接受站之间。

A. 被动,无须,主动,必须 B. 主动,必须,被动,无须

C. 主动,无须,被动,必须 D. 被动,必须,主动,无须

8. 拒绝服务攻击的后果是（E）。

A. 信息不可用 B. 应用程序不可用

C. 系统宕机 D. 阻止通信 E. 上面几项都是

9. 机密性服务提供信息的保密，机密性服务包括（D）。

A. 文件机密性 B. 信息传输机密性

C. 通信流的机密性 D. 以上 3 项都是

10．最新的研究和统计表明，安全攻击主要来自（B）。

A. 接入网 B. 企业内部网 C. 公用 IP 网 D. 个人网

11．攻击者用传输数据来冲击网络接口，使服务器过于繁忙以至于不能应答请求的攻击方

式是（A）。

A. 拒绝服务攻击 B. 地址欺骗攻击

C. 会话劫持 D. 信号包探测程序攻击

12．攻击者截获并记录了从 A 到 B 的数据，然后又从早些时候所截获的数据中提取出信息，重新发往 B 称为（D）。

A. 中间人攻击 B. 口令猜测器和字典攻击

C. 强力攻击 D. 回放攻击

13. 网络安全是在分布网络环境中对（D）提供安全保护。

A. 信息载体 B. 信息的处理、传输

C. 信息的存储、访问 D. 上面 3 项都是

14. ISO 7498-2 从体系结构观点描述了 5 种安全服务，以下不属于这 5 种安全服务的是（B）。

A. 身份鉴别 B. 数据报过滤

C. 授权控制 D. 数据完整性

15 数据保密性安全服务的基础是（D）。

A. 数据完整性机制　　B. 数字签名机制

C. 访问控制机制　　D. 加密机制

16. 可以被数据完整性机制防止的攻击方式是（D）。

A. 假冒源地址或用户的地址欺骗攻击

B. 抵赖做过信息的递交行为

C. 数据中途被攻击者窃听获取

D. 数据在途中被攻击者篡改或破坏

第二章　密码学及密码体制

一、密码学的概述

密码学包括两个分支：**密码编码学**和**密码分析学**。**加密的基本方法是替代和置换**

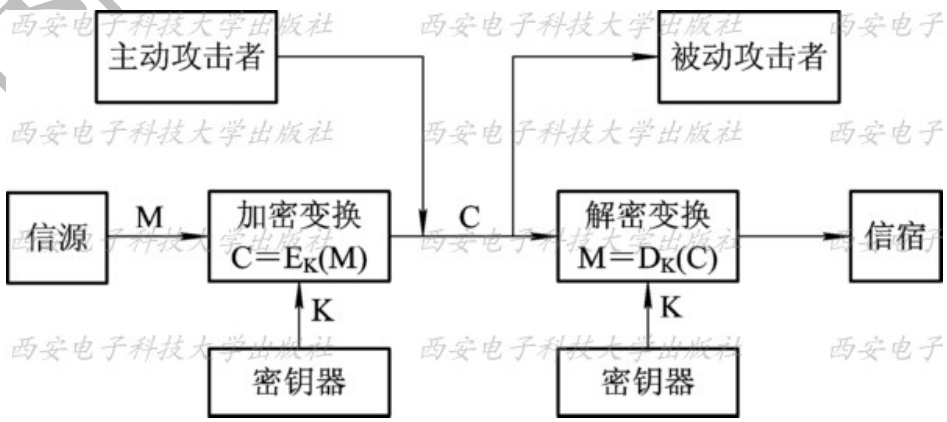
替代算法指的是：明文的字母由其他字母或数字或符号所代替。

置换密码指的是：对明文字符按某种规律进行位置的置换。

密码学中一些常用的术语：

- 明文(Message)：指待加密的信息，用M或P表示。明文可能是文本文件、位图、数字化存储的语音流或数字化的视频图像的比特流等。
- 密文(Ciphertext):用C表示。
- 密钥(Key)：指用于加密或解密的参数，用K表示。
- 加密Encryp或者 Encipher
- 解密Decryp 或者Decipher

密码系统模型



二、古典密码

古典密码与现代密码的区别是：古典密码体制中，数据的保密基于加密算法的保密。而现代密码体制中，数据的安全基于密钥而不是算法的保密。

（1）**棋盘密码**：世界上最早的一种密码产生于公元前两世纪。是由一位希腊人提出的，人们称之为棋盘密码，将 26 个字母放在 5×5 的方格里，“i”“j”放在一个格子里，具体情况如下表所示

	1	2	3	4	5
1	a	b	c	d	e
2	f	g	h	i/j	k
3	l	m	n	o	p
4	q	r	s	t	u
5	v	w	x	y	z

如 c 对应 13，s 对应 43 等。

如果接收到”密文”为 43 15 13 45 42 15 32 15 43 43 11 22 15

则对应的”明文”即为 secure message

（2）“凯撒密码”

凯撒密码有两种模式——移位法和替换法。其中，移位法就是让明文都向固定方向移动特定位数，例如 **I love you** 右移动 4 位就变成了 **M pszi csy**。

但英文或拉丁文，字母出现的频率并不一致。在获得足够多的密文样本后可以通过频率计算准确找到移位规则，从而破解密文。同时由于需要可逆操作，所以实际上秘钥只有 25 种可能。因此，完全可以通过暴力破解来对密文进行解密。

于是大部分凯撒密码在实际应用中都采用了第二种模式——替换法。定义一张明文密文映射表

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

例如 **I love you** 替换就变成了 **B Ehox rhn**。

这种方式可以在一定程度上解决密钥可穷举的问题，但仍对大数据量的频率攻击束手无策。

后来，这种模式发展为，靠引入一些特定参数来扰乱频率，这在一定程度上提高了解密的难度，但仍属于替换法和移位法的范畴。

（3） **“维吉尼亚密码”**：它以置换移位为基础的周期替换密码。

在维吉尼亚密码中，加密密钥是一个可被任意指定的字符串。加密密钥字符依次逐个作用于明文信息字符。明文信息长度往往会大于密钥字符串长度，而明文的每一个字符都需要有一个对应的密钥字符，因此密钥就需要不断循环，直至明文每一个字符都对应一个密钥字符。

对密钥字符，我们规定密钥字母 a，b，c，d……y，z 对应的数字 n 为：0，1，2，3……24，25。每个明文字符首先找到对应的密钥字符，然后根据密钥字符对应的数字 n 向后顺序推后 n 个字母，即可得到明文字符对应的密文字符。如果密钥字为 deceptive ， 明文为 wearediscoveredsaveyourself，则加密的过程为：

明文： wearedisc overedsav eyourself

密钥： deceptive deceptive deceptive

密文： zicvtwqng rzgvtwavz hcqyglmgj

对明文中的第一个字符 w，对应的密钥字符为 d，它对应需要向后推 3 个字母 x,y,z,因此其对应的密文字符为 z。上面的加密过程中，可以清晰的看到，密钥 deceptive 被重复使用。

（4）置换密码： 又叫换位密码，其特点就是保持明文的所有字符不变，打乱明文字符的位置和次序。常见的置换密码有两种：列置换密码和周期置换密码

- **列置换加密**

将明文字符 P 以固定的分组宽度 m 按行写出，构成 m x n 的矩阵[M]mxn，不够的按双方约定的字符补充，比如空格字符。然后通过某一交换列的位置次序的到矩阵[Mp]mxn，最后输出举证[Mp]mxn，即得到密文。

比如明文 P="Sit down please!"，密钥为：$\sigma=(1,2,4)(3,5)$，即将第一列放到第 2 列，第 2 列放到第 4 列，第 4 列放到第一列，第 3 列放到第 5 列，第 5 列放到第 3 列，得到的密文 Pm="dSoitlwenp!a se"最终加密过程如下：

$$[M]_{3X5}=\begin{bmatrix} S & i & t & d & o \\ w & n & p & l & e \\ a & s & e & ! & \square \end{bmatrix}\xrightarrow{\sigma}[M_p]_{3X5}=\begin{bmatrix} d & S & o & i & t \\ l & w & e & n & p \\ ! & a & \square & s & e \end{bmatrix}$$

- **列置换解密**

列置换的解密过程就是加密的逆过程，根据上面的例子，可以知道密钥的逆置换为：

$\sigma^{-1}=(1,4,2)(3,5)$，则机密的过程如下：

$$[M_p]_{3X5}=\begin{bmatrix} d & S & o & i & t \\ l & w & e & n & p \\ ! & a & \square & s & e \end{bmatrix}\xrightarrow{\sigma^{-1}}[M]_{3X5}=\begin{bmatrix} S & i & t & d & o \\ w & n & p & l & e \\ a & s & e & ! & \square \end{bmatrix}$$

- **周期置换：其实就是在列置换的基础上，进行行输出。**

周期置换密码

明文：ming chen jiu dian fa dong fan gong

加密密钥：3421（i=1,2,3,4 的一个置换 f(i) =3,4,2,1）

加密：将明文分组（4 个字母一组），然后根据规定顺序变换

ming chen jiud ianf adon gfan gong

ngim enhc udij nfai onda anfg ngog

密文：ngimenhcudijnfaiondaanfgngog

解密密钥：4312（3412 的逆置换）

古典密码后期发展出 ROT5/13/18/47、摩尔斯密码等一系列密码种类。但都是以替换法和移位法为核心基础，安全性也主要是靠算法不公开来保证。所使用的加密算法只能算是现在加密算法的雏形，或者仅作为可以借鉴的最初加密思路。

古典密码体制将数学的方法引入到密码分析和研究中。这为现代加密技术的形成和发展奠定了坚实的基础。

三、 现代加密体制

现代加密算法可以分为对称加密、不对称加密和不可逆加密三类算法

- 对称秘钥密码体制：加解密使用同一个密钥
- 非对称秘钥密码体制：加解密使用不同的密钥，而且两种密钥不能相互推导。
- **不可逆加密算法**：加密过程中不需要使用密钥，输入明文后由系统直接经过加密算法处理成密文，这种加密后的数据是无法被解密的只有重新输入明文，并再次经过同样不可逆的加密算法处理，得到相同的加密密文并被系统重新识别后，才能真正解密。而所谓解密实际上就是重新加一次密，**所应用的“密码”也就是输入的明文**。不可逆加密算法不存在密钥保管和分发问题，非常适合在分布式网络系统上使用，但因加密计算复杂，工作量相当繁重，通常只在数据量有限的情形下使用，如广泛应用在计算机系统中的口令加密，利用的就是不可逆加密算法。在计算机网络中应用较多不可逆加密算法的有 RSA 公司发明的 **MD5 算法**和由美国国家标准局建议的**不可逆加密标准 SHS**(Secure Hash Standard:**安全杂乱信息标准**)等。

(1)、对称秘钥密码体制：分为两种算法，序列算法和分组算法。

序列算法是对单个比特或字节进行运算.分组算法是对一组比特或字节进行运算.

- **DES：数据加密标准。是一种分组密码，密钥使用一个 56 位的密钥以及 8 位奇偶校验位。以 64 位的分组为处理对象。这是一个迭代的分组密码，**

使用称为 Feistel 的技术，其中将加密的文本块分成两半。使用子密钥对其中一半应用循环功能，然后将输出与另一半进行“异或”运算；接着交换这两半，这一过程会继续下去，但最后一个循环不交换。**DES 使用 16 个循环，使用异或，置换，代换，移位操作四种基本运算**。

DES 算法的入口参数有三个：Key、Data、Mode。

Key 为 8 个字节共 64 位，是 DES 算法的工作密钥；

Data 也为 8 个字节 64 位，是要被加密或被解密的数据；

Mode 为 DES 的工作方式，有两种：加密或解密。

DES 算法是这样工作的：

如 Mode 为加密，则用 Key 去把数据 Data 进行加密，生成 Data 的密码形式**（64 位）作为 DES 的输出结果；**

如 Mode 为解密，则用 Key 去把密码形式的数据 Data 解密，还原为 Data 的明码形式**（64 位）作为 DES 的输出结果。**

在通信网络的两端，双方约定一致的 Key，在通信的源点用 Key 对核心数据进行 DES 加密，然后以密码形式在公共通信网（如电话网）中传输到通信网络的终点，数据到达目的地后，用同样的 Key 对密码数据进行解密，便再现了明码形式的核心数据。这样，便保证了核心数据（如 PIN、MAC 等）在公共通信网中传输的安全性和可靠性。

通过定期在通信网络的源端和目的端同时改用新的 Key，便能更进一步提高数据的保密性，这正是现在金融交易网络的流行做法

DES 算法描述

1)、输入 64 位明文数据，并进行初始置换 IP；

2)、在初始置换 IP 后，明文数据再被分为左右两部分，每部分 32 位，以 L0，R0 表示；

3)、在秘钥的控制下，经过 16 轮运算(f)；　　4)、16 轮后，左、右两部分交换并连接再一起，再进行逆置换；　　5)、输出 64 位密文。

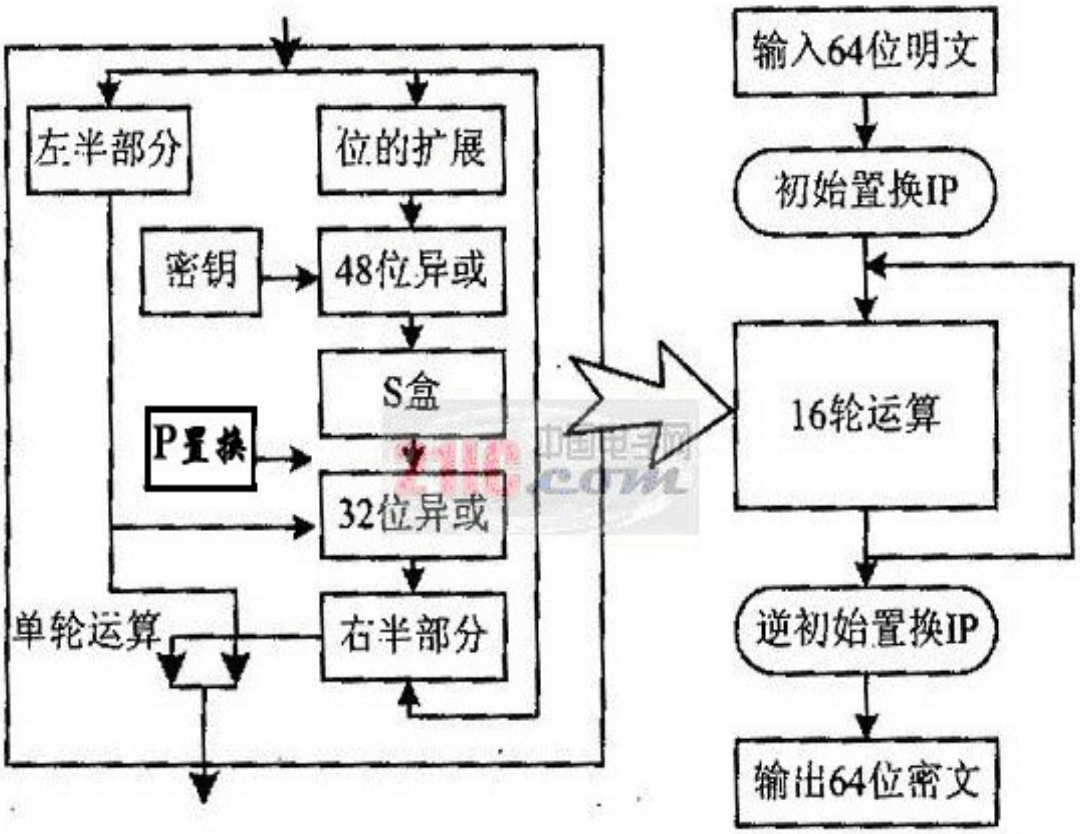
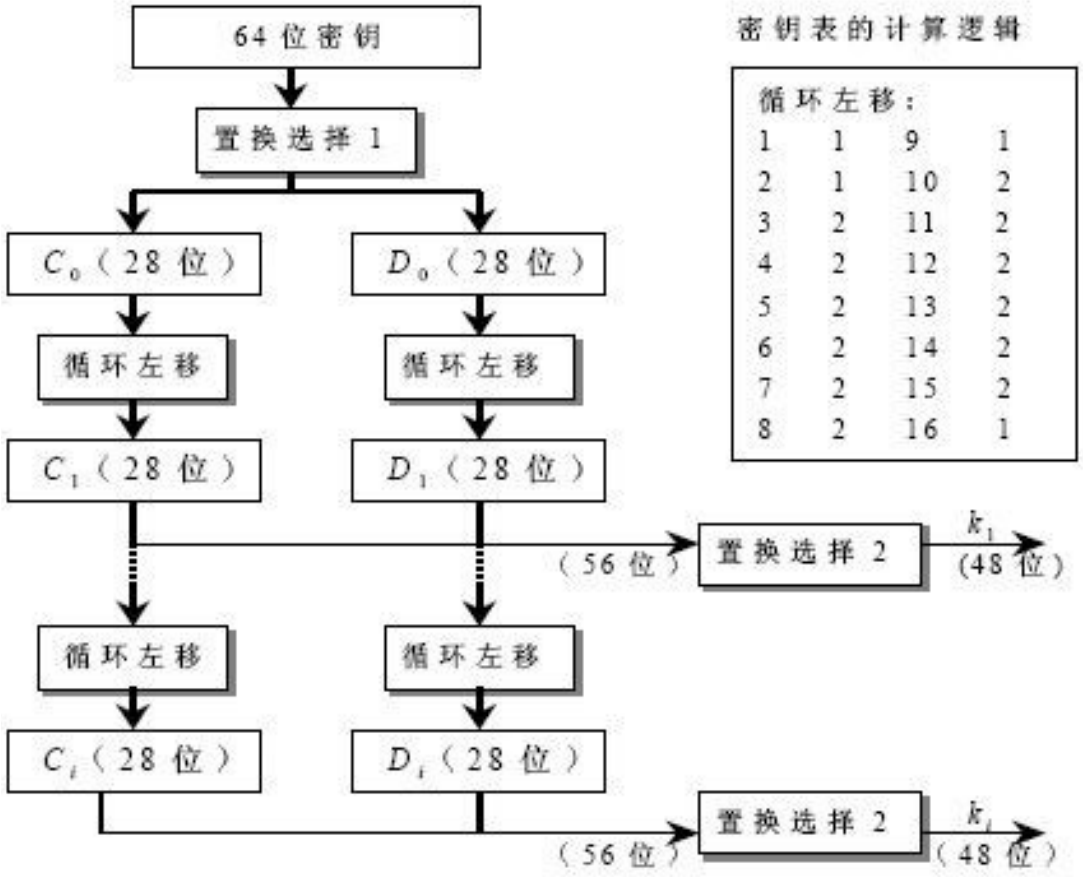


图1 DES算法结构



4子密钥的生成过程

- **3DES** ： 3DES 是 DES 加密算法的一种模式，它使用 3 条 64 位的密钥对数据进行三次加密。**密钥长度 128 位或 192 位**。它使用 3 个密钥 K1,K2，k3。若数据对安全性要求不那么高，K1 可以等于 K3，一般实际使用 K1 加密，然后用 K2 解密，再用 K1 加密。增加安全性。
- IDEA ： **国际数据加密算法。密钥长度：128 位**，在 DES 算法的基础上发展出来的，类似于三重 DES
- **RC4 算法**：是目前最安全的加密算法之一，密钥长度是可变的，**可变范围为 1-256 字节**(8-2048 比特)，但一般为 256 字节。它算法简单，运行速度快，该算法的速度可以达到 DES 加密的 10 倍左右。
- **AES :** 高级加密标准。这个标准用来替代原先的 DES，已经被多方分析

且广为全世界所使用。**密钥长度：128 位、192 位、256 位**。是下一代的加密算法标准，速度快，安全级别高，。

（2）公钥密码体制（RSA）

公钥密码体制使用不同的加密密钥与解密密钥，相互配对使用。具有唯一对应的关系。并且“**由已知一个密钥推导出解另一个密钥在计算上是不可行的**”。它是利用数学上“大素数分解困难”的原理来建立的密码算法。虽然没有在数学上得到证明，但至今没有被破解。 它广泛用于网络环境下数据加密和数据与身份的鉴别。

1、公钥和私钥

在公钥密码体制中，**加密密钥(即公钥) PK（Public Key） 是公开信息**，而**解密密钥**(即私钥或秘钥) SK(Secret Key) 是**需要保密的**。

2、算法（了解）

1. 选择两个大素数，p 和 q ，计算出 n=qp，n 称为 RSA 算法的模数。p，q 必须保密，一般要求 p，q 为安全素数，n 的长度大于 1024bit ，这主要是因为 RSA 算法的安全性依赖于因子分解大数问题。

2. 计算 n 的欧拉数

φ(n)=(p-1)(q-1)

φ(n)定义为不超过 n 并与 n 互质的数的个数。

3. 然后随机选择加密密钥 e，从[0,φ(n)-1]中选择一个与 φ(n)互质的数 e 作为公开的加密指数。

4. 最后，利用欧几里德算法（Euclid 算法）计算解密密钥 d, 满足 de≡1(mod φ(n))。其中 n 和 d 也要互质。数 e 和 n 是公钥，d 是私钥。两个素数 p 和 q 不再需要，应该丢弃，不要让任何人知道。

5.得到所需要公开密钥和秘密密钥：

公开密钥（即加密密钥） PK=（e，n）

秘密密钥（即解密密钥） SK=（d，n）

3、公钥算法的特点

- **私钥用于数字签名和解密，公钥用于身份验证和加密**

- **公私钥间不能相互推导**
- **缺点：速度太慢，产生密钥很麻烦，难以做到一次一密**

➢ 发送者 A 用 B 的公钥 PK（B）对明文 X 加密（E 运算）后，在接收者 B 用自己的私钥 SK（B） 解密（D 运算），即可恢复出明文。

➢ 解密密钥是接收者专用的秘钥，对其他人都保密。公钥是公开的用于加密数据。

➢ 发送者 A 用自己的私钥 SK（A）对数据签名后，接收者 B 用 A 的公钥 PK（A）对数据解密来验证是 A 发的数据。 由于是唯一的关系所以 A 无法抵赖，B 仅需保持 A 发来的数据和 A 的公钥就可以了。

➢ 加密和解密算法都是公开的，加密和解密算法的运算可以对调 。

➢ 速度太慢，由于 RSA 的分组长度太大，为保证安全性，n 至少也要 600 bits 以上，使运算代价很高，尤其是速度较慢，较对称密码算法慢几个数量级；

➢ 产生密钥很麻烦，受到素数产生技术的限制，因而难以做到一次一密。

- **例题：**用 RSA 算法加密时,已知公钥是(e=7,n=20),私钥是（d=3,n=20）,用公钥对消息 m=3 加密,得到的秘文是?

公式：加密 $C=m^e \bmod n$ 解密 $m=c^d \bmod n$

解： $C=m^e \bmod n$ $m^e=3^7=2187$ $2187 \bmod 20 = 7$ $C=7$

$m=c^d \bmod n$ $c^d=7^3=343$ $343 \bmod 20 = 3$ $m=3$

三、鉴别

在信息的安全领域中，**对付被动攻击**的重要**措施是加密**，而**对付主动攻击中的篡改和伪造则要用鉴别**(authentication) 。

1、鉴别有两种：实体鉴别和报文鉴别

- **实体鉴别：**验证通讯的对方是真实的而非冒充者。**可以使用数字签名的**

手段来完成。

- **报文鉴别**：使接收方能够验证所收到的**报文内容的真伪**，包括报文的内容、发送时间、发送序列等，**可以使用 MD5 或 SHA 等消息认证算法完成。**
- **消息认证所用的摘要算法**与一般的对称或非对称加密算法不同，**它并不用于防止信息被窃取，而是用于证明原文的完整性和准确性**。也就是说，**消息认证主要用于防止信息被篡改**
- 使用加密就可达到报文鉴别的目的。但在网络的应用中，许多报文并不需要加密。应当使接收者能**使用简单而高效的方法鉴别报文的真伪。**

2、 报文内容鉴别技术（消息认证技术）

Hash 函数：又称杂凑函数、单向散列算法，输入一个长度不定的字符串，返回一个唯一定长的字符串，**称为 Hash 值。但已知 Hash 值不能推导出原字符串。所以又称单向散列函数**

Hash 函数的算法有两种：

1、MD5 报文摘要：输入按 512 位的分组进行处理，**摘要长度 128 位**

2、SHA 安全散列算法：输入按 512 位的分组进行处理，**摘要长度 160 位**

消息认证过程：发送者发送前利用上述算法计算“摘要信息”，并将信息和摘要一同发给接收者，接收者将信息再次用相同算法计算比对后，确认数据的真实性。

应用：可以使用信息摘要技术结合 RSA 加密技术完成消息认证。

四、数字签名

数字签名可以而且必须保证以下三点：

(1) **身份鉴别：**接收者能够**核实发送者**对报文的签名，并且不能伪造对报文的签名；

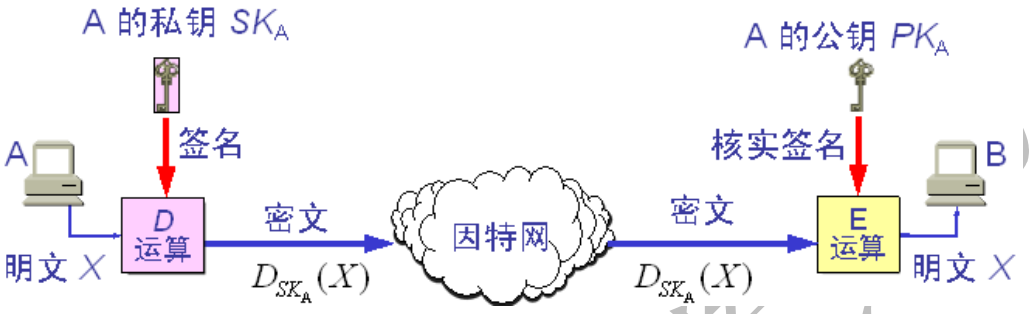
(2) **报文完整性：**接受者可以确认收到的报文与发送的报文完全一样，**没有被**

篡改和伪造

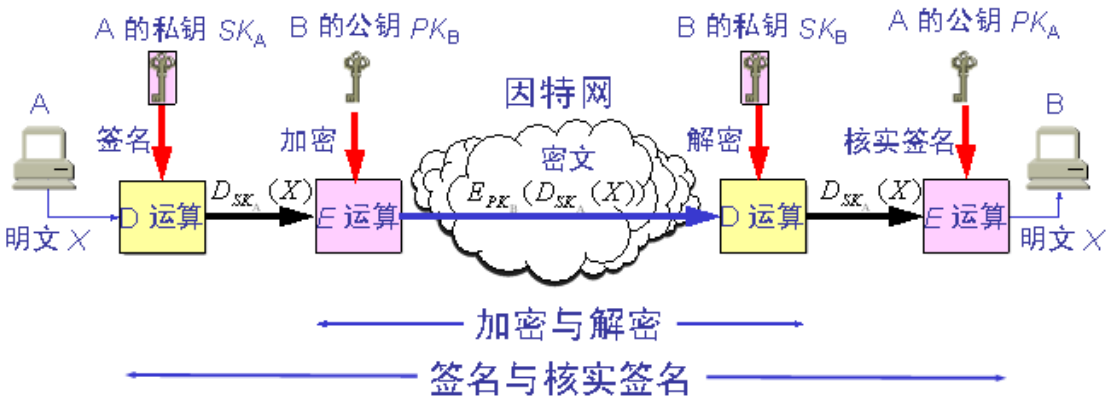
(3) **不可否认**：发送者事后**不能抵赖**对报文的签名。

现在已有多种实现数字签名的方法。但采用公钥算法更容易实现。

数字签名的实现：



- 因为除 A 外没有别人能具有 A 的私钥，所以除 A 外没有别人能产生这个密文。因此 B 相信报文 X 是 A 签名发送的。
- 若 A 要抵赖曾发送报文给 B，B 可将明文和对应的密文出示给第三者。第三者很容易用 A 的公钥去证实 A 确实发送 X 给 B。
- 反之，若 B 将 X 伪造成 W，则 B 不能在第三者前出示对应的密文。这样就证明了 B 伪造了报文。



具有保密性的数字签名

过程：

1. Alice 准备好要传送的数字信息（明文）。

2. Alice 对数字信息进行哈希（hash）运算，得到一个信息摘要。

3. Alice 用自己的私钥（SK）对信息摘要进行加密得到 Alice 的数字签名，并将其附在数字信息上。

4. Alice 随机产生一个加密密钥（对称），并用此密钥对要发送的信息进行加密，形成密文

5. Alice 用 Bob 的公钥（PK）对刚才随机产生的加密密钥进行加密，将加密后的密文传送给 Bob

6. Bob 收到 Alice 传送过来的密文，用自己的私钥（SK）对对称密钥和密文解密。

7. Bob 用 Alice 的公钥（PK）对 Alice 的数字签名进行解密，得到信息摘要。

8. Bob 用相同的 hash 算法对收到的明文再进行一次 hash 运算，得到一个新的信息摘要。

9. Bob 将收到的信息摘要和新产生的信息摘要进行比较，如果一致，说明收到的信息没有被修改过。

采用数字签名，能完成这些功能：

（1）确认信息是由签名者发送的；

（2）确认信息自签名后到收到为止，未被修改过；

（3）签名者无法否认信息是由自己发送的

五、密钥分发中心（KDC）

- 对称密钥分发：需要有秘密信道。通常在一个组织内部网络使用，由一台专门的机器担当，使用的是 **Kerberos 协议**。
- **PKI 公钥基础设施**：用于非对称密钥分发
  - **CA 认证中心（颁发数字证书）**，分发公钥密钥。它由有公信力的第三方机构建立。
    - **X.509 证书** 包括以下内容：版本号，序列号，有效期，签名算法标识符，签发人姓名，主体名，**主体公钥**等
    - **CA 认证中心间也可以通过相互信任，而实现不同认证中心间用户间的信任链。**
    - **根证书是 CA 自己的证书**，是证书验证链的开头。根证书没有机构

（已经是权威了）再为其做数字签名，所以都是自签证书。

例题：

填空：

1. 现代密码系统的安全性是基于**密钥**的安全而不是基于对加密算法和解密算法的保密。
2. 一个现代密码系统包括所有可能的明文、密文、**密钥**、加密算法和解密算法。
3. 密码学是研究信息系统安全保密的科学，它包含**密码编码学**和密码分析学两个分支。
4. 密码系统从原理上可以分为两大类，即**单钥体制**和双钥体制。
5. 单钥体制根据加密方式的不同又分为流密码和**分组密码**。
6. 相对于单钥体制，双钥体制的一个优越性是无需事先分配**密钥**。
7. 古典密码的两个基本工作原理是**代换**和置换。
8. **代换密码**的主要思想是通过符号的简单替换而达到掩盖明文信息的目的，也就是将明文中的字母由其他字母、数字或者符号取代的一种方法，其中的替代方案就称为**密钥**。
9. **多表代换**使用从明文字母到密文字母的多个映射来隐藏字母出现的频率分布，明文字符和密文字符的关系是一对多的。
10. 通过重新排列消息中元素的位置而不改变元素本身来变换一个消息的密码方案称为**置换密码**。
11. **DES** 密码算法是 1977 年由美国国家标准局公布的第一个分组密码算法。
12. DES 在国际通信保密舞台上活跃了 25 年后，在 21 世纪初被新的数据加密标准 **AES** 取代。
13. RSA 非对称密码体制的安全性依赖于**大整数分解**的困难性。
14. 公钥密码系统中，信息发送方用接收方的**公钥**加密报文，则只有接收者可以用自己的**私钥**解密该信息。
15. 为了在网络通信中实现发送消息的不可否认性，即发送方不能否认曾经发送了某个消息，可以借助**数字签名**技术来实现。
16. **非对称**密码体制是实现数字签名的技术基础。

17. 凯撒密码变换是对英文 26 个字母进行位移代换的密码，将每一字母循环向后移位 k=3 位，则明文“CAESAR”经凯撒密码变换后得到的密文是：FDHVDU

18. 分组密码算法的设计思想是由 C.E.Shannon 提出的，主要通过扩散和混淆来实现。

19. 一个分组密码有两个重要的参数：一个是密钥长度,一个是分组长度。

ok 判断

1. 维吉尼亚密码属于古典密码中，而且是多表密码中非常知名的密码。
2. 双钥密码体制中每个用户都有一对选定的密钥（公钥 PK 和私钥 SK），特点还可以使其用于对消息的数字签名。
3. 将明文中的字母由其他字母、数字或者符号取代的一种加密方法就是代换加密，其中的替代方案就称为密钥。
4. 设计分组密码算法的核心技术是：复杂函数是通过简单函数迭代若干轮而实现的，通过简单的轮函数及置换等运算，充分利用非线性运算，实现加、解密目的。
5. 非对称密码体制的发明是现代密码的具有里程碑意义的重要事件，它的出现标志着现代密码学的创立。
6. 双钥体制也称为对称密码体制，其中明显存在的问题是如何将加密密钥通过秘密信道分发给消息的接收者，即密钥的生成和管理问题
7. 单钥体制也称为非对称密码体制或公钥体制，每个用户都有一对选定的密钥（公钥 PK 和私钥 SK），公开的密钥 PK 可以像电话号码一样进行注册公布，而私钥 SK 则由用户保密持有。
8. 双钥密码体制的加解密算法效率高，而被用于大量消息的加密。
9. 单钥密码体制的突出优点是没有密钥分发问题。
10. 维吉尼亚密码是对英文 26 个字母进行位移代换的密码，将每一字母循环向后移位 k=3 位。
11. 凯撒密码密钥 K 表示的时字母循环移动的位数，其可能的取值是任意自然数 n，因此对其进行简单的穷举试验是不可能找到密钥并解密密文的。
12. DES 是目前最著名应用最广泛的非对称密码体制，1977 年由美国国家标准

局公布。

13. RSA 是目前最著名应用最广泛的非对称密码体制，1977 年由美国国家标准局公布。

ok 简答

1. 分组密码的设计要求？

主要有以下几点：一是分组长度足够长（一般为 64～128 比特）；二是密钥长度要足够长（64～128 比特）；三是算法足够复杂，包括加、解密算法和子密钥产生算法；四是加密、解密算法简单，易于软件和硬件的实现；五是便于分析，即算法简洁清晰，但破译困难。

2. 非对称密码体制和传统的对称密码体制相比较各有什么优缺点？

非对称密码体制和传统的对称密码体制相比较，对称密码体制加密的优点是速度快，加密解密所需要的计算量小，而缺点是密钥管理工作量很大；公钥密码体制（即非对称公钥密码体制）加密解密所需要的计算量很大，但是密钥管理工作量很小。

3. 代换密码的主要思想是什么？

代换密码的主要思想是通过符号的简单替换而达到掩盖明文信息的目的，也就是将明文中的字母由其他字母、数字或者符号取代的一种方法，其中的替代方案就称为密钥。

4. 什么是单表代换密码？

单表代换密码（Monoalphabetic Cipher），是指对于一个给定的加密密钥，明文消息空间中的每一元素将被代换为密文消息空间中的唯一元素。

5. 单表代换密码有什么缺点？

单表代换密码的密钥量很小，显然不能抵抗利用现代计算机进行的穷举搜索攻击。其另一个缺陷则是，这种加密系统没有将明文字母出现的概率隐藏起来容易受到频率分析方法的攻击。

6. 什么是频率分析攻击？

频率分析攻击的根据是基于语言中各个字符出现频率的统计，而这种规律在单表代换密码中得以维持，从而可以通过统计、推测和验证的过程实现密码分析。

7. 什么是多表代换密码？

如果 M 中的明文消息元可以代换为 C 中的许多、可能是任意多的密文消息元，这种代换密码就称为多表密码（Polyalphabetic Cipher）。

8. 多表代换密码相比单表代换密码有什么优点？

多表代换使用从明文字母到密文字母的多个映射来隐藏字母出现的频率分布，明文字符和密文字符的关系是一对多的，在隐藏语言字母的频率上是有优势的，它使得攻击者不能用单字母频率统计来破解密文。

9. 如何理解分组密码的设计思想中扩散？通常如何实现扩散？

扩散是将明文组及密钥组的影响迅速地散布到输出的密文组中，通常通过置换（Permutation）的方法来实现扩散。

10. 如何理解分组密码的设计思想中扩散？通常如何实现扩散？

11. 混淆的目的是使作用于明文的密钥和密文之间的关系复杂化，实现明文和密文之间，密文和密钥之间的统计相关性的极小化，从而使统计分析攻击无法奏效，通常通过代换（Substitution）的方式实现混淆。

12. 设计分组密码算法的核心技术是什么？

复杂函数是通过简单函数迭代若干轮而实现的，通过简单的轮函数及置换等运算，充分利用非线性运算，实现加、解密目的。

13. 流密码的主要思想是什么，其密钥流有什么特点？

流密码的基本思想是加密和解密运算每次只处理一个符号，可以是一个字符或一个比特。理想的流密码属于一次一密的密码体制，其中使用的密钥流的长度与消息流长度相同。

14. 分组密码工作模式中的电码本模式如何工作？

电码本模式是最简单的工作模式，该模式将输入的消息分成一定比特长度的分组（将最后的分组填充），使用秘密密钥加密每个分组。另一端在接收到加密的分组后，解密每个分组并得到初始消息

密钥管理技术

1. 密码系统的安全性包括两个方面，一方面是系统抗密码分析的安全性；另一方面是秘密密钥保管的安全性。
2. 对于密钥安全性的研究结果表明，必须从限制一个密钥的使用时间和密钥长度两个方面保证密钥的安全基础。

3. 密钥从作用上可以分为会话密钥、密钥加密密钥、主密钥三种。
4. 56 比特的密钥长度 DES 算法的密钥量是 2^{56}
5. 密钥的完整性保护用于防止**密钥被入侵者篡改或替代**。
6. 密钥的机密性保护是为了防止**密钥被非法窃取**。
7. 典型的密钥分发方案有两类：**集中式分配方案**和分布式分配方案。
8. 密钥的机密性保护可以通过**密码**技术实现。
9. 密钥的完整性保护可以采用**数字签名**技术实现。

ok 判断：

1. 称密码中的密钥和非对称密码中的私钥都需要通过一定的机制安全地分发给用户。
2. 密码系统本身的安全性依赖于系统中基于的困难问题或者复杂的算法结构。
3. 当密码系统除了穷举攻击之外再没有其他的破译捷径时，密钥的长度越长密码体制的安全性越高。
4. 公钥密码体制的密钥管理主要是公钥的管理问题，目前较好的解决方案是引进证书（Certificate）机制。
5. 密钥管理就是管理密钥从产生到销毁的过程，包括密钥的产生、存储、分配、保护、更新、吊销和销毁等。在这一系列的过程中，除密钥的产生外其他各个过程都存在威胁系统密钥安全的安全隐患。
6. 在非对称密码系统中只有私钥所有者能够通过公开的公钥推导出私钥。
7. 非对称密钥当用于数字签名服务时，信息的发送方用接收方的私钥生成数字签名，
8. 在非对称密码系统中只有私钥所有者能够通过公开的公钥推导出私钥。
9. 非对称密钥当用于数字签名服务时，信息的接收者则利用发送方的公钥验证签名的真实性。
10. 会话密钥是指在通信或者数据交换中，用来对用户数据进行加密操作的密钥。
11. 会话密钥往往是仅对当前一次会话有效或在一个短时期内有效。
12. 会话密钥一般是非对称密钥，在加密前由系统自动生成。
13. 会话密钥一般在使用后立即销毁，从而提高安全性。
14. 理想的密钥分发方案中对会话密钥的保护是采用对称密钥。
15. 会话密钥是在一对用户之间的长期共享的秘密密钥。
16. 密钥加密密钥往往作为生成会话密钥或主密钥的种子，实现这些密钥的分发和安全保护。
17. 主密钥的分发则一般使用离线安全物理通道完成。
18. 主密钥位于密钥层次的高层，在信源与信宿之间一般有多个主密钥。
19. 对称密码体制很好地解决了密钥管理问题。

在对称密码体制中，密钥管理工作量很大。例如，一个由 n 个人组成的团体，每

个用户必须保密和其他任何一个用户的密钥，每个用户的密钥保管量将达到**n*（n-1）个。**

20. 层次化密钥的高层主密钥因为量少而易于机密保存
    为了提高密码攻击的难度，会话密钥和主密钥应该频繁更换

21. 在公钥密码系统中，由于私钥是用户秘密持有，故不存在私钥的分发问题。
22. 公钥基础设施 PKI 是用于公钥权威发布的一系列组件。
23. 构建密码服务系统的核心内容是如何实现密钥管理（主要指私钥的管理）。
24. PKI 中证书的创建、分配和撤销等一系列证书管理工作主要由 CA 负责完成。

ok 简答

1. 什么是会话密钥，有什么特点？

会话密钥是指在通信或者数据交换中，用来对用户数据进行加密操作的密钥。会话密钥往往是仅对当前一次会话有效或在一个短时期内有效。会话密钥一般是对称密钥，在加密前由系统自动生成。其生成一般是由系统根据主密钥产生在使用后立即销毁，从而提高安全性。

2. 什么是密钥加密密钥，一般采用什么加密体制？

密钥加密密钥是指，用于对密钥（会话密钥）进行加密操作的密钥。密钥加密密钥可以由对称密钥承担，也可以由非对称密钥承担，由非对称密钥对会话密钥提供保护，充分利用了非对称密码体制在密钥分发上的优势和对称密钥在加密效率上的优势，成为理想的密钥分发方案。

3. 什么是主密钥，有什么特点？

主密钥是在一对用户之间的长期共享的秘密密钥，它往往作为生成会话密钥或密钥加密密钥的种子，实现这些密钥的分发和安全保护。而主密钥的分发则一般使用离线安全物理通道完成。

4. 层次化密钥的优点？

主要有两个方面，一方面体现在密码系统的安全性上，因为层次化密钥的高层主密钥因为量少而易于机密保存，层次化密钥的低层会话密钥则由于频繁变动而提高了攻击的难度和破坏程度；另一方面，层次化密钥的优点还在于密钥的生成和管理可以自动化，因为只需要通过物理方式安全分发主密钥并为双方长期持有，其他的各层密钥则可以由算法自动生成。

5. 典型的密钥分发方案有哪些，各有什么特点？

目前，典型的密钥分发方案有两类：集中式分配方案和分布式分配方案。所谓集中式分配方案是指利用网络中的“密钥管理中心”来集中管理系统中的密钥，“密钥管理中心”接收系统中用户的请求，为用户提供安全分配密钥的服务。分布式分配方案则是由通信方自己协商完成会话密钥的共享工程，不受任何其他方面的限制。

6. 什么是密钥协商，为什么在互联网中必须使用密钥协商？

密钥协商是指需要保密通信的双方通过公开信道的通信来达成一个共享的秘密密钥的过程。在密钥协商协议中，往往最终形成的双方所共享的秘密密钥是某个函数值，而该函数的输入是由双方各提供一部分。在互联网这一开放网络环境中实现数据的保密通信时，密钥协商是非常必要的，因为通信的双方可能没有条件通过物理安全渠道达成共享的秘密密钥。

7. 密钥分发中心如何解决对称密钥的共享密钥管理问题？

通信各方建立一个大家都信赖的密钥分发中心 KDC，并且每一方和 KDC 之间都保持一个长期共享密钥。使用通信双方与中心之间的密钥，在通信双方之间创建一个会话密钥（Session Key）。在会话密钥建立之前，通信双方与 KDC 之间的长期共享密钥用来进行中心对通信方验证以及他们双方之间的验证。

8. 什么是 PKI，它包含哪些组成部分？

是公钥基础设施，是由 1.认证机构 2.公钥证书库 3，密钥备份及恢复系统 4.公钥证书撤销系统 5.PKI 应用接口等

9. 什么是 CA，为什么它签发的证书是可信的？

是认证机构在基于公钥密码体制的网络环境中，对任何一个实体的公钥进行公证，证明实体的身份以及公钥的匹配关系的认证机构。

CA 查验申请者 B 的身份（运用 ID 图和一些别的证据，可以是物理的手段），然后他为申请者生成公钥并把公钥写在证书上，为了避免证书本身被伪造，CA 用它自己的私钥在证书上签名。用户 B 可以在需要证明自己身份的场合提交由 CA 签了名的证书。任何需要使用用户 B 的公钥的人，都可以下载这个证书，并运用 CA 中心的公钥进行验证，进一步可以提取证书中的公钥。

10. 密码系统的安全性包括哪些方面？

密码系统的安全性包括两个方面，一方面是系统本身的安全性，即系统抗密码分析的安全性；另一方面是系统中秘密密钥的安全性，即秘密密钥保管的安全性。

11. 从哪两个方面保证密钥的安全基础，为什么？

其一是限制一个密钥的使用时间。因为一个密钥使用时间太长，则攻击者就可以收集该密钥加密的大量密文，大量密文的拥有显然有助于密码分析，使得密钥被攻破的可能性增加，因此必须对一个密钥的使用时间有所限制。另一方面，密钥长度也是安全性方面需要考虑的，随着运算能力的提升，密钥的安全性需要评估。

12. 什么是 PKI 信任模型？有哪几种信任模型？

所谓的 PKI 信任模型(trust model)就是一系列的规则，这些规则说明了用户怎样验证从 CA 收到的证书

信任模型的种类：

1) 层次结构信任模型
2) 网状信任模型
3) WEB 信任模型
4) 以用户为中心的信任

13. PKI 的层次结构信任模型的工作原理是什么？

层次结构信任模型

在这种模式中，认证机构（CA）是严格按照层次结构组织的，整个 CA 体系可以描绘成一个倒转的树

【例】用户 3 把一系列证书 CA<<CA1>> 和 CA1<<User3>>发给用户 1。用户 1 验证证书并提取用户 3 的公钥的步骤如下。

① 用户 1 用 CA 的公钥确认 CA<<CA1>>。

② 用户 1 从 CA<<CA1>>中提取 CA1 的公钥。

③ 用户 1 用 CA1 的公钥确认 CA1<<User3>>。

④ 用户 1 从 CA1<<User3>>中提取用户 3 的公钥

在这种层次信任模型中，所有的信任基础是建立在根 CA 基础上的，根 CA 的公钥为所有用户所共知。这样从验证 CA1 的证书到验证终端用户的证书

就构成了一个证书链

数字签名与认证技术

ok 填空：

1. 数字签名与认证技术是信息完整性和不可否认性的重要保障。
2. 数字签名与认证技术是公钥密码体制的重要应用。
3. 数字签名可用来保护信息的真实性、完整性。
4. 数字签名技术是以公钥密码体制为基础而发展和成熟起来的。
5. RSA 公钥密码体制是第一个可用于数字签名的公钥密码体制。
6. 数字签名就是用私有密钥进行加密。
7. 认证的就是利用公开密钥进行解密。
8. 最著名的哈希算法有 MD5、SHA
9. 哈希函数与数字签名算法相结合，提供对于消息的完整性检验
10. SHA-1 算法产生的输出是一个 160 比特长的消息摘要。
11. SHA-1 算法的输入（消息报文）是按 512 比特的分组进行处理的。
12. 目前常用的生物特征识别技术所用的生物特征有基于生理特征的，如人脸、指纹、虹膜。

ok 判断：

1. 同一签名者对不同文件的数字签名是不相同的。
2.
3. 如果某人用其私有密钥加密消息，能够用他的公有密钥正确解密就可认为该消息是某人签字的。。
4. 认证包括数据源认证和实体身份认证两种。
5. 数据源认证是一种安全服务，消息接收者用它来验证消息是否完整。
6. 通过人脸、虹膜、指纹等进行身份认证的方法其实就是固有某事在现实生活中的进行身份认证的实例。
7. 基于密码技术实现身份认证可以采用对称密码技术，也可以采用非对称密码技术

- 基于公钥密码学的数字签名方案被定义为一个算法三元组(Gen, Sig, Ver)，其中 Gen 是密钥生成算法。

- 基于公钥密码学的数字签名方案被定义为一个算法三元组(Gen, Sig, Ver)，其中 Sig 是签名生成算法。
- 基于公钥密码学的数字签名方案被定义为一个算法三元组(Gen, Sig, Ver)，其中 Ver 是签名验证算法。

ok 简答：

1. **一个基于公钥密码学的数字签名方案被定义为一个算法三元组(Gen, Sig, Ver)，方案中共有两方参与：签名者 Signer 与验证者 Verifier，请解释 Signer 发送消息 m 给 Verifier 后，Signer 如何完成数字签名。**

   用户首先用密钥生成算法生成系统的密钥对（Pk,Sk），签名者将公开密钥 Pk 公开，自己安全的保管私密密钥 Sk。当用户需要对某一消息 m 签名时，其采用签名算法 Sig 以自己私密钥 Sk 和 m 为输入得到消息 m 的签名 s=Sig（Sk,m）。

2. **一个基于公钥密码学的数字签名方案被定义为一个算法三元组(Gen, Sig, Ver)，方案中共有两方参与：签名者 Signer 与验证者 Verifier，请解释 Signer 发送消息 m 给 Verifier 后，Verifier 如何验证消息是否为 Signer 所发？。**

   验证着用签名验证算法 Ver 以签名者公开密钥和消息签名对为输入验证签名是否有效。

3. **公钥密码为什么能够用于数字签名、身份认证？**

   公钥密码技术是通过公钥基础设施（PKI）确立用户彼此的信任。PKI 的组成中有一个认证机构 CA，有了认证机关 CA 签发的公钥证书，网络用户就可以让需要通信的对方知道他的公钥，同时对方还能够验证公钥的合法性，因此，公要密码能够用于**数字签名、身份认证。**

4. **消息认证的目的是什么？**

   消息认证的目的有两个：其一是消息源的认证，即验证消息的来源是真实的；其二是消息的认证，即验证信息在传送过程中未被篡改

5. **RSA 算法能否直接用于实际的数字签名，为什么？**

   不能，RSA 算法直接用于实际的数字签名很不安全，任何知道 Alice 公钥 e 的人都可以容易的伪造签名。而实现中间人攻击。

一、选择题

1. Kerberos 的设计目标不包括（B）。

A. 认证　　B.授权　　C.记账　　D.审计

2. 身份鉴别是安全服务中的重要一环，以下关于身份鉴别叙述不正确的是（B）。

A. 身份鉴别是授权控制的基础

B. 身份鉴别一般不用提供双向的认证

C. 目前一般采用基于对称密钥加密或公开密钥加密的方法

D. 数字签名机制是实现身份鉴别的重要机制

3. 基于通信双方共同拥有的但是不为别人知道的秘密，利用计算机强大的计算能力，以该秘密作为加密和解密的密钥的认证是（C）。

A. 公钥认证　　B. 零知识认证

C. 共享密钥认证　　D. 口令认证

5．（C）是一个对称 DES 加密系统，它使用一个集中式的专钥密码功能，系统的核心是 KDC。

A. TACACS　B. RADIUS　C. Kerberos　D. PKI

1. 密码学的目的是（C）。

A. 研究数据加密　B. 研究数据解密

C. 研究数据保密　D. 研究信息安全

2. 假设使用一种加密算法，它的加密方法很简单：将每一个字母加 5，即 a 加密成 f。这种算法的密钥就是 5，那么它属于（A）。

A. 对称加密技术　B. 分组密码技术

C. 公钥加密技术　D. 单向函数密码技术

3. 网络安全最终是一个折衷的方案，即安全强度和安全操作代价的折衷，除增加安全设施投资外，还应考虑（D）。

A. 用户的方便性　B. 管理的复杂性

C. 对现有系统的影响及对不同平台的支持

D. 上面 3 项都是

4．A 方有一对密钥（KA 公开，KA 秘密），B 方有一对密钥（KB 公开，KB 秘密），A 方向 B 方发送，数字签名 M，对信息 M 加密为：M’= KB 公开（KA 秘密（M））。B 方收到密文的解密方案是（C）。

A. KB 公开（KA 秘密（M’））　　B. KA 公开（KA 公开（M’））

C. KA 公开（KB 秘密（M’））　　D. KB 秘密（KA 秘密（M’））

5.“公开密钥密码体制”的含义是（C）。

A. 将所有密钥公开　　B. 将私有密钥公开，公开密钥保密

C. 将公开密钥公开，私有密钥保密　D. 两个密钥相同

1. PKI 支持的服务不包括（D）。

A. 非对称密钥技术及证书管理　B. 目录服务

C. 对称密钥的产生和分发　　D. 访问控制服务

2. PKI 的主要组成不包括（B）。

A. 证书授权 CA　B. SSL

C. 注册授权 RA　D. 证书存储库 CR

3. PKI 管理对象不包括（A）。

A. ID 和口令　B. 证书

C. 密钥　D. 证书撤消

4. 下面不属于 PKI 组成部分的是（D）。

A. 证书主体　　B. 使用证书的应用和系统

C. 证书权威机构　　D. AS

5. PKI 能够执行的功能是（A）和（C）。

A. 鉴别计算机消息的始发者　　B. 确认计算机的物理位置

C. 保守消息的机密　　D. 确认用户具有的安全性特权

1. Kerberos 的设计目标不包括（B）。

A. 认证　　B.授权　　C.记账　　D.审计

2. 身份鉴别是安全服务中的重要一环，以下关于身份鉴别叙述不正确的是（B）。

A. 身份鉴别是授权控制的基础

B. 身份鉴别一般不用提供双向的认证

C. 目前一般采用基于对称密钥加密或公开密钥加密的方法

D. 数字签名机制是实现身份鉴别的重要机制

3. 基于通信双方共同拥有的但是不为别人知道的秘密，利用计算机强大的计算能力，以该秘密作为加密和解密的密钥的认证是（C）。

A. 公钥认证　　B. 零知识认证

C. 共享密钥认证　　D. 口令认证

5．（C）是一个对称 DES 加密系统，它使用一个集中式的专钥密码功能，系统的核心是 KDC。

A. TACACS　B. RADIUS　C. Kerberos　D. PKI

1. 数字签名要预先使用单向 Hash 函数进行处理的原因是（C）。

A. 多一道加密工序使密文更难破译

B. 提高密文的计算速度

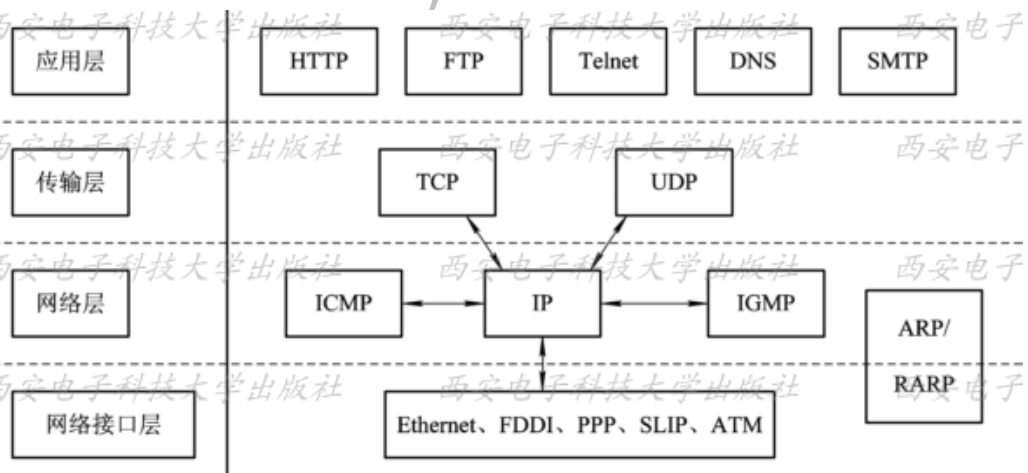
C. 缩小签名密文的长度，加快数字签名和验证签名的运算速度

D. 保证密文能正确还原成明文

第三部分　网络安全协议

一、TCT/IP 协议簇

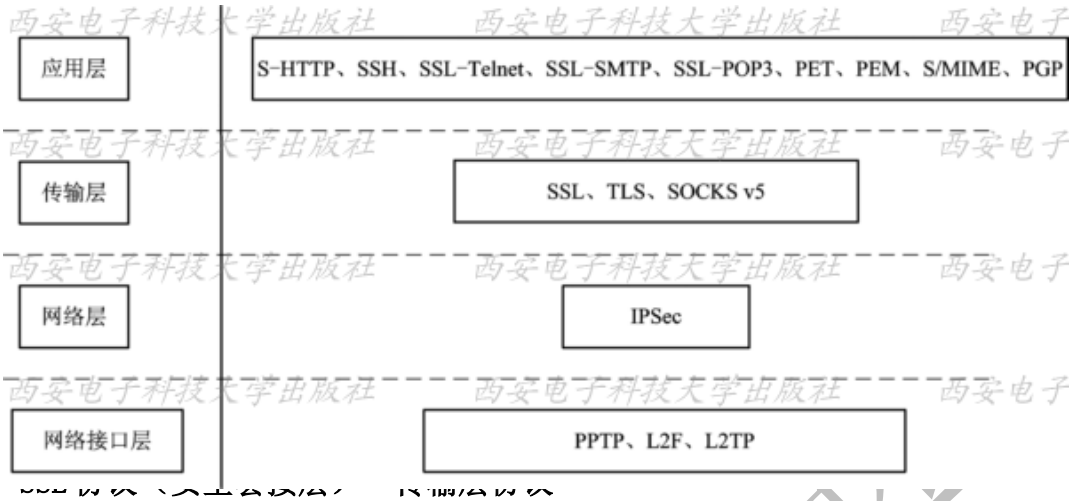
TCP/IP 协议簇是因特网的基础协议，不能简单说成是 TCP 协议和 IP 协议的和，它是一组协议的集合，包括传输层的 TCP 协议和 UDP 协议等，网络层的 IP 协议、ICMP 协议和 IGMP 协议等以及数据链路层和应用层的若干协议。



二、网络安全协议架构（了解）

为了解决 TCP/IP 协议簇的安全性问题，弥补 TCP/IP 协议簇在设计之初对安全功能的考虑不足，以 Internet 工程任务组(IETF)为代表的相关组织不断通过对现有协议的改进和设计。新的安全通信协议，对现有的 TCP/IP 协议簇提供相关的安全保证，在协议的不同层次设计了相应的安全通信协议，从而形成了由

各层安全通信协议构成的 TCP/IP 协议簇的安全架构。



三、[illegible]

最初为浏览器专门设计，现在已经是事实上的安全标准。**安全传输层协议（TLS） 就是在此标准上建立的 INTER 网安全标准协议。**

构成：

SSL 协议位于传输层与各种应用层协议之间，为数据通讯提供安全支持。

SSL 协议可分为两层（了解）：

SSL 记录协议（SSL Record Protocol）：它建立在可靠的传输协议（如 TCP）之上，为高层协议提供数据封装、压缩、加密等基本功能的支持。

SSL 握手协议（SSL Handshake Protocol）：它建立在 SSL 记录协议之上，用于在实际的数据传输开始前，通讯双方进行身份认证、协商加密算法、交换加密密钥等。

提供服务

- **认证用户和服务器**，确保数据发送到正确的客户机和服务器；
- **加密数据**以防止数据中途被窃取；
- **维护数据的完整性**，确保数据在传输过程中不被改变

四、 IPSec ：IP 安全协议 --网络层协议

- **它工作在网络层，保证 IP 包的安全**
- 它有两个相互独立，可选的协议。AH 协议（认证头协议）和 ESP 协议

（封装安全载荷）

- **AH 协议**为 IP 包提供**信息议**可以实现通信内**源鉴别和数据完整性**服务，但没有加密。
- **ESP 协**容的**保密性并可选地提供各种鉴别服务**。

五、PGP(Pretty Good Privacy) －应用层

- 它专为安全电子邮件开发。
- 是一个完整的方案，包含鉴别、加密、签名、压缩。

六、安全电子交易 SET (Secure Electronic Transaction)

- **SET 专为在因特网上进行安全支付交易而设计**
- SET 协议涉及到三方，即顾客、商家和商业银行。所有在这三方之间交互的敏感信息都被加密， 要求这三方都有证书。

七、PPTP（点对点隧道协议）--数据链路层

- **虚拟专用网（VPN）协议:是**在 PPP 协议的基础上开发的一种**新的增强型安全协议**。
- 有**密码验证**协议（PAP）、**可扩展认证**协议（EAP）**等方法增强安全性**
- 用于远程用户安全地访问企业网。

第四部分 网络攻击

一、行为分析

1、信息收集技术

信息收集是指通过各种方式获取所需要的信息。网络攻击的信息收集技术主要有网络踩点、网络扫描和网络监听等。

网络攻击的一般步骤

- **隐藏 IP**
- **踩点扫描**
- **获得系统或管理员权限**
- **种植后门**
- **在网络中隐身**

2、漏洞扫描的概念

漏洞源自“vulnerability”（脆弱性）。**一般认为，漏洞是指硬件、软件或**

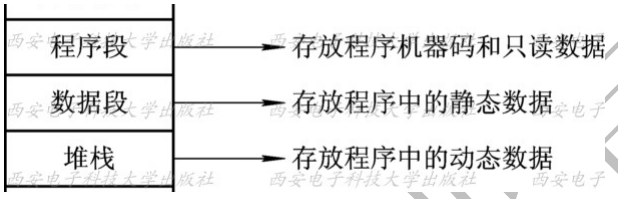
策略上存在的的安全缺陷，从而使得攻击者能够在未授权的情况下访问、控制系统。

信息系统存在着许多漏洞，这些**漏洞来自于组成信息系统的各个方面**。如：**软硬件组件**（组件脆弱性）存在的问题、**网络和通信协议（网络脆弱性）**的不健全问题等方面

端口扫描：就是根据扫描对象的服务端口号（TCP、UDP），来发现被攻击者对外所提供的服务，进而根据服务程序的漏洞攻击对方。

3、缓冲区溢出漏洞攻击

- **通过往程序的缓冲区写入精心挑选的超出其长度的内容，造成缓冲区的溢出（监视和控制的缺失），从而造成程序崩溃或使程序转而执行其它指令，以达到攻击的目的。**



- 缓冲区溢出就好比给自己的程序开了个后门，这种安全隐患是致命的。缓冲区溢出在各种操作系统、应用软件中广泛存在。
- **利用缓冲区溢出漏洞实施的攻击就是缓冲区溢出攻击。缓冲区溢出攻击，可以导致程序运行失败、系统关机、重新启动，或者执行攻击者的指令，比如非法提升权限。**

4、拒绝服务攻击-DOS

- **它是远程、通过网络进行的攻击。这种攻击行动使网站服务器充斥大量要求回复的信息，消耗网络带宽或系统资源，导致网络或系统不胜负荷以至于瘫痪而停止提供正常的网络服务。**
- 最常见的 DoS 攻击有**计算机网络带宽攻击和连通性攻击**。
- **Ddos :是分布式拒绝服务攻击，是的危害更大，更难于防御。**

拒绝服务攻击通常采用的防御方法

1. 过滤不必要的服务和端口　　2. 异常流量的清洗过滤

3. 分布式集群防御　　4. 高防智能 DNS 解析

5、口令攻击

入侵者常常采用下面几种方法获取用户的密码口令：**密码窃听（Sniffer 密码嗅探、信息收集），暴力破解（穷举法，字典法），种植木马程序**等

6、欺骗攻击

1. DNS 欺骗攻击

域名解析过程中，域名解析请求的数据包被截获，攻击者将一个虚假的 IP 地址作为应答信息返回给请求者。客户没有得到正确的 IP 地址而无法连接或连接到错误的 IP。

2. Web 欺骗攻击

攻击者通过伪造某个 WWW 站点，使用户误入到网站中，而达到攻击者监控受攻击者的任何活动以获取有用信息的目的。

3. IP 欺骗攻击

IP 地址欺骗是指行动产生的 IP 数据包为伪造的源 IP 地址，以便冒充其他系统或发件人的身份。

4、 电子邮件欺骗

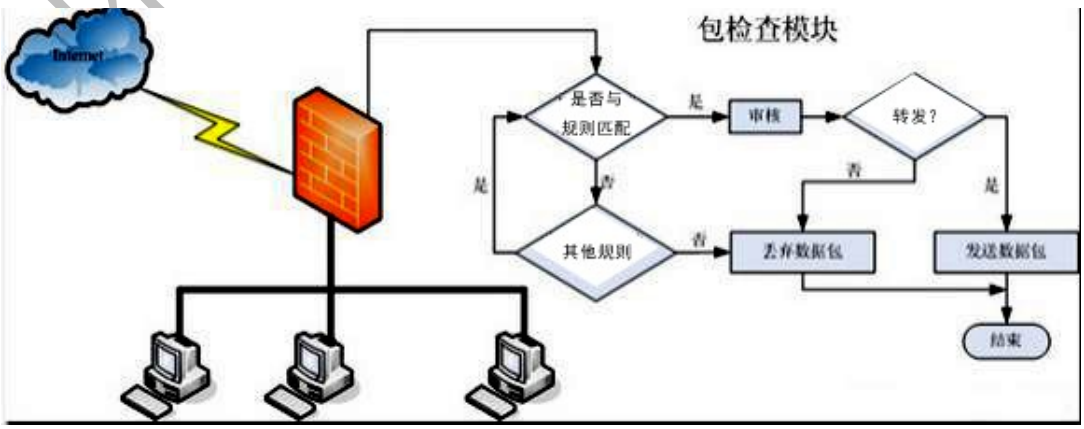
电子邮件欺骗是伪造电子邮件头，导致信息看起来来源于某个人或某个地方，而实际却不是真实的源地址。

5. ARP 欺骗攻击（重点理解）

ARP 是地址解析协议，负责将 IP 地址转换为 MAC 地址。为了减少网络流量，当一台主机的 ARP 处理机制中接收到一个 ARP 应答的时候，该主机不进行验证，即使该主机从未发出任何的 ARP 请求，仍然会把接收的 MAC 地址(网卡地址)映射信息放入 ARP 缓冲，也就是说，一台主机从网上接收到的任何 ARP 应答都会更新自己的地址映射表，而不管其是否真实。ARP 欺骗正是利用这个缺陷。攻击者给用户提供错误的 MAC 地址映射。结果是在局域网内，主机间无法互联或通过网关上网。

二、防火墙技术（FireWall）

1、防火墙：是位于两个(或多个)网络间，实施网络间访问控制的一组组件的集合。它是保护内部网免受非法用户侵入的第一道关口。它是最重要的网络防护设备之一



2、防火墙技术分类

- **包过滤：**最简单常用的技术，**工作在网络层与传输层**，根据数据包头中的源与目的 IP 地址、运输层的端口号和协议等确定是否允许数据包通过。**它速度快，但安全性低。日志功能不强。**
- **应用网关代理：**工作在第 7 层应用层，通过编写应用各个协议的代理程序，实现对应用层数据的检测和分析。**它使用存储转发技术工作完全阻断内外网络的连接，安全性高但速度慢，有完善的日志功能。**
- **状态检测：**工作在 2—4 层，控制方式与包过滤相同，**但处理的对象不是单个数据包，而是整个连接，通过规则表（管理人员和网络使用人员事先设定好的）和连接状态表，综合判断是否允许数据包通过。在提高安全性的同时又提高了处理速度。**
- **完全内容检测：需要很强的性能支撑，既有包过滤功能、也有应用代理的功能。工作在 2-7 层，**不仅分析数据包头信息、状态信息，而且对应用层协议进行还原和内容分析，有效防范混合型安全威胁。

3、防火墙的组成—有五个部分

■安全操作系统

■过滤器

■网关

■域名服务

■函件服务

4、防火墙体系结构

1、 过滤路由器

优点：处理速度快、费用低（许多路由器中已经包含）、对用户透明

缺点：无法对信息提供全面控制、规律规则增加会大大降低吞吐量。

不支持用户认证、日志功能有限。

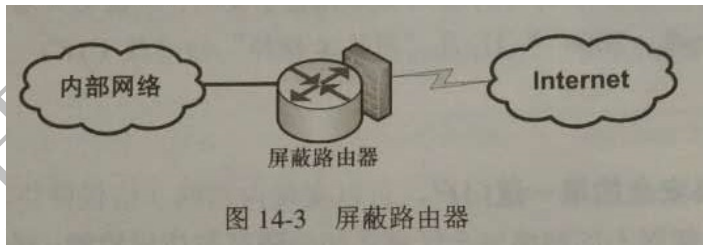


图 14-3 屏蔽路由器

2、 多宿主主机

优点：安全性比屏蔽路由器高

缺点：入侵者一旦得到主机的控制权，内部网络就会被入寝，因此需要具有强大的身份认证系统。

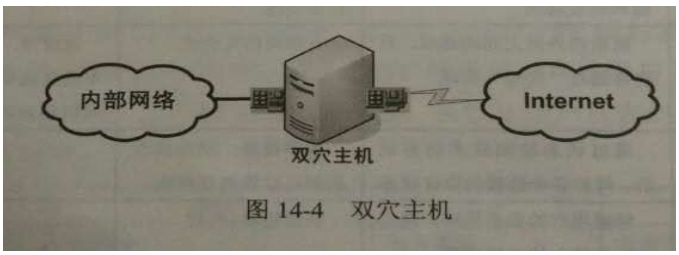


图 14-4 双穴主机

3、 屏蔽主机

优点：它实现了网络层安全（包过滤）与应用层安全（代理），因此安全等级比屏蔽路由器高

缺点：堡垒主机可能被绕过，堡垒主机与内网主机间没有安全防护一旦攻破，内网将暴露。

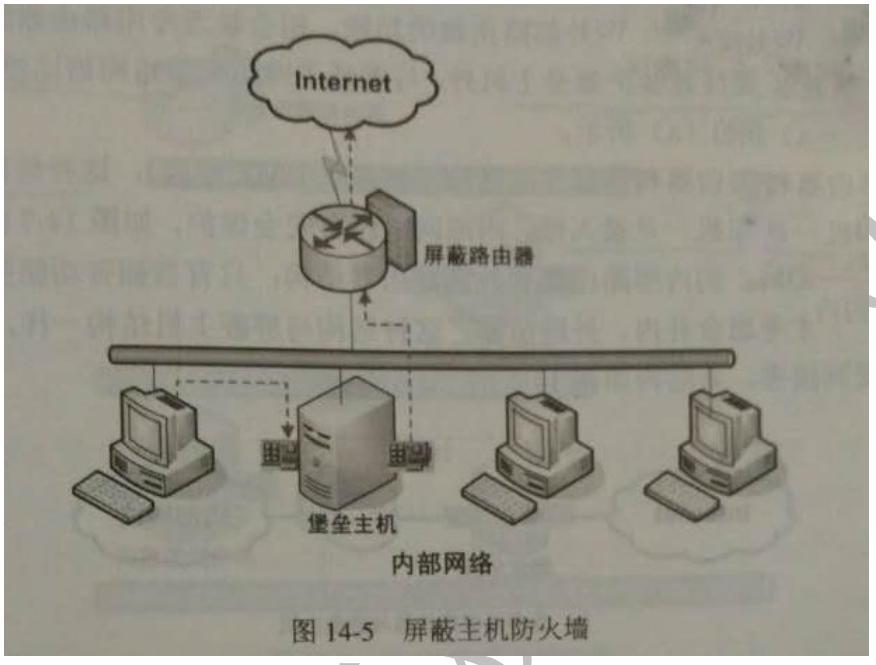


图 14-5　屏蔽主机防火墙

4、　**屏蔽子网**

优点：它定义了“非军事区（DMZ）”网络，支持包过滤与应用代理安全。这是目前最安全的防火墙系统。

DMZ 网络：通常较小，处于 Internet 和内网之间，一般将其配置为 Internet 和内网对其访问会受限的系统。如它不可主动发起访问内网和外网的请求，而内网和外网可以发起访问请求。通常放置对外公开的服务器。

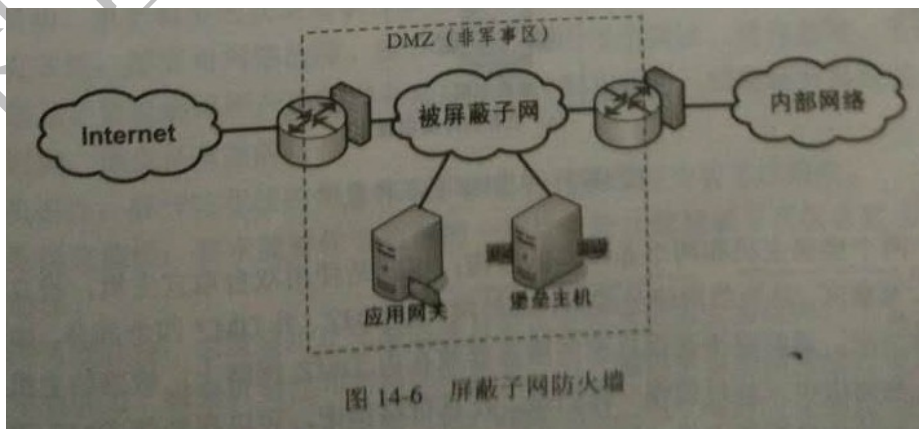


图 14-6　屏蔽子网防火墙

五、防火墙基本功能

1、**访问控制**（防火墙是一种高级的访问控制设备）

2、地址转换（都会部署在内外网之间，尤其是互联网出口，因此会涉及到**地址转换问题**）

3、网络环境支持（2 层或 3 层之间的内部连接，IP 分配等）

4、带宽管理功能（如观看视频时，同时其它人要去炒股，）

5、入侵检测和攻击防御

6、用户认证

7、高可用性

六、防火墙性能介绍－防火墙性能的五大指标

1、吞吐量：该指标直接影响网络的性能，吞吐量

2、时延：处理一帧所用的时间

3、丢包率：在稳态负载下，被丢弃的帧的百分比。现在性能发展了，这种情况已经较少了。

4、并发连接数：指穿越防火墙的主机之间或主机防火墙之间能同时建立的最大连接数

5、新建连接数能力： 1 秒之内能够新建的连接数量，体现了防火墙的反应能力或者说是灵敏度

七、防护墙---硬件芯片（ASIC）

ASIC 是专用集成电路芯片。具有以下几个方面的优越性：

1. 缩小体积、减轻重量、降低功耗；

2. 提高可靠性。

3. 易于获得高性能。

4. 可增强保密性。

三、 入侵检测系统（IDS）

1. 概述

入侵检测 ID（Intrusion Detection）是对入侵行为的发觉，它通过计算机网络或计算机系统中的若干关键点搜集信息并对其进行分析，从中发现网络或系统中是否有违反安全策略的行为和遭到袭击的迹象的一种机制。

入侵检测系统 IDS（Intrusion Detection System）是使用入侵检测技术对网络与其上的系统进行监视，并根据监视结果进行不同的安全动作，最大限度地降低可能的入侵危害。

2．按入侵检测系统的数据的来源来分，可以**分为三类：**

1） **基于主机的入侵检测系统**：其输入数据来源于系统的审计日志，一般只能检测该主机上发生的入侵；

2） **基于网络的入侵检测系统**：其输入数据来源于网络的信息流，能够检测该网段上发生的网络入侵；

3） 采用上述两种数据来源的**分布式入侵检测系统**：它能够同时分析来源于系统的审计日志和来源于网络的信息流，这种系统一般由多个部件组成。

3．系统组成

IETF将一个入侵检测**系统分为四个组件：**

- **事件产生器**（Event generators），它的目的是从整个计算环境中获得事件，并向系统的其他部分提供此事件。
- **事件分析器**（Event analyzers），它经过分析得到数据，并产生分析结果。
- **响应单元**（Response units ），它是对分析结果作出反应的功能单元，它可以作出切断连接、改变文件属性等强烈反应，也可以只是简单的报警。
- **事件数据库**（Event databases ）事件数据库是存放各种中间和最终数据的地方的统称，它可以是复杂的数据库，也可以是简单的文本文件。

4．入侵检测技术

入侵检测系统的检测分析技术主要**分为两大类，异常检测和误用检测。**

异常检测技术（Anomaly Detection）也称为**基于行为的检测技术**，是指根据用户的行为和系统资源的使用状况判断是否存在网络入侵。

误用检测技术（Misuse Detection）也称为**基于知识的检测技术或者模式匹配检测技术**，它的前提是假设所有的网络攻击行为和方法都具有一定的模式或特征，如果把以往发现的所有网络攻击的特征总结出来并建立一个**入侵信息库**，那么入侵检测系统可以将当时捕获到的网络行为特征与入侵信息库中的特征信息相比较，如果匹配，则当前行为就被认定为入侵行为。

四、 计算机病毒

1、计算机病毒的概述

计算机病毒（Computer Virus）是编制的一组计算机指令或者程序代码。它具有自我复制能力。它可以独立存在或插入程序中。目的是破坏或窃取计算机数据，影响计算机使用。

2、计算机病毒的**基本结构**

计算机病毒是一种特殊程序，其最大的特点是具有感染能力。病毒的感染动作受到触发机制的控制，同样受病毒触发机制控制的还有病毒的破坏动作。**病毒程序一般由主控模块、感染模块、触发模块和破坏模块组成，但并不是所有的病**

毒都具备这 4 个模块，如巴基斯坦病毒就没有破坏模块。

3、 计算机病毒的基本原理

（1）计算机病毒的引导

计算机病毒的引导过程一般分为三步：驻留内存、窃取控制权和恢复系统功能。

1. 驻留内存

病毒要发挥其破坏作用，多数要驻留内存。为了驻留内存，就必须开辟内存空间或覆盖系统占用的部分内存空间。

2. 窃取控制权

计算机病毒驻留内存后，接下来的工作是取代或扩充系统原有功能，并窃取系统的控制权。

3. 恢复系统功能

计算机病毒窃取系统控制权后，就要开始潜伏等待，即根据其设计思想，隐蔽自己，等待时机，在条件成熟时，再进行传染和破坏。然而，病毒为了隐蔽自己，驻留内存后还要恢复系统，使系统不致死机

（2）计算机病毒的触发机制

计数器触发：计算机病毒内部设定一个计数单元，对系统事件进行计数，判定是否激活。例如，2708 病毒当系统启动次数达到 32 次时被激活，发起对串、并口地址的攻击。

键盘触发：当敲入某些字符时触发（如 AIDS 病毒，在敲如 A、I、D、S 时发作）、或以击键次数（如 Devil’s Dance 病毒在用户第 2000 次击键时被触发）或组合键等为激发条件（如 Invader 病毒在按下 Ctrl+Alt+Del 键时发作）。

启动触发：以系统的启动次数作为触发条件。例如 Anti-Tei 和 Telecom 病毒当系统第 400 次启动时被激活。

感染触发：以感染文件个数、感染序列、感染磁盘数、感染失败数作为触发条件。例如，Black Monday 病毒在运行第 240 个染毒程序时被激活；VHP2 病毒每感染 8 个文件就会触发系统热启动操作等。

组合条件触发：用多种条件综合使用，作为计算机病毒的触发条件。

（3）计算机病毒的传播

计算机病毒的传播过程就是其传染过程。

病毒的传染大体上有：1、文件传染　2、引导扇区传染　3、及电子邮件　4、网络　5、即时聊天工具

4、反病毒技术

反病毒技术一般有如下几种：

1.特征值扫描技术 ：扫描已知病毒的特征值。

2.启发式分析技术：是在原有的特征值识别技术基础上，根据反病毒总结分析可疑程序样本的经验，在没有符合特征值比对时，判断程序是否为病毒、

恶意软件，符合判断条件即报警提示用户发现可疑程序，达到防御未知病毒、恶意软件的目的。解决了单一通过特征值比对存在的缺陷。

3. 完整性验证技术：对文件的内容是否被改变来判定

4. 虚拟机技术：“虚拟机杀毒技术”即是在内存中虚拟一个程序运行环境，将被检测程序在虚拟环境中执行，根据其行为或释放出的已知病毒特征码，来判断是否是病毒程序。

5. 沙箱技术（Sandboxie）：是一款专业的虚拟类软件，它通过重定向技术，把程序生成和修改的文件，定向到自身文件夹中。这些数据的变更，包括注册表和一些系统的核心数据。通过加载自身的驱动来保护底层数据，属于驱动级别的保护。在里面运行病毒可以说也是安全操作。

5、典型的病毒

1、木马病毒：木马（Trojan）**是指通过特定的程序（木马程序）来控制另一台计算机。木马通常有两个可执行程序：一个是服务器端，另一个是客户端。与一般的病毒不同，它不会自我繁殖，也并不“刻意”地去感染其他文件，它通过将自身伪装吸引用户下载执行，**向攻击者提供后门，使攻击者者可以任意毁坏、窃取被种者的文件，甚至远程操控被种主机。

2、蠕虫病毒：是一种常见的计算机病毒。它是**利用网络进行复制和传播，传染途径是通过网络和电子邮件。**

蠕虫病毒是自包含的程序(或是一套程序),它能传播它自身功能的拷贝或它的某些部分到其他系统中(通常是经过网络连接)。请注意，**与一般病毒不同，蠕虫不需要将其自身附着到宿主程序，它可以独立存在。**

3、 宏病毒：是一种寄存在文档或模板的宏中的计算机病毒。一旦打开这样的文档，其中的宏就会被执行，于是宏病毒就会被激活，转移到计算机上，并驻留在 Normal 模板上。从此以后，所有自动保存的文档都会“感染”上这种宏病毒，而且如果其他用户打开了感染病毒的文档，宏病毒又会转移到他的计算机上。**它存在于 office 文档中，感染 office 文件。**

6、病毒清除方法

方法一、清除未被激活的非系统文件中的病毒。

在 Windows 正常模式下，采用常用的普通杀毒软件或手工将其清除

方法二、清除已经被激活或发作的非系统文件内的病毒。

在 Windows 正常模式下，由于带毒文件正在运行，是无法对这些文件直接进行操作的。因此杀此类病毒应在 Windows 安全模式下进行。在 Windows 安全

模式下，这些病毒都不会在启动时被激活

方法三，清除系统文件内病毒

这类病毒比较难缠，所以在操作前请先备份。杀此类病毒一定要在干净的操作系统环境下进行。有时候还要反复查杀才能彻底清除。

方法四、清除通过网络传播的病毒

此类病毒必须在断网、关闭网络共享的情况下才能清除，而且清除后很容易重新被感染！在清除病毒后还需要给操作系统和浏览器打上补丁。

五、数据备份（了解内容）

数据备份就是创建数据的副本。一旦原始数据被删除、覆盖或由于故障而无法访问时，可以利用副本恢复。

1、数据备份一般分为两个层次：系统数据的备份；用户数据的备份。

2、数据备份的分类 **：1. 系统数据　2. 网络数据　3. 用户数据。**

3、使用的存储技术：

（1）直接连接存储

（2）网络附加存储(通过网络设备与存储设备连接)

（3）存储区域网络（SAN）：是一种专门为存储建立的独立于 TCP/IP 网络之外的专用网络。

4、常见的备份的类型

- **完全备份**

就是用对整个系统进行完全备份，包括系统和数据。这种备份方式的好处就是很直观，容易被人理解。而且当发生数据丢失的灾难时，只要用一盘磁带（即灾难发生之前一天的备份磁带），就可以恢复丢失的数据。然而它也有不足之处：首先由于每天都对系统进行完全备份,因此在备份数据中有大量是 重复的；其次，由于需要备份的数据量相当大，因此备份所需时间较长。

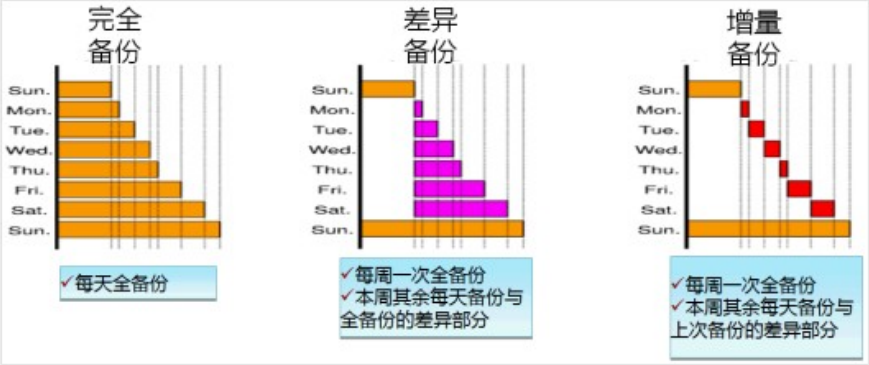
- **差异备份**

备份自从上次完全备份后被修改过的文件。它不将文件标记为已经备份（换句话说，没有清除存档属性）。在进行恢复时，我们只需对第一次全备份和最后一次差异备份进行恢复。它具有了增量备份需要时间短、节省磁盘空间的优势；其次，它又具有了全备份恢复所需磁盘少、恢复时间短的特点。

- **增量备份**

是指在一次全备份或上一次增量备份后，以后每次的备份只需备份与前一次相比增加或者被修改的文件。这就意味着，第一次增量备份的对象是进行全备后所产生的增加和修改的文件；第二次增量备份的对象是进行第一次增量备份后所产生的增加和修改的文件，如此类推。优点就是：没有重复的备份数据，因此备份的数据量不大，备份所需的时间很短。但增量备份的数

据恢复是比较麻烦的。您必须具有上一次全备份和所有增量备份磁盘（一旦丢失或损坏其中的一盘磁盘，就会造成恢复的失败），并且它们必须沿着从全备份到依次增量备份的时间顺序逐个反推恢复，因此这就极大地延长了恢复时间。



5、磁盘RAID技术（了解）

RAID简称为独立冗余磁盘阵列。简单的说，RAID是一种把多块独立的硬盘（物理硬盘）按不同的方式组合起来形成一个硬盘组（逻辑硬盘），从而提供比单个硬盘更高的存储性能和提供数据备份技术。

目前磁盘阵列模式已经拥有从RAID 0到RAID 6共7种基本级别。**常用的磁盘阵列有5种模式：RAID 0、RAID 1、RAID 0 +1、RAID 3、RAID 5。**

- RAID 0：为了提高存储性能。把连续的数据分散到多个磁盘上存取，这样，系统有数据请求就可以被多个磁盘并行的执行，这种数据上的并行操作可以充分利用总线的带宽，显著提高磁盘整体存取性能。但数据安全性下降了。
- RAID 1通过磁盘镜像实现数据冗余，在成对的独立磁盘上产生互为备份的数据。当原始数据繁忙时，可直接从镜像拷贝中读取数据，可以提高读取性能。但单位成本最高，提供了很高的数据安全性和可用性。
- RAID 0 +1： RAID 0和RAID 1的结合使用，先RAID 0再在RAID 0基础上做RAID 1。综合了它们的特点。
- RAID 3：把数据分成多个“块”，按照一定的容错算法，存放在N+1个硬盘上。实际数据占用的有效空间为N个硬盘的空间总和，而第N+1个硬盘上存储的数据是校验容错信息，当某个硬盘故障时，就从其它硬盘中的恢复原始数据。由于在一个硬盘阵列中，多于一个硬盘同时出现故障率的几率很小，所以一般情况下，使用RAID3，安全性是可以得到保

障的。

- RAID5：数据以块为单位分布到各个硬盘上。RAID 5 不对数据进行备份，而是把数据和与其相对应的奇偶校验信息存储到组成 RAID5 的各个磁盘上，并且奇偶校验信息和相对应的数据分别存储于不同的磁盘上。当 RAID5 的一个磁盘数据损坏后，利用剩下的数据和相应的奇偶校验信息去恢复被损坏的数据。