网络安全——技术与实践

第 1 章　网络安全概论

信息安全 3 个基本目标：

（1）保密性

（2）完整性

（3）可用性

1.1 对网络安全的需求

1.1.1 网络安全发展态势

（1）计算机病毒层出不穷，肆虐全球，并且逐渐呈现新的传播态势和特点。

（2）黑客对全球网络的恶意攻击势头逐年攀升。

（3）由于技术和设计上的不完备，导致系统存在缺陷或安全漏洞。

（4）世界各国军方都在加紧进行信息战的研究。

1.1.2 敏感信息对安全的需求

根据多级安全模型，通常将信息的密级由低到高划分为秘密级、机密级和绝密级，以确保每一级的信息仅能让那些具有高于或等于该权限的人使用。

1.1.3 网络应用对安全的需求

1.2 安全威胁与防护措施

1.2.1 基本概念

- 安全威胁，是指某个人、物、事件或概念对某一资源的保密性、完整性、可用性或合法使用所造成的危险。
- 攻击就是安全威胁的具体实施。
- 防护措施，是指保护资源免受威胁的一些物理的控制、机制、策略和过程。
- 脆弱性是指在实施保护措施中或缺少防护措施时，系统所具有的弱点。
- 风险，是对某个已知的、可能引发某种成功攻击的脆弱性的代价的测度。
- 安全威胁可以分为故意的和偶然的。故意的威胁又可以进一步分为被动攻击和主动攻击。被动攻击只对信息进行监听，而不对其进行修改。主动攻击却对信息进行故意的修改。
- 威胁分析的 3 个阶段：首先对基本的威胁加以区分；其次，对主要的可实现的威胁进行分类；最后，对潜在的威胁进行分类。

1.2.2 安全威胁的来源

1.基本威胁

（1）信息泄露

（2）完整性破坏

（3）拒绝服务

（4）非法使用

2.主要的可实现威胁

主要的渗入类型的威胁：

（1）假冒

（2）旁路控制

（3）授权侵犯

主要的植入威胁：

（1）特洛伊木马

（2）陷阱门

3.潜在威胁

（1）窃听
（2）流量分析操作
（3）操作人员的不慎所导致的信息泄露
（4）媒体废弃物所导致的信息泄露
1.2.3 安全防护措施
（1）物理安全
（2）人员安全
（3）管理安全
（4）媒体安全
（5）辐射安全
（6）生命周期控制
1.3 网络安全策略
安全策略，是指在某个安全域内，用于所有与安全相关活动的一套规则。
安全策略等级：
（1）安全策略目标：它是一个机构对于所保护的资源要达到的安全目标而进行的描述。
（2）机构安全策略：它是一套法律、规则及实际操作方法，用于规范一个机构如何管理、保护和分配资源，以便达到安全策略所规定的安全目标。
（3）系统安全策略：它描述如何将一个特定的信息系统付诸工程实现，以支持此机构的安全策略要求。
1.3.1 授权
是指主体对客体的支配权利，它等于规定了谁可以对什么做些什么。
1.3.2 访问控制策略
（1）基于身份的策略
（2）基于任务的策略
（3）多等级策略
1.3.3 责任
1.4 安全攻击的分类
1.4.1 被动攻击
被动攻击的特性是对说传输的信息进行窃听和监测。
第一种被动攻击是信息泄露攻击。
第二种被动攻击是流量分析
1.4.2 主动攻击
主动攻击包括对数据流进行篡改或伪造数据流。
可以分成四类：（1）伪装攻击（2）重发攻击（3）消息篡改（4）拒绝服务
1.5 网络攻击的常见形式
1.5.1 口令窃取
口令猜测攻击有 3 种基本方式：
第一种方式是利用已知的或假定的口令尝试登陆。
第二种方式是根据窃取的口令文件进行猜测。
第三种方式是通过窃听某次合法的终端之间的会话，记录所使用的口令。
1.5.2 欺骗攻击
1.5.3 缺陷和后门攻击
网络蠕虫传播的方式之一是通过向 finger 后台程序发送新的代码来实现的。
缓冲器溢出攻击也称为“堆栈粉碎”攻击。常采用的一种扰乱程序的攻击方法。

缺陷，是指程序中的某些代码并不能满足特定的要求。
（1）在编写网络服务器软件的时候，要充分考虑对黑客的攻击行为采取措施。
（2）必须要对输入语法做出正确的定义
（3）必须遵守“最小特权”原则
1.5.4 认证失效
1.5.5 协议缺陷
1.5.6 信息泄露
1.5.7 指数攻击——病毒和蠕虫
1.5.8 拒绝服务攻击
4 种防御措施：
（1）寻找一种办法来过滤掉这些不良的数据包
（2）提高对接收数据进行处理的能力
（3）追查并关闭那些发动攻击的站点
（4）增加硬件设备或提高网络容量以从容处理正常的负载和攻击数据流量
1.6 开放系统互联安全体系结构
研究目的，就是将普遍性安全体系原理与信息系统的实际相结合，形成满足信息系统安全需求的安全体系结构。
应用目的，就是从管理上和技术保证完整、准确地实现安全策略，满足安全需求。
1.6.1 安全服务
1.认证
2.访问控制
3.数据保证性
4.数据完整性
5.不可否认性
6.可用性服务
1.6.2 安全机制
1.6.3 安全服务与安全机制的关系
1.6.4 在 OSI 层中的服务配置

第 2 章　低层协议的安全性
2.1 基本协议
2.1.1 IP
IP 数据包是一组数据，这些数据构成了 TCP/IP 协议族的基础。每个数据包含有源地址和目标地址以及一些选项，如此特位、头校验和数据净荷等。
2.1.2 ARP
作用是发送包含目标 IP 地址的以太网广播数据包，目标主机或其他系统将对此作出响应，发回一个含有 IP 地址和以太地址对的数据包。
2.1.3 TCP
每个 TCP 消息都含有发送消息的主机地址和端口号，也包含目标主机地址和端口号。
2.1.4 SCTP
称为流控制传输协议
2.1.5 UDP
用户数据报协议
2.1.6 ICMP

低层通信机制，用来影响 TCP 和 UDP 连接的行为。

2.2 地址和域名管理
2.2.1 路由协议
是一种动态寻找恰当路径的机制。
2.2.2 域名系统
是一个分布式数据库系统，用来实现主机名到 IP 地址或 IP 地址到主机名的映射。
2.2.3BOOTP 和 DHCP
动态主机配置协议用来分配 IP 地址，并提供启动计算机的其他信息。
2.3IPv6
2.3.1IPv6 简介
IPv6 由一个简化的、长度固定的基本报头和多个可选的扩展报头组成。头部没有校验和字段。
2.3.2IPv6 地址
IPv6 采用一种称为冒号分十六进制的表示格式，即 128 位地址按 16 位分成若干分组，每个分组以 4 个十六进制数表示，中间用冒号风格。
2.3.3IPv6 地址配置
提供两种地址自动配置机制：无状态地址自动配置和状态地址自动配置
2.3.4 邻居发现协议
ND 协议取代 IPv4 中的 ARP 协议，ND 协议含有可达性检测功能，目的是确认相应 IP 地址代表的主机或路由器是否还能继续收发数据包。
2.3.5 移动 IPv6
移动 IP 的基本目标就是移动点从家乡链路移动到外地链路后（以及在移动过程中）仍然可以用其家乡地址与其他结点通信。
移动 IPv6 的基本操作包括移动检测、家乡代理注册、三角路由以及路由优化等。
2.3.6IPv6 的安全性
IPv6 通过 IPSec 协议来保证 IP 层安全，并且 IPSec 是 IPv6 的一个组成部分，IPv6 协议把 AH 和 ESP 作为两个可选的扩展头部。
2.4 网络地址转换器
NAT：它们监听某个接口，并对外出的数据包重写其源地址和端口号。外出数据包的源地址使用为另一个接口分配的公开源 IP 地址。对于返回的数据包，它们实行相反的操作。
2.5 无线网的安全
最常见形式采用 IEEE802.11b，又称为 WiFi，为了防止随意和偶然地访问这些网络，增加了有线等效保密（WEP）的对称密钥加密算法。

第 3 章　高层协议的安全性
3.1 消息发送
3.1.1 SMTP
简单邮件传输协议
3.1.2 MIME
多用途网际邮件扩展协议
3.1.3 POP3
Post Office Protocol 3 即邮局协议的第 3 个版本
3.1.4 IMAP4

网际消息访问协议
3.1.5 即时消息
Instant Messaging (IM)
IRC (Internet Relay Chat)
3.2 互联网电话
3.2.1 H.323
是 ITU 的因特网电话协议
3.2.2 SIP
一个通信协议，它使用户的通信系统更为开放、更好地保持连续、使用更方便、选择更多也更为个性化。
3.3 基于 RPC 的协议
3.3.1 RPC 与 Rpcbind
（Remote procedure call，RPC）远程过程调用
Rpcbind 来登记说分派的端口号。
3.3.2 NIS
网络信息服务
3.3.3 NFS
网络文件系统
3.3.4 AFS
（Andrew File System）可以与 NFS 进行互操作。主要用途是对某个机构或整个因特网提供一个独立可升级的、全球化的、位置独立的文件系统。
3.4 TFTP 和 FTP
3.4.1 TFTP
一个简单的基于 UDP 的文件传输协议
3.4.2 FTP
文件传输协议支持文本和二进制文件的传输和字符集翻译
3.4.3 SMB 协议
服务消息块
3.5 远程登录协议
3.5.1 Telnet
提供简单终端到每台主机的访问
3.5.2 “r”命令
依赖于 BSD 认证机制
3.5.3 SSH
Secure Shell.称为安全壳协议，是一种基于安全会话目的的应用程序。
3.6 SNMP
简单网络管理协议
3.7 NTP
网络时间协议主要用于调节系统时钟，从而与外部时间源达到同步。
3.8 信息服务
3.8.1 Finger——用户查询服务
Finger 功能可以帮助用户查询系统中某一个用户的细节。
3.8.2 Whois——数据库查询服务
运行于各域名注册机构

3.8.3 LDAP
轻量级目录访问协议
3.8.4 WWW 服务
3.8.5 NNTP——网络消息传输协议
网络消息通常通过网络消息传输协议进行传输。
3.8.6 多播及 MBone
多播是单播和广播概念的广义化。
3.9 专有协议
3.9.1 RealAudio
最常用的实现方案：一个客户端使用 TCP 协议连接到一个 RealAudio 服务器上，音频数据通过 UDP 数据包，并随机使用一些高标号端口发送回来。
3.9.2 Oracle 的 SQL*Net
提供了对数据库服务器的访问，该访问通常来自某个 Web 服务器。
3.9.3 其他专用服务
3.10 对等实体联网
P2P 直接将人们联系起来，让人们通过因特网直接交互。P2P 直接连接到其他用户的计算机、交换文件，而不是像过去那样连接到服务器去游览与下载。
3.11 X11 视窗系统
X11 是在 UNIX 系统中占统治地位的视窗系统。
当应用程序希望与用户会话时，这些应用程序就向 X11 服务器发出呼叫。
X11 保护机制：
第一个 X11 保护机制是基于主机地址的认证。服务器恢复应用程序的网络源地址，并把它与允许的源地址列表进行比较。那些来自于未授权主机的连接请求将被拒绝，服务器通常不会给该用户发任何提示信息。
第二个 X11 安全机制使用了 magic cookie。应用程序和服务器之间共享一个秘密 8 位字符串；没有这个字符串的进程不能连接到服务器。
第三个 X11 安全机制使用了一种密码学上的“询问/应答”机制。
目前，使用 X11 最好的方式是对其施加限制，只允许他访问本地工作站，或者使用 ssh 或 IPSec 打通 X11 隧道。
3.12 其他小的服务

第 4 章　单（私）钥加密体制
单钥加密体制也称为私钥加密体制，通信双方采用的密钥相同时也称其为对称加密体制。
可以按照其加解密运算的特点，将其分为流密码和分组密码。
4.1 密码体制的定义
密码体制的语法定义：
- 明文消息空间 M：某个字母表上的串集；
- 密文消息空间 C：可能的密文消息集；
- 加密密钥空间 K：可能的加密密钥集；解密密钥空间 K’：可能的解密密钥集；
- 有效的密钥生成算法 ζ：N→K×K’；
- 有效的加密算法 ε：M×K→C；
- 有效的解密算法 υ：C×K’→M。

对于整数 l^l，ζ（l^l）输出长为 l 的密钥对（ke，kd）∈K×K’，
对于 ke∈K 和 m∈M,将加密变换表示为

$c= \varepsilon_{ke}(m)$
读作“c 是 m 在密钥 ke 下的加密”；将解密变换表示为
$m= \upsilon_{kd}（c）$
读作“m 是 c 在密钥 kd 下的解密”。对于所有的 m∈M 和所有的 ke∈K，一定存在 kd∈K’；
$\upsilon_{kd}（\varepsilon_{ke}（m））= m$
对好的密码体制总结：
算法 ε 和 υ 不包含秘密的成分或设计部分；
ε 将有意义的消息相当均匀地分布在整个密文消息空间中，甚至可以由 ε 得某些随机的内部运算来获得随机的分布；
使用正确的密钥， ε 和 υ 是实际有效的；
不使用正确的密钥，要由密文恢复出相应的明文是一个有密钥参数的大小惟一决定的困难问题，通常取长为 s 的密钥，使得解这个问题所要求计算资源的量级超过 p（s），p 是任意多项式。
4.2 古典密码
4.2.1 代换密码
1.简单的代换密码
2.多表密码
3.弗纳姆密码和一次一密
4.2.2 换位密码
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称作换位密码（也称置换密码）
4.2.3 古典密码的安全性
古典密码两个基本工作原理：代换和换位。
4.3 流密码的基本概念
流密码是将明文划分成字符，或其编码的基本单元，字符分别与密码流作用进行加密，解密时以同步产生的同样的密钥流实现。
4.3.1 流密码框图和分类
令 $m=m_1m_2\cdots m_i$ 是待加密消息流，其中 $m_i\in M$。密文流 $c=c_1c_2\cdots c_i\cdots=E_{k1}(m_1)E_{k2}(m_2)\ \cdots Eki(mi)\ \cdots,ci\in C$。其中$\{k_i\}$（$i\geqslant 0$）是密钥流。
加法流密码
同步流密码
自同步流密码
4.3.2 密钥流生成器的结构和分类
Rupeppel 用一个更清楚的框图，将密钥生成器分成两个主要组成部分，即驱动部分和组合部分
4.3.3 密钥流的局部统计检验
对于密钥流生成器输出的密钥序列，必须进行必要的统计检验，以确保密钥序列的伪随机性和安全性，常用的方法有频度检验、序偶或联码检验、扑克（图样分布）检验、游程或串长分布检验、自相关特性检验和局部复杂性检验等。
4.3.4 随机数与密钥流
在网络安全系统中，如交互认证协议中 Nonce（一次性随机数）、密钥分配系统的会话密钥等，需要一种一次性且不要求在收端重新同步产生的随机数。
4.4 快速软、硬件实现的流密码算法
4.4.1 A5

A5 是欧洲数字蜂窝移动电话系统中采用的加密算法，用于电话手机到基站线路上的加密。

4.4.2 加法流密码生成器

1.加法生成器

2.FISH 算法

3.PIKE 算法

4.Mush 算法

4.4.3 RC4

密钥长度可变流密码

4.4.4 SEAL

SEAL 是一种适合软件实现的流密码算法。预先计算好一组表可以加速加解密运算

4.4.5 PKZIP

PKZIP 算法广泛用于文档数据压缩，其中融入了 R.Schlafiy 设计的加密算法是一种按字节加密的流密码。该算法有 3 个 32b 变量，即 96b 存储。

4.5 分组密码概述

分组密码易于构造拟随机数生成器、流密码、消息认证码（MAC）和杂凑函数等，还可进而成为消息认证技术、数据完整性机构、实体认证协议以及单钥数字签名体制的核心组成部分。

4.6 数据加密标准

4.6.1 DES 介绍

DES 是分组密码，其中的消息被分成定长的数据分组，每一分组称为 M 或 C 中的一个消息。

4.6.2 DES 的核心作用：消息的随机非线性分布

DES 的核心部分是在“S 盒函数”f 中。正是在这里，DES 实现了明文消息在密文消息空间上的随机非线性分布。

4.6.3 DES 的安全性

DES 的主要缺点：DES 的密钥长度较短。

4.7 高级加密标准

AES

4.7.1 Rijndael 密码概述

Rijndael 是分组长度和密钥长度均可变的分组密码，密钥长度和分组长度可以独立指定位 128 比特或 256 比特。

4.7.2 Rijndael 密码的内部函数

Rijndael 密码的 4 个内部函数，因为每个内部函数都是可逆的，为了实现 Rijndael 的解密，只需要在相反的方向使用他们各自的逆就可以了。

Rijndael 密码中，一个消息分组（一个状态）和一个密钥分组被分成字节。

1.内部函数 SubBytes（State）

2.内部函数 ShiftRows（State）

3.内部函数 MixColumns（State）

4.内部函数 AddRoundKey（State，RoundKey）

5.解密运算

4.7.3 Rijndael 内部函数的功能小结

（1）SubBytes 目的是为了得到一个非线性的代换密码。

（2）ShiftRows 和 MixColumns 目的是获得明文消息分组的在不同位置上的字节的混合。

（3）AddRoundKey 给出了消息分布所需的秘密随机性

4.7.4 AES 对应用密码学的积极影响

几个积极的变化：
首先，随着 AES 的出现，多重加密，加长的可变的密钥及 128，192 和 256 比特的数据分组长度为各种应用要求提供了大范围可选的安全强度。
其次，AES 的广泛使用将导致同样强度的新的杂凑函数的出现。
4.8 其他重要的分组密码算法
国际数据加密算法 IDEA
4.8.1 IDEA
1.算法原理
2.加密过程
3.解密过程
4.安全性
5.变形
4.8.2 SAFER K−64
非专用分组密码算法，算法明文密文数据分组为 64b。面向直接运算，K-64 的密钥为 64b，K-128b 的密钥为 128b。
1.算法描述 SAFER K-128
2.SAFER K128
3.SAFER K-64 的安全性
4.8.3 RC5
是一种分组长(为两倍字长 wb)、密钥长（按字节数计）和迭代轮数 r 都可变的一种分组迭代密码体制
1.算法描述
2.实现
3.安全性
4.9 分组密码的工作模式
分组密码将消息作为数据分组处理（加密或解密）
4.9.1 电码本模式
电码本模式（ECB）
对一系列连续排列的消息段进行加密（或解密）的一个最直接方式就是对它们逐个加密（或解密）。
4.9.2 密码分组链接模式
密码分组链接（CBC）运行模式是用于一般数据加密的一个普通的分组密码算法。使用 CBC 模式，输出是 n 比特密码分组的一个序列，这些密码分组链接在一起使得每个密码分组不仅依赖于所对应的原文分组，而且依赖于所有以前的分组。
4.9.3 密码反馈模式
密码反馈（CFB）运行模式的特点在于反馈相继的密码分段，这些分段从模式的输出返回作为基础分组密码算法的输入。
4.9.4 输出反馈模式
输出反馈（OFB）运算模式的特点是将基本分组密码的连续输出分组回送回去。这些反馈分组构成了一个比特串，被用作弗纳姆密码的密钥集的比特串，就是密钥流与明文分组相异或。
4.9.5 计数器模式
计算器（CTR）模式的特征是，将计数器从初始值开始计数所得到的值馈送给基础分组密码算法
第 5 章　双（公）钥密码体制

最大的特点是在采用两个密钥将加密和解密能力分开：一个公开作为加密密钥；一个为用户专用，作为解密密钥，通信双方无需事先交换密钥就可进行保密通信。

5.1 双钥密码体制的基本概念

5.1.1 单向函数

定义 5-1 令函数 f 是集 A 到集 B 的映射，用 f：A→B 表示。若对任意 $x_1 \neq x_2, x_1, x_2 \in A$，有 $f(x_1) \neq f(x_2)$,则称 f 为单射，或 1-1 映射，或可逆的函数。

F 为可你的充要条件是，存在函数 g：B→A，使对所有 x∈A 有 g[f(x)]=x

定义 5-2 一个可逆函数 f：A→B，若它满足：

(1)对所有 x∈A，易于计算 f（x）；

(2)对“几乎所有 x∈A”由 f(x)求 x“极为困难”，以至于实际上不可能做到，则称 f 为一单向函数

5.1.2 陷门单向函数

定义 5.3 馅门单向函数是一类满足：f_z：$A_z \rightarrow B_z, z \in Z$,Z 是馅门信息集

5.1.3 公钥系统

定义 5-4 对 z∈Z 和任意 $x \in X, F_i(x) \rightarrow y \in Y=X$。若

$F_j(F_i(x)) = F_i(F_j(x))$

5.1.4 用于构造双钥密码的单向函数

1.多项式求根

2.离散对数 DL

3.大整数分解 FAC

4.背包问题

5.Diffie-Hellman 问题（DHP）

6.二次剩余问题

7.模 n 的平方根问题

5.2 RSA 密码体制

5.2.1 体制

5.2.2 RSA 的安全性

1.分解模数 n

2.其他途径

3.迭代攻击法

4.选择明文攻击

5.公用模攻击

6.低加密指数攻击

7.定时攻击法

8.消息隐匿问题

5.2.3 RSA 的参数选择

1.n 的确定

2.e 的选取原则

3.d 的选择

5.2.4 RSA 体制实用中的其他问题

1.不可用公共模

2.明文熵要尽可能地大

3.用于签名时，要采用 Hash 函数

5.2.5 RSA 的实现

5.2.6 RSA 体制的推广
5.3 背包密码体制
利用背包问题构造双钥密码，只适用于加密，修正后才可用于签名。
5.3.1 背包问题
5.3.2 简单背包
5.3.3 Merkle　Hellman 陷门背包
5.3.4 M-H 体制的安全性
5.3.5 背包体制的缺陷
5.3.6 其他背包体制
5.4 Rabin 密码体制
5.4.1 Rabin 体制
5.4.2 Williams 体制
5.5 ElGamal 密码体制
5.5.1 方案
5.5.2 加密
5.5.3 安全性
5.6 椭圆曲线密码体制
与 RSA 相比，ECC 的主要优点是可以使用比 RSA 更短的密钥获得相同水平的安全性，其计算量大大减少
5.6.1 实数域上的椭圆曲线
椭圆曲线并不是椭圆。之所以称为椭圆曲线，是因为他们与计算椭圆周长的方程相似，也用三次方程来表示
5.6.2 有限域 Z_p 上的椭圆曲线
椭圆曲线密码体制使用的是变元和系数均为有限域中元素的椭圆曲线。
5.6.3 GF(2^m)上的椭圆曲线
有限域 GF(2^m)由 2^m 个元素及定义在多项式上的加法和乘法运算组成。
5.6.4 椭圆曲线密码
将 ECC 中的加密算法运算与 RSA 中的模乘运算相对应，将 ECC 中的乘法运算与 RSA 中的模幂运算相对应。
5.6.5 椭圆曲线的安全性
5.6.6ECC 的实现
5.6.7 当前 ECC 的标准化工作
1.IEEE P1363
2.ANSI X9
3.ISO/IEC
4.AISO/IEC
5.ATM
5.6.8 椭圆曲线上的 RSA 密码体制
5.6.9 用圆锥曲线构造双钥密码体制
有人提出用圆锥曲线构造双钥密码体制，但由于圆锥曲线是二次的，以证明存在有亚指数分解算法，在其上求离散对数的困难程度等价于 F_p 上的离散对数
5.7 其他双钥密码体制
5.7.1 McEliece 密码体制
提出利用纠错码构造公钥密码体制。由于纠错码依赖多余度从而造成数据扩展

，同时，又由于其密钥量太大，致使这类体制未能得到广泛研究。
5.7.2 LUC 密码体制
5.7.3 有限自动机体制
5.7.4 概率加密体制
概率加密的基本想法是使公钥体制的信息泄露为 0，即从密文不能推出有关明文或密钥的任何信息。
5.7.5 秘密共享密码体制
5.7.6 多密钥公钥密码体制
5.8 公钥密码体制的分析
主动攻击 3 种方式：
（1）选择明文攻击（CPA）
（2）选择密文攻击（CCA）
（3）适用性选择密文攻击（CCA2）

第 6 章　消息认证与杂凑函数
6.1 认证函数
6.1.1 消息加密
1.对称加密
2.公钥加密
6.1.2 消息认证码
消息认证码又称 MAC，也是一种认证技术，它利用密钥来生成一个固定长度的短数据块，并将该数据块附加在消息之后
6.1.3 杂凑函数
杂凑函数是将任意长的数字串 M 映射成一个较短的定长输出数字串 H 的函数，以 h 表示，h（M）易于计算，称 H=h（M）为 M 的杂凑值，也称杂凑码、杂凑结果等或简称杂凑。
6.1.4 杂凑函数的性质
混合变换
抗碰撞攻击
抗原象攻击
实用有效性
6.2 消息认证码
MAC 也称为密码校验和
6.2.1 对 MAC 的要求
为了获得保密性，可用对称或非对称密码对整个消息加密，这种方法的安全性一般依赖于密钥的位长。除了算法中本身的弱点外，攻击者可以对所有可能的密钥进行穷举攻击。
6.2.2 基于密钥杂凑函数的 MAC
密码杂凑函数自然而然地称为数据完整性的一种密码原型。在共享密钥的情况下，杂凑函数将密钥作为它的一部分输入，另一部分输入为需要认证的消息。
6.2.3 基于分组加密算法的 MAC
构造密钥杂凑函数的标准方法是使用分组密码算法的 CBC 运行模式。
6.3 杂凑函数
6.3.1 单向杂凑函数
6.3.2 杂凑函数在密码学中的应用
6.3.3 分组迭代单向杂凑算法的层次结构

6.3.4 迭代杂凑函数的构造方法
6.3.5 基本迭代函数的选择
1.将分组密码算法作为迭代函数
2.用 RSA 来构造迭代函数
3.背包法
4.基于胞元自动机的算法
5.专门设计的具有数据压缩的单向迭代函数
6.矩阵单向迭代函数
7.以 FFT 构造单向迭代函数
8.以有限域中元素的指数运算构造迭代函数
9.IBC-HASH 算法
10.用流密码构造杂凑函数
6.3.6 应用杂凑函数的基本方式
杂凑算法可与加密及数字签名结合使用，实现系统的有效、安全、保密与认证。
6.4MD-4 和 MD-5
该算法特别适于软、硬件快速实现。输入消息可任意长，压缩后输出为 128b
6.4.1 算法步骤
6.4.2MD-5 的安全性
6.4.3MD-5 的实现
速度：用 32b 软件易于高速实现
简洁与紧致性：描述简单，短程序可实现，易于对其安全性进行评估
6.4.4MD-4 与 MD-5 算法差别
MD-5 较 MD-4 复杂，且较慢，但安全性较高。
6.4.5MD-2 和 MD-3
6.5 安全杂凑算法
6.5.1 算法
1.主环路
2.SHA 的基本运算
6.5.2SHA 的安全性
SHA 与 MD-4 很相似，主要变化是增加了扩展变换，将前一轮输出加到下一轮，以加速雪崩效应。
6.5.3SHA 与 MD-4，MD-5 的比较
6.6 其他杂凑算法
6.6.1RIPEMD-160
修正了 MD-4 的旋转和消息的次序。
6.6.2SNEFRU 算法
对于长杂凑值，差值分析也优于穷举法
6.6.3GOST 杂凑算法
它是利用 64bGOST28147-89 分组密码构造的 256b 杂凑算法，密钥 k、消息分组 M_i 和杂凑值的长度均为 256b，是 GOST34.10.94 的一个重要组成部分。
6.6.4HAVAL 算法
是一种变长杂凑函数，是 MD-5 的一种修正形式。以 8 个 32b 连接变量，两倍于 MD-5 的杂凑值，轮数也可变。
6.6.5 RIPE−MAC

首先将消息填充为 64b 的倍数，然后划分成 64b 的组，最后在钥匙的控制下对消息进行杂凑
6.6.6 其他
利用模 n 运算构造的杂凑算法，如 MASH-1 已作为 ISO/IEC 标准（草案）
6.7HMAC
HMAC 将杂凑函数看做是“黑匣子”
第一，实现 HMAC 时可将现有杂凑函数作为一个模块，这样可以对许多 HMAC 代码预先封装，并在需要时直接使用；第二，若希望替代 HMAC 中的杂凑函数，则只需要删去现有的杂凑函数模块。
第 7 章　数字签名
7.1 数字签名基本概念
数字签名两种：
一种是对整体消息的签名，他是消息经过密码变换的被签消息整体；一种是对压缩消息的签名，他是附加在被签名消息之后或某一特定位置上的一段签名图样。若按明、密文的对应关系划分，每一种又可分为两个子类：一类是确定性数字签名，其明文与密文一一对应，它对一特定消息的签名不变化；另一类是随机化或概率式数字签名，它对同一消息的签名是随机变化的，取决于签名算法中的随机参数的取值。
7.2RSA 签名体制
1.体制参数
2.签名过程
3.验证过程
4.安全性
7.3Rabin 签名体制
1.体制参数
2.签名过程
3.验证过程
4.安全性
7.4ElGamal 签名体制
1.体制参数
2.签名过程
3.验证过程
4.安全性
7.5Schnorr 签名体制
1.体制参数
2.签名过程
3.验证过程
4.Schnorr 签名与 ElGamal 签名的不同点
7.6DSS 签名标准
7.6.1 概况
DSS 中采用的算法简记为 DSA
这类签名标准具有较好的兼容性和适应性，已成为网中安全体系的基本构件之一
7.6.2 签名和验证签名的基本框图
7.6.3 算法描述
7.6.4DSS 签名、验证框图
7.6.5 公众反应

7.6.6 实现速度
7.7GOST 签名标准
1.体制参数
2.签名过程
3.验证过程
4.安全性
5.性能
7.8ESIGN 签名体制
1.体制参数
2.签名过程
3.验证过程
4.安全性
7.9 Okamoto 签名体制
1.体制参数
2.签名过程
7.10 OSS 签名体制
1.体制参数
2.签名过程
3.验证过程
4.安全性
7.11 其他数字签名体制
7.11.1 离散对数签名体制
ElGamal，DSA，GOST，ESIGH，Okamoto 等签名体制都是基于离散对数问题。这些体质都可以归结为离散对数签名体制的特例
有关一般离散对数签名也称为广义 ElGamal 签名
7.11.2 不可否认签名
其中最本质的是在无签名者合作的条件下不可能验证签名，从而可以防止复制或散布他所签文件的可能性，这一性质使产权拥有者可以控制产品的散发。
7.11.3 防失败签名
这是一种强化安全性的数字签名，可防范有充足计算资源的攻击者。当 A 的签名受到攻击，甚至分析出 A 的秘密钥条件下，也难于伪造 A 的签名， A 也难以对自己的签名进行抵赖。
7.11.4 盲签名
有时需要对一个文件签名，但又不让他知道文件内容，把这种签名称为盲签名
7.11.5 群签名
它是研究面向社团或群体中所有成员需要的密码体制。在群体密码中，有一个公用的公钥，群体外面的人可以用它像群体发送加密消息，密文收到后，由群体内部成员的子集共同进行解密。
特点：只有群中成员能代表群体签名；接收到签名的人可以用公钥验证群签名，但不可能知道到由群体中哪个成员所签; 发生争议时，由群体中的成员或可信赖机构识别群签名的签名者。
7.11.6 代理签名
代理签名是某人授权其代理进行的签名。
有时可能需要更强的可识别性，即任何人可以从委托签名确定出代理签名人的身份。
7.11.7 指定证实人的签名

一个机构中指定一个人负责证实所有人的签名，任何成员所签的文件都具有不可否认性，但证实工作均由指定人完成，这种签名称作指定证实人的签名，它是普通数字签名和不可否认数字签名的折中。

7.11.8 一次性数字签名

若数字签名机构至多只能对一个消息进行签名，否则签名就可被伪造，这种签名被称作一次性签名体制。在公钥签名体制中，它要求对每个消息都要用一个新的公钥作为验证参数。一次性数字签名的优点是产生和证实都较快，特别适用于要求计算复杂定低的芯片卡。

7.11.9 双有理签名方案

7.11.10 数字签名的应用

第 8 章　密码协议

8.1 协议的基本概念

协议指两个或两个以上的参与者为完成某项特定的任务而采取的一系列步骤。

这个定义包涵层含义：

第一，协议自始至终是有序的过程，每一步骤必须依次执行。在前一步没有执行完之前，后面的步骤不可能执行。

第二，协议至少需要两个参与者。一个人可以通过执行一系列的步骤来完成某项任务，但它不构成协议。

第三，通过执行协议必须能够完成某项任务。

8.1.1 仲裁协议

仲裁者是某个公正的第三方。

8.1.2 裁决协议

由于在协议中引入仲裁人会增加系统的造价，所以在实际应用中引入另外一种协议，称为仲裁协议

8.1.3 自动执行协议

这种协议不需要仲裁者的参与，也不需要裁决者来解决争端。如果协议中的一方试图欺骗另一方，那么另一方会立刻检测到该欺骗的发生，并停止执行协议。

8.2 安全协议分类及基本密码协议

8.2.1 密钥建立协议

1.采用单钥体制的密钥建立协议

2.采用双钥体制的密钥交换协议

3.中间人攻击

4.联锁协议

5.采用数字签名的密钥交换

6.密钥和消息传输

7.密钥和消息广播

8.Diffie-Hellman 密钥交换协议

8.2.2 认证建立协议

1.采用单向函数的认证协议

2.字典攻击和掺杂

3.SKEY 认证程序

4.采用双钥体制的认证

5.采用联锁协议的双向认证

6.SKID 身份识别协议

7.消息认真
8.2.3 认证的密钥建立协议
1.大嘴青蛙协议
2.Yahalom 协议
3.Needham-Schroeder 协议
4.Otway-Rees 协议
5.Kerberos 协议
6.Neuman-Stubblebine 协议
7.DASS
8.Denning-Sacco 协议
9.Woo-Lam 协议
10.EKE 协议
8.3 秘密分拆协议
8.4 秘密广播协议和会议密钥分配
8.4.1 秘密广播协议
8.4.2 会议密钥分配协议
8.4.3Tatebayashi−Matsuzaki−Newman 协议
8.5 密码协议的安全性
安全漏洞的原因：
（1）协议设计者有可能误解了所采用的技术，或者不适当地照搬了已有的协议的某些特性
（2）人们对某一特定的通信环境及其安全需求研究不够
8.5.1 对协议的攻击
常用的方法是对协议施加各种可能的攻击来测试其安全度
密码攻击目标：
第一是协议中采用的密码算法
第二是算法和协议中采用的密码技术
第三是协议本身
对协议的攻击可以分为被动攻击和主动攻击
被动攻击是指协议外部的实体对协议执行的部分或整个过程实施窃听
主动攻击对密码协议来说具有更大的危险性
1.已知明文攻击
2.选择密文攻击
3.预言者会话攻击
4.并行会话攻击
8.5.2 密码协议的安全性分析
1.攻击检验方法
2.形式语言逻辑分析法

第 9 章　PKI 与 PMI
9.1PKI 的组成
1.安全策略
2.认证系统
3.密钥管理
9.1.1 实施 PKI 服务的实体

用数字签名的数字证书实现身份；用对称密码算法对要传输的信息进行加密，然后用非对称密码算法对对称密码加密再进行传输，以实现数据的保密性；用数字签名和数字时间戳的方法实现不可否认性

1.好密钥的安全生成

2.初始身份的确认

3.证书的颁发、更新和终止

4.证书有效性的检查

5.证书和相关信息的分发

6.密钥的安全存档和恢复

7.数字签名和数字时间戳的产生

8.信任关系的建立和管理

9.1.2 认证中心

1.认证中心的组成

（1）签名和加密服务器

（2）密钥管理服务器

（3）证书管理服务器

（4）证书发布和 CRL 发布服务器

（5）再现证书状态查询服务器

（6）We 服务器

2.认证中心功能的实现

（1）证书发放

（2）证书更新

[1]最重实体证书更新

[2]CA 证书更新

（3）证书注销

（4）证书验证

9.1.3 注册中心

1.注册中心简介

2.RA 的功能

3.证书注册的实现

（1）初始化

（2）初始信任

（3）注册要求

（4）私钥拥有者确认

4.技术方案

5.基础设施

6.动作管理

9.2 证书

工要证书是将证书持有者的身份信息和其所拥有的公钥进行绑定的文件。证书文件还包含签发证书的权威机构认证中心 CA 对该证书的签名。

9.2.1X.509 证书

1.密钥用途

2.扩展密钥用途

3.证书策略