普通高等教育“十一五”国家级规划教材

职业技术教育规划教材——高职·电子商务类

网络信息安全（第2版）

主编　陈月波

武汉理工大学出版社
WUTP Wuhan University of Technology Press

普通高等教育“十一五”国家级规划教材
职业技术教育规划教材——高职·电子商务类

网络信息安全

（第2版）

主　编　陈月波
副主编　马兆丰　叶忠杰

武汉理工大学出版社
武汉

内容提要

全书分为9章，在第1版的基础上，进行了全面的修订，减少了理论部分的内容，增加了实践训练的内容，使可操作性大大提高。在编写的体系上，围绕企业的桌面安全、防火墙、企业网络核心安全等主线层层展开；在编写的体例上，第1章、第9章理论内容采用传统的方法进行编写，第2章到第8章实践性强的部分，则采用项目化的方法进行编写。

全书介绍了网络信息安全基础、桌面安全、网络防火墙设置、企业网络核心安全、INTERNET安全、安全防范、网络信息安全协议与安全标准、企业VPN与网络安全、企业网络信息安全防范与立法等。

该书遵从高职高专教学规律，每章配有有针对性的实验，具有较强的可操作性。本书可以用作本、专科以及高职高专信息安全、计算机、电子商务等相关专业的教材。本书内容丰富，结构合理，同样适合广大计算机网络与信息安全爱好者和大专院校相关专业的师生阅读参考。

图书在版编目（CIP）数据

网络信息安全/陈月波主编．—2版．—武汉：武汉理工大学出版社，2009.8
职业技术教育规划教材——高职·电子商务类
普通高等教育“十一五”国家级规划教材
ISBN 978-7-5629-3038-9

Ⅰ．网…　Ⅱ．陈…　Ⅲ．计算机网络-安全技术　Ⅳ．TP393.08

中国版本图书馆CIP数据核字（2009）第151430号

出版发行：武汉理工大学出版社（武汉市洪山区珞狮路122号　邮政编码：430070）
HTTP：//www.techbook.com.cn　理工图书网
经 销 者：各地新华书店
印 刷 者：湖北恒泰印务有限公司
开　　本：787×1092　1/16
印　　张：23
字　　数：589千字
版　　次：2005年8月第1版，2009年8月第2版
印　　次：2009年8月第3次印刷
印　　数：5001～8000册
定　　价：40.00元

本社购书热线电话：（027）87397097　87394412
E-mail：quswwutp@163.com　wutp2005@126.com

前　言

随着互联网的普及，网络信息安全的重要性和对社会的影响也越来越大。通过互联网兴起的电子商务、电子支付、网络银行、网上证券、网上理财、网上保险等，使得网络与信息系统的安全与保密问题显得越来越重要。进入21世纪以来，我国的网络信息安全形势更加严峻，研究和解决我国的网络信息安全问题刻不容缓。各个高校纷纷开设信息安全专业和有关课程，培养紧缺的信息安全专业人才。

本书是在第1版的基础上，进行了全面的修订，减少了理论部分的内容，增加了实践训练的内容，使可操作性大大提高。在编写的体系上，围绕企业的桌面安全、防火墙、企业核心安全等主线层层展开；在编写的体例上，第1章、第9章理论内容采用传统的方法进行编写，第2章到第8章实践性强的部分，则采用项目化的方法进行编写。

本书的总参考学时数控制在72课时范围内。全书共9章，第1章主要介绍了网络信息安全基础，内容包括：网络信息安全概述，信息加密技术，PKI基础，数字签名与CA认证技术，数字证书，病毒基本知识。第2章介绍了桌面安全，内容包括：项目一Windows XP自带防火墙设置，项目二用TCP/IP过滤保护用户计算机，项目三通过本地安全策略提高安全性，项目四EFS加密，项目五其他安全设置等。第3章介绍了网络防火墙设置，内容包括：项目一ISA Server 2006的安装与测试，项目二ISA Server 2006的使用，项目三硬件防火墙的安装与管理等。第4章介绍了企业网络核心安全，内容包括：项目一安装企业根CA和独立根CA，项目二使用证书实现安全Web通信，项目三在企业中实现智能卡基本架构，项目四利用SUS服务统一管理企业安全更新，项目五利用组策略进行软件限制，项目六利用组策略进行证书自动化管理，项目七利用组策略进行更新管理等。第5章介绍了INTERNET安全，内容包括：项目一INTERNET安全，项目二FTP服务器安全设置，项目三E-mail安全，项目四Web安全，项目五PROXY安全等。第6章介绍了安全防范，内容包括：项目一局域网中的ARP攻击及防护，项目二常见入侵软件的使用，项目三灾难恢复等。第7章介绍了网络信息安全协议与安全标准，内容包括：项目一利用SSL协议实现Web站点服务器的安全访问，项目二利用首信易支付平台（电子钱包）进行网上购物等。第8章介绍了企业VPN与网络安全，内容包括：项目一VPN服务器设置，项目二VPN网关配置与应用，项目三SSL VPN等。第9章介绍了企业网络信息安全防范与立法，内容包括：企业网络信息安全防范，企业网络信息安全防范体系，常见的网络攻击与防范，物理安全防范策略，黑客攻击防范策略，灾难恢复，网络信息安全立法概述，我国网络信息安全立法状况。附录包括我国关于信息安全方面的立法附录等内容。

该书遵从高职高专教学规律，每章配有有针对性的实验，具有较强的可操作性。本书可以用作本、专科以及高职高专信息安全、计算机、电子商务等相关专业的教材。本书内容丰富，结构合理，同样适合广大计算机网络与信息安全爱好者和大专院校相关专业的师生阅读参考。

在本书的编写过程中，得到了武汉理工大学出版社曲生伟老师的指导，并对本书的大纲提出了许多宝贵的意见，在此深表敬意！

本书还参考了许多有关的教材和互联网信息，大部分已经列出来，对于疏忽遗漏未列出来的参考教材和网址，一并致谢并表歉意。

本书由陈月波老师主编并总撰全书，同时编写第 8 章 8.2、8.3 节和第 9 章，马兆丰老师为副主编并编写第 4 章，叶忠杰老师为副主编并编写第 1 章，张艳老师编写第 2 章、第 5 章和 8.1 节，靳静老师编写第 3 章和第 6 章，潘明风老师编写第 7 章。

编　者

2009 年 4 月

目　录

1 网络信息安全基础

1.1 网络信息安全概述

什么是网络信息？简单来说就是从网络上来的信息，即网络上传播的信息就是网络信息。

网络信息安全是一个关系到国家安全和主权、社会稳定、民族文化继承和发扬的重要问题，也是一个涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科的边缘学科。

网络信息安全的重要性已有目共睹。特别是随着全球信息基础设施和各个国家的信息基础逐渐形成，国与国之间变得“近在咫尺”，电子化信息已成为现代社会的一个重要特征。另外，由于网络信息的快速、普及，客户端软件多媒体化，协同计算，资源共享、开放，远程管理化，电子商务、金融电子化成为网络时代必不可少的一个产物。事实表明，确保网络信息的安全已经是一件刻不容缓的大事。有人预计，未来计算机网络信息安全问题比核威胁还要严重，因此，解决网络信息安全问题具有十分重要的理论意义和现实背景。

1.1.1 信息安全的含义

面对越来越严重的危害计算机网络信息的种种威胁，必须采取措施来保证信息的安全。但是现有的计算机网络大多数在建设之初都忽略了安全问题，即使考虑了安全，大部分是把安全机制建立在物理安全上。随着网络互联程度的扩大，这种安全机制对于网络信息来讲形同虚设。同时，目前网络上使用的协议，如 TCP/IP 协议，在制定之初也没有把安全考虑在内，所以网络协议本身就是不设防的。TCP/IP 协议中存在很多的安全问题，不能满足网络信息安全的要求。另外，网络的开放性和资源共享也是安全问题的一个主要根源，解决这个问题主要依赖于信息加密、用户身份鉴别、存取控制策略等各种技术手段。

网络信息的安全措施一般分为三类：逻辑上、物理上和政策上的。面对危害计算机网络信息安全的种种威胁，仅仅利用物理上和政策上的手段是十分有限和困难的，因此也应采用逻辑上的措施，即研究开发有效的网络信息安全技术，例如，安全协议、密码技术、数字签名、防火墙、安全管理、安全审计等，以防止网络上传输的信息被非法窃取、篡改、伪造，保证其保密性(Secrecy)和完整性(Integrity)；防止非法用户(或程序)的侵入，限制网络上用户(或程序)的访问权限，保证信息存放的私有性(Privacy)。除了私有性和完整性

之外，一个安全的计算机网络还必须考虑通信双方身份的真实性(Authenticity)和信息的可用性(Available)。

网络信息安全就是要保证网络上存储和传输信息的安全性。为了解决这个问题，国内外很多研究机构在这方面做了很多工作，主要有数据加密、身份认证、数字签名、防火墙、安全审计、安全管理、安全协议、IC卡(存储卡、加密存储卡、CPU卡)、拒绝服务、网络安全性分析、网络信息安全监测和信息安全标准化等方面的研究。

信息安全的主要目标是保护信息资源在其生命周期内免受毁坏、替换、盗窃和丢失。信息资源包括设备、存储介质、软件、计算机数据等。从广义来说，凡是涉及网络上信息的保密性、完整性、可用性、真实性和可控性的相关技术和理论都是网络信息安全所要研究的领域。

网络信息安全是指网络系统的硬件、软件及其系统中的数据受到保护，不因偶然的或恶意的原因而遭到破坏、更改、泄露。

网络信息安全在不同的应用环境中有不同的解释。

从用户角度来说，他们希望涉及个人隐私或商业利益的信息在网络上传输时受到保密性、完整性和真实性的保护，避免其他人或对手利用窃听、冒充、篡改、抵赖等手段对用户的利益和隐私造成损害和侵犯，同时也希望保存在计算机系统上的用户信息不受其他非法用户的非授权访问和破坏。

从网络运行和管理者角度说，他们希望对本地网络信息的访问、读写等操作受到保护和控制；避免出现陷阱、病毒、非法存取、拒绝服务和网络资源非法占用和非法控制等威胁，制止和防御网络黑客的攻击。

对安全保密部门来说，希望对非法的、有害的、涉及国家或商业机密的信息进行过滤和防堵，避免其通过网络而泄露，避免由于这类信息的泄密对社会产生危害，对机构造成经济损失。

从社会教育和意识形态角度来讲，网络上不健康的内容会对社会的稳定和人类的发展造成阻碍，因此，必须对其进行控制。

网络上信息传播安全，即信息传播后果的安全性，主要是信息过滤。它侧重于防止和控制非法、有害的信息进行传播，避免公用通信网络上大量自由传输的信息失控，本质上是维护道德、法律和国家利益。

网络上信息内容的安全，即我们讨论的狭义的“信息安全”。它侧重于保护信息的保密性、真实性和完整性，避免攻击者利用系统的安全漏洞进行窃听、冒充、诈骗等有损于合法用户的行为，本质上是保护用户的利益和隐私。

显而易见，网络信息安全的本质是在信息的安全期内保证其在网络上流动时或者静态存放时不被非授权用户非法访问。因此，网络信息安全的含义是通过各种计算机、网络、密码技术和信息安全技术，保护在公用通信网络中传输、交换和存储的信息的保密性、完整性和真实性，并对信息的传播及内容具有控制能力。

1.1.2 信息安全的要求

(1)保密性

信息不应泄露给非授权的用户、实体或进程。信息保密性是保证只有授权用户可以

访问，而限制其他用户对信息的访问。信息保密性分为网络传输保密性和信息存储保密性两个方面。就像电话可以被窃听一样，网络传输也可以被窃听，解决的办法是对传输的信息进行加密处理。信息存储保密性主要是通过访问控制来实现的，管理员对信息进行分类，分成敏感型、机密型、私有型和公用型等几类，对这些信息的访问加以不同的访问控制，如经理可以访问所有信息，一些技术人员除了敏感型信息以外都能进行访问，一般职员只能访问私有信息和公司信息。这种访问控制许多安全型操作系统都能做到，如UNIX、Windows 200×等操作系统。

保证信息保密性的一个容易被忽视的环节是人的安全意识。一个黑客可能会收买一个职员，或欺骗一个职员，从而获得机密信息，这是一种常见的攻击方式，被称为社会工程(Social Engineering)。

(2)完整性

完整性是指信息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。信息完整性的目的是保证计算机系统上的信息处于一种完整和未受损害的状态，这就是说信息不会因有意或无意的事件而被改变或丢失，信息完整性的丧失直接影响到信息的可用性。

影响信息完整性的因素很多，有人为的蓄意破坏，有人为的无意破坏，有软、硬件设备的失效，还有自然灾害等。但可以通过访问控制、备份和冗余设置来实现信息的完整性。

(3)可用性

可用性是指可被授权实体访问并按需求使用的特性，即当需要时能否存取和访问所需的信息，例如，网络环境下拒绝服务、破坏网络和有关系统的正常运行等都属于对可用性的攻击。Internet 蠕虫就是依靠在网络上大量复制并且传播，它占用大量 CPU 处理时间，导致系统越来越慢，直到网络发生崩溃，用户的正常信息请求不能得到处理，这就是一个典型的“拒绝服务”攻击。信息不可用也可能是由软件缺陷造成的，如微软的 Windows 系统总是有缺陷被发现。

(4)不可否认性

不可否认性也称不可抵赖性。在信息交互过程中，确信参与者的真实同一性，即所有参与者都不能否认和抵赖曾经完成的操作和承诺，利用信息源证据可以防止发信方不真实地否认已发信息，利用提交接收证据可以防止收信方事后否认已经接收的信息。数字签名技术是解决不可否认性的重要手段之一。

(5)可控性

可控性是人们对信息的传播路径、范围及其内容所具有的控制能力，即不容许不良内容通过公共网络进行传输。

1.1.3 网络信息的安全威胁

网络技术和应用的发展，使信息共享应用日益广泛与深入。但是信息在公共通信网络上存储、共享和传输，会被非法窃听、截取、篡改或毁坏而导致不可估量的损失。如果因为安全因素使得信息不敢放进像 Internet 这样的公共网络，那么办公效率及资源的利用率都会受到影响。任何事物总要辩证地看待，一方面，网络提供了信息资源的共享性、用

户使用的方便性，通过分布式处理提高了系统效率和可靠性；另一方面，正是这些特点增加了网络信息受到攻击的可能性。对网络信息的威胁来自很多方面，并且随着时间的变化而变化。网络信息安全威胁是指对信息构成威胁的用户、事物、想法、软件等，信息安全威胁利用系统暴露的要害或弱点，导致信息的保密性、完整性和可用性程度下降，造成不可估量的经济和政治损失。信息安全威胁有两种：无意的和有意的。无意的威胁包括人为操作错误、设备故障、自然灾害等很多不以人的意志为转移的事件，有意的威胁包括窃听、计算机犯罪等人为的破坏。当前主要的威胁来自以下几个方面：

- 自然灾害、意外事故。
- 人为行为，比如使用不当、安全意识差等。
- 黑客行为，由于黑客的入侵或侵扰，造成非法访问、拒绝服务、计算机病毒、非法链接等。
- 内部泄密和外部的信息泄密、信息丢失。
- 电子间谍活动，比如信息战、信息流量分析、信息窃取等。
- 操作系统及网络协议中的缺陷，例如 Windows 系统、TCP/IP 协议的安全问题等。

为了实现网络信息的安全，抵御上述安全威胁，更好地为人类服务，不仅要靠先进的技术，而且也要靠严格的安全管理、安全教育和法律规章的约束。

- 先进的网络安全技术是网络信息安全的根本保证。用户对自身面临的威胁进行风险分析和评估，决定其所需要的安全服务种类，选择相应的安全机制，然后综合先进的安全技术，形成全方位的安全技术系统。
- 严格的安全管理。使用计算机网络的机构、企业和单位应建立相应的网络信息管理办法，加强内部管理，建立合适的网络信息安全管理系统、安全审计体系，提高整体安全意识。
- 制定严格的法律规范体系。计算机网络是一种现代高科技的新生事物，法律规范相对滞后。许多行动无法可依、无章可循，因此导致了一段时间内对计算机犯罪处置的无序状态。因此，必须完善相应的法律和规范，同时严格执行，坚决打击这些犯罪活动，保护国家机密和用户的合法权益，使犯罪分子慑于法律规范，不敢轻举妄动。

1.1.4 网络信息安全体系

参照 TCP/IP 的层次结构，可以在不同的层次提供不同的安全性，例如，在网络层提供虚拟专用网络，在传输层提供安全套接字层服务，如表 1-1 所示。下面对不同层次的信息安全性和提高安全性的方法进行分析和论述。

表 1-1 TCP/IP 协议的网络安全体系结构的基础框架

层 名	相关安全协议
应用层	PEM MOSS PGP MINE S-HTTP SSH Kerberos SNMPv2
传输层	SSH SSL PCT TLS
网络互联层	IPv6 IPsec SKIP ISAKMP SKEME OAKLEY

1.1.4.1 IP 层的安全性

对 IP 层的安全协议进行标准化的想法早就存在。在过去十年里，已经提出了一些方

案。例如,“安全协议 3 号”(SP3)就是美国国家安全局以及标准技术协会作为“安全数据网络系统”(SDNS)的一部分而制定的,“网络层安全协议”(NLSP)是由国际标准化组织为“无链接网络协议”(CLNP)制定的安全协议标准,“集成化 NLSP”(I-NLSP)是美国国家科技研究所提出的包括 IP 和 CLNP 在内的统一安全机制。所有这些提案都大同小异。它们用的都是 IP 封装技术,本质是纯文本的包被加密,封装在外层的 IP 报头里,用来对加密的包进行 Internet 上的路由选择。到达另一端时,外层的 IP 报头被拆开,报文被解密,然后送到收报地点。

Internet 工程特遣组(IETF)责成 Internet 协议安全协议(IPsec)工作组对 IP 安全协议(IPSP)和对应 Internet 的密钥管理协议(IKMP)进行标准化工作。IPSP 的主要目的是使需要安全措施的用户能够使用相应的加密安全体制。该体制兼容 IPv4 和 IPv6,要求该体制与算法无关,即使加密算法替换了,也不对其他部分的实现产生影响。按照这些要求,IPsec 制定了一个规范:认证头(Authentication Header,AH)和封装安全有效负荷(Encapsulating Security Payload,ESP)。简而言之,AH 提供 IP 包的真实性和完整性,ESP 提供主要内容。

Internet 层安全性的主要优点是它的透明性,即安全服务的提供不需要应用程序、其他通信层次和网络部件做任何改动;缺点是 Internet 层一般对属于不同进程和相应条例的包不做区别。对所有去往同一地址的包,它将按照同样的加密密钥和访问控制策略来处理。这可能导致提供不了所需的功能,也会导致性能下降。

1.1.4.2 *传输层的安全性*

在 Internet 应用程序中,通常使用广义的进程间通信(IPC)机制来与不同层之间的安全协议打交道。在 Internet 中提供安全服务的一个想法是强化 IPC 界面,如 BSD Socket 等,具体做法包括双端实体的认证、数据加密密钥的交换等。Netscape 通信公司遵循这个思路,制定了建立在可靠的传输服务(如 TCP/IP 所提供)基础上的安全套接层协议(SSL)。SSL 版本 3(SSLv3)于 1995 年 12 月制定,它主要包含以下两个协议:

SSL 记录协议。它涉及应用程序提供的信息的分段、压缩、数据认证和加密。SSLv3 提供对数据认证用的 MD5 和 SHA 以及数据加密用的 R4 和 DES 等的支持,用来对数据进行认证,加密的密钥可以通过 SSL 的握手协议来协商。

SSL 握手协议。用来交换版本号、加密算法、(相互)身份认证并交换密钥。SSLv3 提供对 Deffie-Hellman 密钥交换算法、基于 RSA 的密钥交换机制和另一种实现名 Fortezza Chip 上的密钥交换机制的支持。

Netscape 通信公司已经推出了 SSL 的参考实现(称为 SSLref)和免费的 SSL 实现(称为 SSLeay)。SSLref 和 SSLeay 均可给任何 TCP/IP 应用提供 SSL 功能。Internet 号码分配中心(IANA)也已经为 SSL 功能的应用分配了固定端口号,例如,带 SSL 的 HTTP(https)被分配的端口号为 443,带 SSL 的 SMTP(ssmtp)被分配的端口号为 465,带 SSL 的 NNTP(snntp)被分配的端口号为 563。

微软推出的 SSLv2 的改进版本 PCT(私人通信技术)和 SSL 十分相似。其主要差别是在版本号字段的最显著位上的取值有所不同:SSL 该位取 0,PCT 该位取 1。

1996 年 4 月,IETF 授权一个传输层安全(TLS)工作组着手制定一个传输层安全协议(TLSP),以便作为标准提案向 IESG 正式提交。TLSP 将会在许多地方酷似 SSL。

Internet层安全机制的主要优点是它的透明性，即安全服务的提供不要求应用层作任何改变，而对传输层来说是做不到的。同网络层安全机制相比，传输层安全机制的主要优点是它提供基于进程对进程（而不是主机对主机）的安全服务。传输层安全机制的主要缺点就是要对传输层IPC（界面）和应用程序两端都进行修改，另一个缺点是基于UDP的通信很难在传输层建立起安全机制来。

1.1.4.3 应用层的安全性

网络层（传输层）的安全协议允许为主机（进程）之间的数据通道增加安全属性。本质上，这意味着真正的（或许再加上机密的）数据通道还是建立在主机（或进程）之间的，但却不可能区分在同一通道上传输的一个具体文件的安全性要求。比如说，一个主机与另一个主机之间建立起一条安全的IP通道，那么所有在这条通道上传输的IP包就都要自动地被加密。同样，如果一个进程和另一个进程之间通过传输层安全协议建立起了一条安全的数据通道，那么两个进程间传输的所有消息就都要自动地被加密。

如果要区别一个具体文件的不同的安全性要求，那就必须借助于应用层的安全性。提供应用层的安全服务实际上是最灵活的处理单个文件安全性的手段。例如，一个电子邮件系统可能需要对要发出的信件的个别段落实施数据签名。而低层的协议提供的安全功能一般不知道任何要发出的信件的结构，从而不可能知道该对哪一部分进行签名。只有应用层是唯一能够提供这种安全服务的层次。

在应用层提供安全服务的做法是对每个应用（及应用协议）分别进行修改。一些重要的TCP/IP应用已经这样做了。在RFC1421至RFC1424中，IETF规定了私用强化邮件（PEM）来为基于SMTP的电子邮件系统提供安全服务。

S-HTTP是Web上使用的超文本传输协议（HTTP）的安全增强版本，由企业集成技术公司设计。S-HTTP提供了文件级的安全机制，每个文件都可以被设成私人/签字状态。用作加密及签名的算法可以由参与通信的收发双方协商。S-HTTP提供了对多种单向散列（Hash）函数的支持，如MD2、MD5及SHA；对多种单钥体制的支持，如DES、RC2、RC4以及CDMF；对数字签名体制的支持，如RSA和DSS等。

Internet上一个重要的应用是电子商务，尤其是信用卡交易系统。为保证信用卡交易的安全，MasterCard公司牵头制定了安全电子付费协议（SEPP），Visa国际公司和微软（和其他一些公司一道）制定了安全交易技术（STT）协议。同时，MasterCard、Visa国际和微软联手推出Internet的安全信用卡交易服务，发布了相应的安全电子交易（SET）协议，规定了持卡人用其信用卡通过Internet进行付费的方法。

上面提到的所有这些安全功能的应用都面临一个主要的问题，就是要各自单独进行修改。赫尔辛基大学的Tatu Yloenen开发的安全Shell（SSH）实现了统一的修改手段。SSH允许用户安全地登录到远程主机上，执行命令和传输文件。实现了一个密钥交换协议以及主机及客户端认证协议。把SSH的思路再往前推进一步，就是认证和密钥分配系统。从本质上讲，认证和密钥分配系统提供的是一个应用编程界面（API），它可以用来为任何网络应用程序提供安全服务，例如，认证、数据保密性和完整性、访问控制以及非否认服务。目前已经有了一些实用的认证和密钥分配系统，例如，MIT的Kerberos（v4与v5）、IBM的Crypto Knight Network Security Program、DEC的SPX、Karlsruhe大学的指数安全系统（TESS）等，都是得到广泛采用的实例。

1.2 信息加密技术

1.2.1 信息加密技术概述

信息加密技术是一个既古老又新颖的领域。对于加密(Encryption),一般是指将一组信息(或称明文,Plaintext)经过密钥(Key)及加密函数的转换过程,变成无阅读意义的密文(Ciphertext);而接收方则将此密文经过解密(Decryption)密钥和解密函数还原成明文。其基本模型如图 1-1 所示。

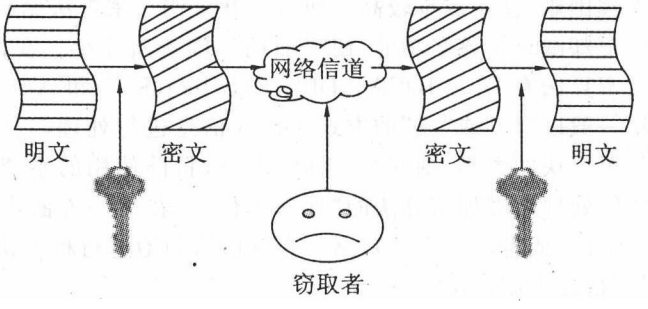

图 1-1 信息加密系统模型

在古代,因为只有少数人才有读书、写字的特权,如果一个秘密是书写下来的,那么只有数量极少的人才知道它是什么意思。

早期的加密方法非常简单。如"恺撒密码"(The Caesar Cipher),是一种简单的替换加密法:字母表中的每个字母依次都被靠后的第三个字母取代。换言之,字母 A 变成 D、B 变成 E……X 变成 A、Y 变成 B、Z 变成 C,以此类推。

到了近代,密码在技术和应用等领域都占据了一个重要的地位。在第二次世界大战中,德国使用一种名为 Enigma 的加密设备,对自己的通信进行加密。这种设备使用了一系列转轮(Enigma 机器共有 5 个,每次通信使用其中的 3 个)。这些转轮包含了字母表中的所有字母,每个都可以单独进行设置。对正常输入的文字来说,其中每个字母都被转换成看似随机的输出字符,之所以说它"看似"随机,是由于换位顺序的组合是一个天文数字。

每种通信方法的安全取决于建立通信的媒体。媒体越开放,消息落入外人之手就越有可能。现代通信方法一般都是开放和公用的。打一次电话,或者发一次传真,信号会穿越一个共享的、公共的"电路交换"网络。而发一次 E-mail 也会穿越一个共享的、公共的、包交换的 Internet 网络。在网络中,位于通信双方两个端点之间的任何一个实体均可将消息(信号)轻易拦截下来。如果要通过现代的通信技术来进行数据的保密传输,便必须采用某种形式的加密技术,防范那些"偷窥者"窃取秘密。

1.2.2 对称加密算法

1.2.2.1 基本原理

对称加密算法是应用较早的加密算法,技术成熟。在对称加密算法中,数据发信方将

明文（原始数据）和加密密钥一起经过特殊加密算法处理后，使其变成复杂的加密密文发送出去。收信方收到密文后，若想解读原文，则需要使用加密用过的密钥及相同算法的逆算法对密文进行解密，才能使其恢复成可读明文。在对称加密算法中，使用的密钥只有一个，发收信双方都使用这个密钥对数据进行加密和解密，这就要求解密方事先必须知道加密密钥。

对称加密算法的特点是算法公开、计算量小、加密速度快、加密效率高。不足之处是，交易双方都使用同样钥匙，安全性得不到保证。此外，每对用户每次使用对称加密算法时，都需要使用其他人不知道的唯一钥匙，这会使得发收信双方所拥有的钥匙数量呈几何级数增长，密钥管理成为用户的负担。对称加密算法在分布式网络系统上使用较为困难，主要是因为密钥管理困难，使用成本较高。而与公开密钥加密算法比起来，对称加密算法能够提供加密和认证却缺乏了签名功能，使得使用范围有所缩小。在计算机专网系统中广泛使用的对称加密算法有 DES、IDEA、3DES、Blowfish、RC5 和 AES 等。

对称加密算法一般以“块”或“流”的方式对输入信息进行处理，它们一般每次对一个数据块进行处理。至于块的大小，则取决于算法本身（目前使用的系统多数采用 64 位的块长度），对一个块的处理叫做加密算法的“处理单位”。在另一方面，“流加密算法”每次处理的是数据的一个位（或者一个字节），用一个键值适当地进行种子化处理，便能生成一个位流（这里的“位”指二进制的位）。

注意无论是块加密还是流加密，它们都适用于批量信息的加密处理。块加密算法可采用不同的模式工作，一种模式是每次都用同一个密钥；另一种是将上一次操作的结果“喂”给当前操作，从而将数据块链接到一起。综合运用这些模式，便可使一种加密算法变得更为“健壮”，对特定的攻击产生更强的免疫力。举个例子来说，块加密算法的基本应用就是“电子密码本”（Electronic Code Book，ECB）模式。每个明文块都加密成一个密文块，由于使用相同的密钥，相同的明文块会加密成相同的密文块，所以对一段已知的明文来说，完全能构建出一个密码本，其中包含所有的密文组合。如果知道一个 IP 数据包已进行了加密处理，那么由于密文的头 20 个字节代表的是 IP 头，所以可利用一个密码本推断出真实的密钥是什么。

在块加密算法的具体应用中，由于不能保证输入数据的长度正好为一个密码块长度的整数倍，所以根据具体的模式，需要对输入进行适当的填充。假如块的长度是 64 位，而最后一个输入块的大小仅有 48 位，那么就有必要增添 16 位的填充数据，然后才能执行加密（或解密）运算。

加密块链接（CBC）模式可取得前一个密文块，并在对下一个明文块进行加密之前，先对两者执行一次 XOR 运算（如图 1-2 所示）。假如是第一个块，那么与它进行 XOR 运算的是一个初始化矢量（Initialization Vector，IV）。IV 必须具有“健壮”的伪随机特性，以确保完全一致的明文不会产生完全一致的密文。解密过程与加密相反：每个块都会进行解密，并在对前一个块进行解密之前，对两者进行一次 XOR 运算。解密到第一个块，它同样会与 IV 进行 XOR 运算。目前使用的所有加密算法都属于“块加密算法”，采用 CBC 模式运行。

其他流行的模式包括加密回馈模式（Cipher Feedback Mode，CFM）和输出回馈模式（Output Feedback Mode，OFM），前者的前一个密文块会被加密，并与当前的明文块进行

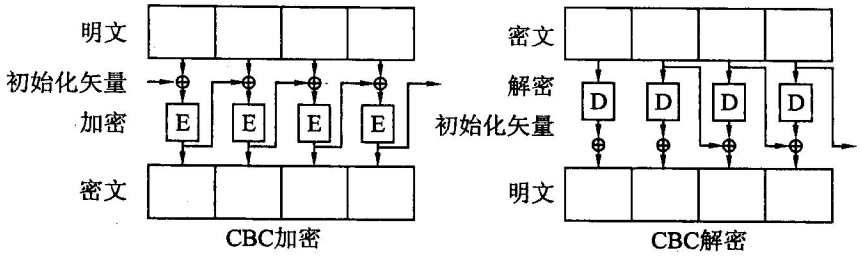

图 1-2 加密块链接方式

XOR 运算(第一个明文块只与 IV 进行 XOR 运算);后者会维持一种加密状态,不断地加密,并与明文块进行 XOR 运算,以生成密文(IV 代表初始的加密状态)。

1.2.2.2 DES 算法

数据加密标准(Data Encryption Standard,DES)是使用最为普遍的私有密钥算法。DES 算法于 1975 年由 IBM 发明并公开发表,并于 1976 年批准成为美国政府标准。DES 算法在 POS、ATM、磁卡及智能卡(IC 卡)、加油站、高速公路收费站等领域被广泛应用,以此来实现关键数据的保密,如信用卡持卡人的 PIN 的加密传输、IC 卡与 POS 间的双向认证、金融交易数据包的 MAC 校验等,均用到 DES 算法。

DES 算法的处理速度比较快。根据 RSA 实验室提供的数据,当 DES 完全由软件实现时,它至少比 RSA 算法快 100 倍。如果由硬件实现,DES 比 RSA 快 1000 甚至 10000 倍。因为 DES 使用 S 盒运算,只使用简单的表查找功能,而 RSA 却是建立在非常大的整数运算上。

DES 使用相同的加密、解密算法,密钥是任意一个 64 位的自然数。算法的工作方式决定了只有 56 位有效位(8 位用作校验)。NIST 授权 DES 成为美国政府的加密标准,但只适用于加密"绝密级以下信息"。尽管 DES 被认为十分安全,但确实存在方法可以攻破它。

通过穷尽搜索密钥空间,提供总共 2^{56}(大约 7.2×10^{16})个可能的密钥。如果每秒能检测一百万个密钥的话,需 2000 年。但有一组 Internet 用户,用了 4 个多月时间分工合作解决了 RSA DES 挑战并最终攻破了这一算法。

该小组在检验大约 18×10^{15} 个密钥后找到了正确的密钥,并恢复了明文:

Strong cryptography makes the world a safer place.

该小组采用"强行攻击"(Brute-Force)的技术,即所有参加这一挑战的计算机搜索所有可能的密钥,一共有超过 72057594037927936 个密钥。当把这一正确密钥报告给 RSA Data Security 公司时,该小组已经搜索了大约所有可能密钥的 25%。强行攻击是破译 DES 密码的通用方法,通过不同的加密分析,可以将密钥数量降至 2^{47} 个,这仍是一个很大的工程。如果 DES 使用长度超过 56 位的密钥,那么破译它的可能性几乎为零。

下面分析一下 DES 的处理过程。DES 加密算法的数据流程如图 1-3 所示。该算法输入的是 64 位的明文,在 64 位的密钥控制下,通过初始换位 IP 变成 $T_0=IP(T)$,再对 T_0 经过 16 层的加密变换,最后再通过逆初始变换得到 64 位的密文。密文的每一位都是由明文的每一位和密钥的每一位联合确定。DES 的加密过程可分为加密处理、加密变换

和子密钥生成几个部分。下面分别进行分析。

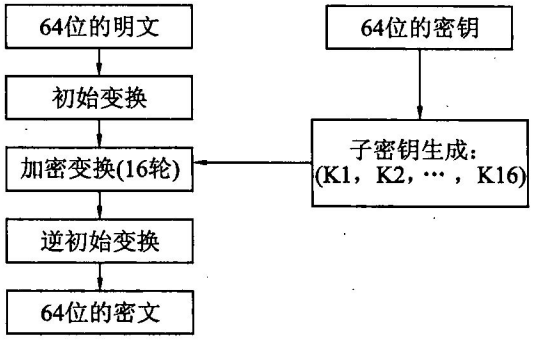

图 1-3 DES数据加密基本流程

1.2.2.3 国际数据加密算法

国际数据加密算法(IDEA)是加密算法中最好、最安全的一种。由瑞士联邦科学技术学院(SFT)的 Xuejia Lai 和 James Massey 提出。IDEA 使用 3 个 64 位的块，以进一步防范加密分析过程。IDEA 使用了密码反馈操作，使得算法强度更高。在这种模式下，密文输出也被用来作为加密运算的输入。

IDEA 的另一个重要特点是它的密钥长度为 128 位。正如我们见到的 DES，密钥越长，其保密性越高。当试图破译 IDEA 时，它和 DES 一样没有泄露任何明文组成的信息。IDEA 能够将 1 位的明文扩散到多个位的密文中去，以达到完全隐藏明文的统计结构。

1.2.2.4 CAST 算法

CAST 算法由 Carlisle Adams 及 Stafford Tavares 开发。该算法使用 64 位的块长及 64 位的密钥，它使用 6 个 8 位输入 32 位输出的 S 盒，这些 S 盒的结构确实太复杂，已经超出了本书的范围。想得到更多关于此方面的信息，可参考相关书籍。

CAST 加密过程是将明文块分为两个子块：左子块和右子块。该算法有 8 圈，每圈一半明文经过“f”函数运算与某一密钥组合，然后将结果与另半部分异或，左子块形成新的右子块，原来的右子块变为左子块。经过 8 次这样的运算之后，这两部分的输出就是密文了，可见这种运算十分简单。表 1-2 给出了一些加密所用的函数。

表 1-2 CAST 中将明文加密成密文所用的函数

序号	函　数
1	把 32 位输入分成 4 个 8 位组：a,b,c,d
2	将 16 位子密钥分成两个 8 位子密钥：e,f
3	将 a 通过 S 盒 1，b 通过 S 盒 2，c 通过 S 盒 3，d 通过 S 盒 4，e 通过 S 盒 5，f 通过 S 盒 6 进行处理
4	将 6 个 S 盒的输出异或得到最终的 32 位输出

S 盒，也称为选择盒，是一组高度非线性函数。在 DES 中 S 盒看起来像一组表，它们是 DES 真正执行加密、解密运算的函数部分。

1.2.2.5 Skipjack 算法

Skipjack 算法是 NSA 为 Clipper 芯片开发的加密算法。它被确定为美国政府机密，