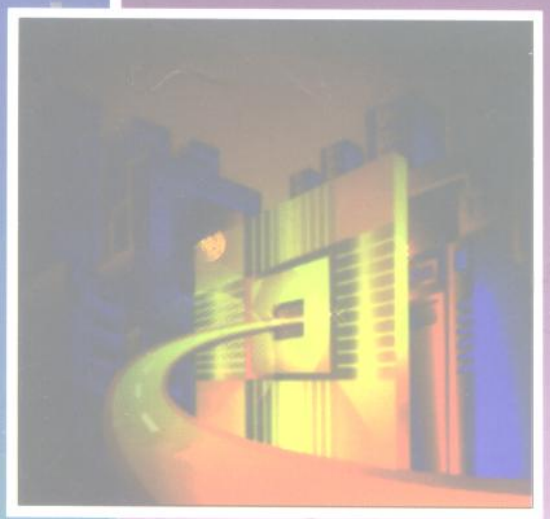
高等学校
电子信息类 规划教材

通信网的安全
—— 理论与技术

国家自然科学基金
原电子工业部通信预研基金
国家密码发展基金
西安电子科技大学 教材基金和研究生教材基金
资助



王育民
刘建伟 编著

西安电子科技大学出版社

高等学校电子信息类规划教材

通信网的安全
——理论与技术

王育民　刘建伟　编著

西安电子科技大学出版社
1999

内容简介

本书研究和讨论通信网安全的理论与技术。本书第1章介绍通信网安全概论，其余各章分为三大部分。第一部分为第2～5章，介绍密码学的基础知识，包括古典密码、信息论、计算复杂度、流密码、分组密码和双钥密码的原理和算法以及一些新的密码体制。第二部分为第6～9章，介绍认证理论与技术，包括认证、认证码、杂凑函数、数字签字、身份证明、认证和协议的理论与算法。第三部分为第10～13章，介绍通信网的安全技术，包括网络安全的基础知识、网络加密方式与密钥管理、实际系统的安全与安全管理技术。有关章末给出所需的数学基础知识。书末给出一些重要的信息安全技术标准和有关的参考文献。

本书可作为有关专业大学生和研究生的教材，也可作为通信工程师和计算机网络工程师的参考读物。

通信网的安全
——理论与技术

王育民　刘建伟　编著

责任编辑　李纪澄　马乐惠
出版发行　西安电子科技大学出版社
（西安市太白南路2号）
邮　编　710071
电　话　(029)8227828
经　销　新华书店
印　刷　空军电讯工程学院印刷厂
版　次　1999年4月第1版
1999年4月第1次印刷
开　本　787毫米×1092毫米　1/16　印张 41.5
字　数　990千字
印　数　1～4 000册
定　价　42.00元
ISBN 7-5606-0711-X/TN·0129

序

近年来，由于信息高速公路在我国大力宣传与倡导，信息技术与信息产业日益受到重视。在信息的传输与处理的过程中，有关如何保护信息使之不被非法窃取或窜改，亦即信息的认证与保密的问题，自然成为历来人们关注的问题。因此密码学理论与技术自然成为信息科学与技术中的一个重要的研究领域。

自从 70 年代中期 W. Diffie 与 M. Hellman 提出公开密钥密码学以来，在密码学领域中爆发了一场深刻的革命。从那时起，密码学理论与技术不再是仅为少数人掌握的服务于政府、军事及外交领域的神秘学科。特别是由于商业与银行业越来越国际化，密码学的理论与技术在民用及经济领域获得了广泛的应用。在今天"制信息权"已经是衡量一个国家实力的一个重要标志。如何保护自己的信息资源以及如何获取对方的信息资源，这正是当代以密码技术为中心，包括微电子学、通信、计算机科学及数学等多学科的一个综合研究体系，它能体现一个国家在高科技领域的强大实力。

在当前，由于 Internet 及各种局域网在我国的开通，银行业务中电子支付系统的广泛应用，使通信网安全的理论与技术成为至关重要的一个新兴研究领域。在这一热点领域中，由于涌进了包括网络工程师，计算机软、硬件工程师在内的大量新军，他们均需要掌握这一学科的基本原理及安全产品研制、开发技术。在当代的专著及文献中，大量侧重在理论方面，对于广大技术工作者显得晦涩难懂。有一本叫《应用密码学》的书(Applied Cryptography，Bruce Schneier 著)，是一本很好的入门书，可惜本书对于密码学的原理与概念的阐述又过于简单，作为手册使用倒是很不错的。

王育民教授与刘建伟博士合著的《通信网的安全——理论与技术》一书，一方面全面而系统地阐述了密码学与信息安全领域的有关理论与概念，另一方面特别在通信网安全方面花了足够的篇幅来阐述有关的原理与实际技术问题。从通信网的安全技术基础，网络加密方式与密钥管理，到目前已知的实际通信网络系统的安全性以及通信网的安全管理技术，做了全面深入的讨论。本书所涉及到的内容包括当前密码学与信息安全的最新研究成果。总之，这是一本理论与技术相结合，深入浅出且引人入胜的好书。它对于有关微电子学、通信及计算机科学与工程领域的广大研究生及高年级大学生均为一本值得推荐的教材和参考书。同时对于密码学及信息安全领域的研究工作者，对于网络工程师，计算机软、硬件工程师，也是一本有价值的参考书。

肖国镇

1998 年 3 月 13 日

前　言

自古以来，通信安全保密在国家的军事和安全部门一直受到十分广泛的关注。在通信安全、保密、密码分析上的优势，被认为是赢得历史上许多主要军事冲突(包括二次世界大战)胜利的关键因素之一。历史上的战争，特别是两次世界大战，对于保密学的理论与技术的发展起了巨大的推动作用。纵观历史，这门科学走过了一段漫长的道路。从原始的手工作业到采用机械设备和电器机械设备，进而发展到今天的以使用电子计算机及微电子技术为标志的电子时代。

1949 年 C. E. Shannon 发表了《保密系统的通信理论》，1976 年 W. Diffie 与 M. E. Hellman 发表了《密码学的新方向》，这两篇重要论文和 1977 年美国公布实施的《数据加密标准(DES)》，标志着保密学的理论与技术的划时代的革命性变革。这主要表现在以下几个方面：第一，传统的密码体制的主要功能是信息的保密，而双钥(公钥)密码体制的出现，不但赋予了通信的保密性，而且还提供了消息的认证性。第二，这种新的双钥密码体制无需事先交换秘密钥就可通过不安全信道安全地传递信息，大大简化了密钥分配的工作量。双钥密码体制和 DES 适应了通信网的需要，为保密学技术应用于商业领域开辟了广阔的天地。第三，双钥密码体制的出现和 DES 的设计充分体现了 Shannon 信息保密理论所阐述的设计密码的思想，使密码的分析和设计提高到新的水平。第四，保密学涉及到数学学科(诸如数论、抽象代数、复杂性理论、组合算法、概率算法以及代数几何等)、信息论、计算机科学与微电子学等广泛的科学领域。

自从 1956 年第一个计算机网络建立以来，网络技术得到了极其迅速的发展。今天，各种通信网络，如用于数据传输的分组交换网络(PSDN)、用于话音通信的公共业务电信网络(PSTN)、综合业务网络(ISN)、(陆地或卫星)移动通信网络等，使我们的生活方式和工作方式发生了巨大的变化。我们正在步入一个崭新的信息社会。随着信息化社会的发展，信息在社会中的地位和作用越来越重要，每个人的生活都与信息的产生、存储、处理和传递密切相关，信息的安全与保密问题成了人人都关心的事情，这使得保密学脱去了神秘的面纱，成为大家感兴趣并为更多人服务的科学。信息空间中的侦察与反侦察、截获和反截获、破译和反破译、破坏和反破坏的斗争愈演愈烈。军事上的电子对抗在 1991 年初的海湾战争中发展成为空前的大规模电子战，商业上的情报战也随着 Internet、Intranet、Extranet，特别是电子商务的发展而步入了新的阶段。近年来，在网络上所进行的各种犯罪活动出现了逐年上升的趋势，由此所造成的经济损失是十分巨大的。信息空间中的信息大战正在悄悄而积极地酝酿中，小规模的信息战一直在不断地出现、发展和扩大。信息战是信息化社会发展的必然产物。在信息战场上能否控制和取胜，是赢得政治、外交、军事和经济斗争胜利的先决条件。因此，信息系统的安全保密问题已成为影响社会稳定和国家安危的战略性问题。

当今密码学和信息安全保密技术已逐步得到广泛的重视，相应的保安软、硬件已逐渐

形成一个新的产业，其中包括认证、加密、访问控制、防火墙、抗病毒等方面的产品。信息安全保密技术在军事系统、政府机构、金融系统、医疗保健、通信网络、教育系统、制造业等方面开始得到广泛应用。

为了培养适应信息社会人才的需求，国内许多院校已在信息与通信工程、计算机等有关专业开设了密码学或数据安全等课程，有的院校还设置了密码学的博士、硕士点，以培养这方面的高级人才。本书就是为适应这一新形势，在多年的教学和科研工作的基础上，参考了国内外有关著作和最新文献，特别是参考了 Schneier、Massey、Stinson、Menezes 和 Stallings 等人的著作写成的。希望本书能对培养密码学和信息安全技术方面的人才有所帮助。

本教材系按原电子工业部《1996～2000 年全国电子信息类专业教材编审出版规划》，由全国电子信息类通信和信息工程教学指导委员会编审、推荐出版的一本国家级重点教材。本教材由西安电子科技大学王育民、刘建伟编著，由西安电子科技大学肖国镇教授任主审，通信和信息工程教学指导委员会李晖委员任责任编委。

本教材参考时数为 50 学时。本书第 1 章介绍通信网安全概论，其余各章分为三大部分。第一部分为第 2～5 章，介绍密码学的基础知识，包括古典密码、信息论、计算复杂度、流密码、分组密码和双钥密码的原理和算法。第二部分为第 6～9 章，介绍认证理论与技术，包括认证、认证码、杂凑函数、数字签字、身份证明和认证协议的理论与算法。第三部分为第 10～13 章，介绍通信网的安全技术，包括网络安全的基础知识、网络加密方式与密钥管理、实际系统的安全与安全管理技术。书末给出最基本的和最新的参考文献。

本教材包括全面的密码学理论与通信网络安全技术方面的知识，篇幅较大，不可能在 3 个学分 50 学时内全部授完，可根据不同专业课程设置的需求进行选取。

在长年不断举办的编码和密码研讨班中，作者不断得到参加讨论班的师生们的启发和帮助，特别是得到肖国镇教授和王新梅教授的许多鼓励、支持和帮助，在本书出版之际，向他们致以真诚的谢意。

本教材由王育民主持编写，第 2～8、11 和 12 章由王育民编写，第 1、9、10、13 章由刘建伟、王育民共同编写。在近三年的写作过程中曾得到很多研究生的大力支持，朱华飞、杨波、孙晓蓉、刘胜利、田建波、郑东、张彤、王常杰、吴克颖等仔细地阅读了有关章节的初稿，改正了不少错误，作者向他们致以衷心的感谢。黄正学女士夜以继日地工作，打印了本书的大部分手稿，绘制了相当部分的图表，进行了大量艰苦而繁琐的校对工作，没有她的全力支持与帮助，本书第一作者很难想象有勇气完成这一工作。

肖国镇教授在百忙中担任本书的主审，为提高本书的质量做了重要贡献。

本书得到了国家自然科学基金、原电子工业部军事通信预研基金、国家密码发展基金以及西安电子科技大学教材建设基金和研究生教材建设基金资助。

西安电子科技大学出版社原社长李纪澄编审和编辑部副主任马乐惠作为本书的责任编辑，为本书的出版付出了辛勤而有效的劳动，西安电子科技大学出版社对本书的出版给予了大力支持，对此我们表示诚挚的感谢。

作　者

1998 年 10 月

于西安电子科技大学

目　录

1

第　章　通信网络安全概论

在本章中，我们介绍以下基本概念：① 开放(分布)网络环境；② 对网络安全的需求；③ 通信网络的安全策略；④ 安全威胁及防护措施；⑤ 通信网络中的五个基本的安全业务，即认证、访问控制、保密性、数据完整性以及服务的不可否认性；⑥ 开放系统互联(OSI)基本参考模型及 TCP/IP 协议。

1.1　开放(分布)网络环境

计算机应用的深度与广度的扩展，是与数据处理方式和计算环境的演变密切相关的，其历程大体可以分为以下四个阶段：

(1) **单机环境**(Monolithic Mainframe Environment)。在单机环境中，各种应用软件都设计成在带有终端和外设的单个主机上执行。它存在的主要问题是，在一种机器上开发的应用软件都需要经过或多或少的修改方可在异种机上运行。

(2) **网络环境**(Networked PC and Mainframe Environment)。在单机环境中加入个人计算机和网络，构成所谓的网络计算机环境。它虽然解决了单机环境中存在的某些问题，却又带来了更多复杂的问题。

(3) **分布式环境**(Distributed Computing Environment)。随着计算机软、硬件技术的发展，在网络环境的基础上，又产生了分布式计算环境。它具有多个处理部件合作自治、并行执行、分布式控制和系统资源透明性。一个应用不仅仅局限于在单机上执行，而是计算具有空间(地理位置)的分布性，人和机器相互为完成某个任务而协调工作。

(4) **协同计算环境**(Cooperative Computing Environment)。协同计算环境是由相应联网的、用户透明的计算机组成的一种计算环境。该环境中，可容纳不同厂商生产的各种类型的计算机，好像将它们集成为单机而进行操作，不论它们是由哪家制造商生产的，也不论它们使用了何种操作系统、数据库，用户都可以方便地存取网络上任何地方的信息，充分利用系统资源。

1.1.1　开放系统的基本概念

开放系统是计算机软、硬件及网络技术发展的必然产物，是人们在当前软、硬件环境下对计算环境新的、更高的要求。其产生的主要原因是计算环境的发展和协同计算的要求，前者为它的产生提供了可能性，而后者则说明了它产生的必要性和迫切性。

所谓开放系统，是指计算机和计算机通信环境，根据行业标准的接口所建立起来的计算机系统。在这样一个开放性系统中，不同厂商的计算机系统和软件都能互相交换使用，并能结合在一个集成式的操作环境里。要达到这样的目标，惟有依赖于标准的接口，使计算机系统具有可移植性、互操作性和可伸展性，可将操作系统或应用软件放在不同厂商的各种型号的计算机上使用，并且可以相互交换信息。

计算机具有可移植性和互操作性时，便可以为计算机用户带来下述好处：

(1) 保障系统原有投资，便于更换计算机硬件或软件厂家，节省了培训和维护费用；便于扩充系统，随时可从市场上采购所需的软、硬件；可充分利用已有的应用软件和快速集成新技术，便于集成不同销售商的产品。

(2) 促进软、硬件技术公开和标准化，促进供应商的竞争并不断降低软、硬件价格；

(3) 便于对不同厂商的计算机系统进行集成，不但解决商务方面的问题，而且能使用户抓住一切有利机会，不断利用新技术来加强系统功能，使系统具有更强的处理能力，达到最佳服务。

1.1.2 开放系统的特征

开放系统是以被广泛采用的各类标准(事实上标准、工业标准、国家标准、国际标准)可以共享的技术标准以及有完整定义的开放标准为基础的。目前，虽然还没有公认一致的确切定义，但可以肯定地说，相对于封闭的专用系统，它具备以下特征：

(1) **符合各类标准**(事实上标准、工业标准、国家标准及国际标准)。根据标准化的程度确定其开放的程度。

(2) **技术公开**。根据技术公开的程度，可见系统分成私有的、OBM 控制的、集团控制的和完全公开的。提供源代码是技术公开的重要方式。

(3) **可移植性**(Portable)。同一软件可以在不同计算机上运行，并且同一软件在不同计算机上进行移植时不需要做任何修改。可移植性要求不同计算机环境提供软件运行的界面是相同的，相同的界面能把硬件平台及操作系统不同之处屏蔽起来。

(4) **兼容性**(Compatible)。应用程序不加改动就可以在任何类型的计算机上运行，包括源代码和目标代码级兼容。

(5) **互操作性**(Interoperation)。互操作性是指不同系统间可以方便地相互连接，或者指不同计算机以及不同应用程序能在一个网络中交换信息、协同工作；每个用户作为网络的一个节点，都能够存取网络上的数据、调用应用程序，从而充分共享系统的资源。

(6) **可伸展性**(Scalable)。可在不同规模、不同配置的硬件环境下运行，在不同档次的计算机运行应用程序，其性能与硬件平台的性能成正比。若在现有的计算机系统中多加几个处理器，或把同一程序移到功能更强的计算机上运行时，应用程序的性能呈线性增长。这意味着应用程序能充分地调度硬件平台的所有处理器资源及其系统功能，从而便于扩充系统规模和运行环境。

1.1.3 标准

所谓“标准”，是指做某些事情时通常或优先采用的方式、方法。无规矩不能成方圆，离开标准不能成大器。通常人们认为标准化就表示相同性，这种说法意味着标准化会导致

大量生产的产品无法显示自我的特色。

其实，以计算机工业的标准来说，绝不会导致相同性。相反，它们会使可行的计算机方案更加丰富、多样化，更为适用。因为标准只针对各种硬件和软件组成元素的界面，标准只定义哪些服务是需要的，并不定义这些服务是如何实现的，因而，标准仍然留给厂商相当的自由度来发展自己。

尽管从词义上看，网络安全与开放系统似乎是矛盾的，但事实并非如此。开放系统的概念代表了购买者多年来对封闭、独立的计算机系统，以及对通信硬件和软件经销商们所寄予的良好愿望。人们总期望可以自由地选择经销商来购买不同的系统部件，而这些部件可以有机地组合起来以满足购买者的需要。因此，开放系统的发展与广泛应用与许多标准的制定密切相关。

计算机系统的联网是与开放系统并肩发展的。开放系统的标志是**开放系统互联模型**(Open System Interconnection Model)的提出。自 70 年代以来，这个模型得到了不断的发展和完善，从而成为全球公认的计算机通信协议标准。除了 ISO 的标准之外，另外一些标准化组织也建立了开放系统的许多网络协议。最为有名的当属 Internet 协会，它提出了著名的 TCP/IP 协议。通过这些围绕开放系统互联所开展的标准化活动，使得不同的厂家所提供的设备进行互联成为可能。

将安全保密措施纳入开放网络系统中是一个比较新的尝试。事实证明，这是一项十分复杂的任务。我们之所以说它复杂，主要是因为它代表了两种技术的完美结合——安全技术的应用和通信协议的设计。为了给开放系统提供安全保证，就必须将安全技术与安全协议相结合，而安全协议则是一般的网络协议的重要组成部分。

当前，我们需要做的工作是要在下面的三个较宽的领域内，设计或建立一些兼容的，或者作为补充的标准：① 安全技术；② 一般用途的安全协议；③ 特殊用途的安全协议，如银行、电子函件等应用。

与以上领域有关的标准主要来自以下四个方面：

(1) 面向信息技术的国际标准。它是由以下组织建立：国际标准化组织(ISO)，国际电子技术协会(IEC)，国际电信联合会(ITU—International Telecommunication Union，原称 CCITT)以及电器与电子工程师协会(IEEE)。

(2) 有关银行方面的标准。它或者是由 ISO 国际性地开发的，或者是由美国国家标准协会(ANSI)面向美国国内的应用而开发的。

(3) 有关国家政府的某些标准。它是由各国政府制定的。

(4) Internet 标准。它是由 Internet 协会开发的。如美国联邦信息处理标准(FIPS)，美国国家标准技术学会(NIST)，美国国家安全局(NSA)，美国计算机安全与保密顾问委员会(CSSPAB)，IAB(Internet Architecture Board)。

本书对以上组织所开发的与安全有关的标准进行了讨论。

1.1.4 因特网与内域网络

因特网(Internet[①])是一个全球性的网络。在这个大网络里，各种不同类型的计算机通过统一的网络协议和通信协议(TCP/IP)连接在一起进行交流，并共享信息资源和计算机资源。任何人与网络连接，使用电子函件(E-mail)、文件传送协议(FTP)、远程登录(Telnet)、地鼠(Gopher)、新闻组(Newsgroup)和浏览器(Browser)等其中的任何一项服务，都可成为 Internet 的用户。

Internet 的起源可以追溯到"冷战"年代。20 世纪 60 年代，美国的兰德公司就如何建立一个能在"核袭击"后，继续保持通信联络功能的系统进行了研究，提出了一个没有中心交点的网络系统。即在一个假设不可靠的网络里，所有节点都处于同等地位。每一节点均可产生、传递和接收信息，而信息本身经过分包编址后，分别经由不同节点传送至预定的接收地点，接收方再按地址把所收到的信息包组合还原成完整的信息。

1968 年，英国国家物理实验室建立了第一个基于兰德理论的测试网络。次年，美国国防部高级计划管理局建立了 ARPAnet，即 Internet 的前身。1973 年运行时仅连接了四所大学的科研机构的四台计算机。1983 年，在 ARPAnet 上成功地运行了 TCP/IP 协议。加州伯克利分校又将 TCP/IP 纳入 BSP UNIX 系统而开始在民间推广，诞生了以分组交换为基础的 Internet。从此，科研界开始采用互联网络，许多协议开始形成，并发展成为标准。从 90 年代初，商业界的介入为因特网的发展注入了巨大的原动力，并逐步发展成为一个全球性的网络。在传统的电子函件、文件传送协议、远程登录、地鼠和新闻组等应用的基础上，开发了一大批简单易用、功能性强的软件和服务。特别是万维网 WWW(World Wide Web)的出现，更为因特网带来了无限生机。万维网是一个无终结的网络超文本系统。文件中的联系可以追溯到地球另一边的计算机中的文件。万维网可作为 WAIS、FTP、Gopher、Telnet 以及 Usenet news 等其它信息服务的一个统一的界面。同时，万维网可以传送图像、声音、录像和超文本标记语言等任何类型的数据。万维网基本上是根据客户软件设计的，浏览器就是这样一种客户软件。据统计，到 1996 年 7 月，在 Internet 上已有 1 288.1 万个主机和 23 万个万维网。至于究竟有多少人使用网络，已无法给出确切的数目。

Internet 已成为全球信息基础设施(GII)的骨干网，它是一种传统媒介无法比拟的新的传播手段，诸如多媒体的传送功能，快速的信息传递，大容量的信息交换，全球性的覆盖范围以及较低的传播成本等。人们把 Internet 看成是第二次信息革命的象征，并认为 Internet不仅将彻底改变信息产业的运行方式，而且将影响世界上大多数行业产业的运行方式，从而导致一场新的产业革命。

Internet 为人类交换信息，促进科学、技术、文化、教育、生产的发展，对提高现代人的生活质量提供了极大的便利，但同时也对国家、单位和个人的信息安全带来极大的威胁。由于因特网的全球性、开放性、无缝连通性、共享性、动态性发展，使得任何人都可以自由地接入 Internet，其中有善者，也有恶者。恶者会采用各种攻击手段进行破坏活动。

在 Internet 这个跨国、跨洲、覆盖全球、无所不包、有着数以亿计用户的网络上，要想

---

① Internet 的原译名为国际互联网络，在 1997 年 7 月 18 日全国科学技术名词审定委员会颁布的英文名词的中文译名中，Internet 译成因特网。

进行集中统一管理、控制通信路由选择、追踪和监控通信过程、控制和封闭信息流通、保证通信的可靠性和敏感信息的安全保密、提供源和目标的认证、实施法律意义上的公证和仲裁，即使不是不可能的，也是极难实现的。对此严峻现实需要有清醒的认识。提高自卫能力，除了加强制度、法规等管理措施外，还要以现代化安全保密科学知识武装自己，强化我们信息系统的安全保密能力，这是在现代国际性信息大社会中生存的必由之路。

所谓内域网(Intranet)，就是在企业内部的网络上，使用 Internet 技术的产物。我们常用“内域网”这个术语表示从全球国际网络信息空间(Cyberspace)中隔离出来的较小的专用信息空间。Intranet 可以是一个局域网(LAN)，也可以是一个广域网(WAN)。内域网是由企业、机构、城市甚至国家采用国际互联网络技术建立的一种虚拟的专用网络。利用防火墙、加密技术以及精心设计的保密安全管理措施，可以把这种专用网络与 Internet 隔离加以保护。大量的通讯、信息、交互都在内域网中进行处理。当需要的时候，这些数据可以进入 Internet 空间，与其它内域网和国际互联网络用户相连接，使它充满了生机和活力，为公司和单位信息的散播和利用提供了极为便利的条件。浏览器为网上用户提供信息，服务器对网络进行管理、组织和存储信息，并提供必要的安全服务。

内域网是 Internet 应用中增长最快的一部分。许多主要跨国企业都在利用自己的内域网把它们在世界各地的办公室连接起来，从而大大地减少了公司在通讯和运作费用上的开支。

Intranet 和 Internet 虽然字面上很相像，却有很大的区别：

(1) Internet 只有一个，任何连入 Internet 的计算机和网络都成为 Internet 的一部分，整个 Internet 是一个开放的整体；而 Intranet 则是每个企业、单位单独拥有的，它不对外或有条件地对外界开放，是一个半封闭甚至是全封闭的集中式可控网。

(2) Internet 的安全机制很松散，资源共享和开放是其特点，其内容基本上不具备商业价值，它可谓是一个巨型知识库和广告栏；而 Intranet 中则存有大量的单位内部的敏感信息，具有极高的商业、政治和军事价值，其安全保密性至关重要，Intranet 决不接收任何未经授权的访问。

(3) Internet 没有统一的管理，各节点只负责自己的维护；而 Intranet 的管理是集中的、可控制的。

如何解决 Intranet 与 Internet 之间的连通性，为用户提供应有的服务，同时又能保证 Intranet 内部资源和信息的安全性，这是 Intranet 的一个非常关键的技术，也是它的一个难点。各国都在大力进行研究和开发各种具有防火、过滤功能的安全服务器、桌面系统、管理工具等。这种内域网模式被商业用户公认为是一种最有效地利用 Internet 技术的模式。

1.2　对网络安全的需求

在今天的计算机技术产业中，网络安全是急需解决的最重要的问题之一。由美国律师联合会(American Bar Association)所做的一项与安全有关的调查发现，有 40%的被调查者承认在他们的机构中曾经发生过计算机犯罪的事件。1995 年 1 月病毒数已增至 6 000，且每年要增加 40%。1992 年伪造支票造成的金融服务系统的损失为 10 亿美元，信用卡伪造所造成的损失达 35 亿美元。报道的黑客入侵事件在 1990 年为 252 起，1994 年增至 2 341

起。据美国 FBI 估计，计算机网每被攻破一次造成的损失为 50 万美元，而一个大银行的数据中心停机一秒钟的损失为 5000 美元[Ahuja 1996]。这些数字所显示的仅仅是美国网络安全犯罪所造成的真正损失的一小部分。许多机构还未意识到在他们的机构中存在有计算机犯罪。此外，即使发现了犯罪事件，许多机构也不愿意公开它们的存在。据专家估计，由计算机犯罪所造成的实际的经济损失每年将高达 150 亿美元。

信息、信息资产以及信息产品对于我们的日常生活及我们所生活的这个世界是至关重要的。加强网络安全的必要性可以从具体发生的安全事件中得到证明。另一方面，我们注意到公开报道的安全事件实际上只占很小的比率。人们对所发生的涉及安全的事件不愿进行宣扬的原因有很多。在政府部门中，对有关安全漏洞及系统脆弱性的信息泄露是受到严格控制的，与安全有关的信息也是严加保密的，因为一旦公开了这些信息，敌方就会利用这些信息来入侵其它类似的系统，从而给这些系统带来潜在的威胁。在商业市场上人们不愿公开与安全有关的信息也是出于自身利益的考虑。例如，银行及其它金融机构都不愿公开承认它们的系统中存在有安全问题，因为公开其安全问题会使用户对其在保护他们的财产方面的能力产生怀疑，从而将他们的资金或资产转移到其它金融机构或银行。造成这种对安全信息进行封锁的环境还受到来自于法律和潜在损失的影响。例如，若某个公司保存有许多用户的信息，有关这些信息的任何非授权的泄露都要承担法律责任。所以一旦该机构的计算机系统被侵入而造成所保护信息的泄露，公司将不会公开承认信息的丢失。虽然在政府部门和商业部门中对所发生的安全事件的报道有着极其严格的限制，但是今天在我们的日常生活中到处都可以见到大量的计算机和计算机网络，这一现实表明对安全事件发生的信息进行全面的保护与限制是不可能的。

在本书中，我们主要讨论与通信网络有关的安全问题。网络安全事实上可以更广泛地定义为“通信安全”，加密仅仅是通信安全的一个方面。其实，安全问题涉及很宽广的技术领域，而这些技术的广泛应用直至今天才成为可能。考虑到在现实中存在着各种强有力的密码分析方法，人们不得不考虑采用复杂的防护措施的成本。然而，由于通信技术的发展存在下面三种主要趋势，使人们对成本的考虑已放至次要的地位，而将通信安全方面的考虑提高到越来越重要的位置上。

(1) 系统互联与网络互联数量的日益增长，使任何系统都潜在地存在着已知或未知用户对网络进行非法访问的可能性。

(2) 人们越来越多地使用计算机网络来传送安全敏感的信息。例如，人们用计算机网络来进行电子资金传递(EFT)、商业数据交换、政府秘密信息传递以及产权信息的交流等。

(3) 对攻击者来说，可以得到的技术越来越先进，并且这些技术的成本在不断地下降，从而使密码分析技术的工程实现变得越来越容易。

网络安全的根本在于保护网络中的信息免受各种攻击。因此，我们有必要对信息的价值、机密信息、产权信息及其敏感性，以及信息安全威胁及其分类加以讨论。

1.2.1 信息业务及其价值

与传统的邮政业务不同，信息传输、信息协同以及规划是通过电子和光子来完成的。现代的信息系统可以让人类实现面对面的电视会议和电话通信。然而，流过这些信息系统