浙江金融职业学院

国家示范性高职院校建设项目成果

计算机信息管理

# 密码技术与应用

龚 力 主 编

高等教育出版社
Higher Education Press

国家示范性高职院校建设项目成果

# 密码技术与应用

龚 力 主 编

高等教育出版社

## 内容提要

本书是国家示范性高职院校建设项目成果之一。本书由八章组成，其内容包括：第1章信息安全需求与目标，介绍安全防范技术体系框架和信息安全的目标；第2章密码技术概述，介绍密码的基本概念和基本原理；第3章对称加密体制，介绍对称加密体制和DES算法，并分析三重DES的工作原理；第4章非对称加密体制，重点介绍非对称加密体制的公钥思想，包括其要求、原理、作用和特点以及RSA算法；第5章数字签名，介绍数字签名的概念、原理、作用、意义和现状，并介绍消息摘要；第6章公钥构架，介绍PKI的定义与组成、体系结构、原理和功能，重点对PKI体系结构中的CA和数字证书的格式与标准进行介绍；第7章数字认证，详细介绍数字证书的申请、安装和使用；第8章数据加密与应用实例是读者体验区，选择中国工商银行电子银行认证系统和广州市数字证书管理中心作为实例，带领读者体验数字认证的应用。本书图文并茂，描述与操作并重，实例丰富，以项目作为引导，并在每章之后附有综合练习供读者巩固所学知识。

本书适合高职高专学校信息、计算机、电子商务和通信等专业的学生作为信息安全类课程的教材使用，也可供计算机技术人员和计算机爱好者参考。

**图书在版编目(CIP)数据**

密码技术与应用 / 龚力主编. —北京：高等教育出版社，2008.11

ISBN 978-7-04-025447-1

Ⅰ.密… Ⅱ.龚… Ⅲ.密码-技术-高等学校-教材 Ⅳ.TN918

中国版本图书馆CIP数据核字(2008)第162413号

**策划编辑** 赵 萍　**责任编辑** 康兆华　**封面设计** 赵 阳　**责任绘图** 尹 莉
**版式设计** 张 岚　**责任校对** 王 雨　**责任印制** 韩 刚

**出版发行** 高等教育出版社
**社　　址** 北京市西城区德外大街4号
**邮政编码** 100120
**总　　机** 010-58581000

**经　　销** 蓝色畅想图书发行有限公司
**印　　刷** 北京中科印刷有限公司

**开　　本** 787×1092　1/16
**印　　张** 13.75
**字　　数** 330 000

**购书热线** 010-58581118
**免费咨询** 800-810-0598
**网　　址** http://www.hep.edu.cn
http://www.hep.com.cn
**网上订购** http://www.landraco.com
http://www.landraco.com.cn
**畅想教育** http://www.widedu.com

**版　　次** 2008年11月第1版
**印　　次** 2008年11月第1次印刷
**定　　价** 22.00元

本书如有缺页、倒页、脱页等质量问题，请到所购图书销售部门联系调换。



**物料号** 25447-00

# 前言

在现代学科门类中，很少有学科像密码学这样既拥有悠久的历史，又能在现代信息社会中仍然闪耀着光芒。密码学的历史已经有数千年，从古希腊由一条带子缠绕在一根木棍上的所谓换位密码器到现代的量子密码，无不渗透着变换的宝贵思想，这种思想揭示了一个自人类社会诞生伊始即具有的神秘现象：隐藏的需要。

人类社会这种隐藏的需要也反映在密码学的教材中。由于密码技术的创造者总是希望增加算法流程的复杂度，以达到为破译者设置障碍的目的，而这种复杂性加剧了人们对密码学的恐惧。再者，很多密码算法来源于数学中的复杂定理，使得大多数人不知道需要对数字系统具备多深的了解才能进入密码学的殿堂。在现代信息系统的环境下，密码技术的应用已经十分普遍，过去认为的密码仅起保密作用还只是一个方面，实际上，现代密码技术已经成为网络认证的重要基础，并据此建立起相互信任的网络环境，以达到处理各种电子事务的需要。为此，本书努力尝试提供浅显易懂、不必过多追求完备的理论，同时又兼顾实际需要的教学内容。

本书的特色在于图文并茂，借助生动的图形来描述复杂的原理应该是一种好方法。此外，本书尽量用浅显易懂的文字来说明相关的原理，使读者不必在具备完备理论的基础上就能了解密码技术的原理。在实例方面，本书提供较为丰富的应用实例，以项目化的形式呈现于每一章的结尾，并据此作为高等职业教育能力培养的目标，从而使读者能够明白现代密码技术的作用范围，提高应用密码技术分析和解决问题的能力。

本书共由八章组成，其内容概述如下。

第1章信息安全需求与目标，介绍安全防范技术体系框架，特别是对信息安全的目标即可靠性、可鉴别性、保密性、完整性、不可抵赖性和可控性进行了重点说明，并对威胁和相应的信息安全策略进行了必要的介绍。最后通过一个信息安全风险分析项目，剖析典型应用所面临的威胁及其对信息安全目标产生的影响。

第2章密码技术概述，主要介绍密码学的基本概念和基本原理，回顾密码技术的历史演变过程及逐渐形成的变换和替换思想。在阐述密码系统的构成后，介绍在电路上容易实现的异或逻辑以及四种加密模式，最后通过对 Windows 加密文件系统的实际操作，帮助读者增加对密码技术的感性认识。

第3章对称加密体制，重点内容是密钥的作用、加密强度与密钥的关系，详细介绍目前在对称加密体制中应用最广泛的 DES 算法，并据此分析三重 DES 的工作原理。另外，对于其他算法，如 IDEA、RC5 和椭圆曲线加密算法进行了简略的介绍，并通过三重 DES 项目和 NTFS 文件加密系统的应用来帮助读者加深对本章内容的理解。

第4章是著名的公钥体制，即非对称加密体制。首先将问题的提出作为本章的起始，在此基

础上，重点介绍非对称加密体制的公钥思想，包括其要求、原理、作用和特点。介绍 RSA 算法，并对 RSA 算法的数学基础作了必要的引入。对于实际应用中将对称与非对称加密技术相结合的数字信封技术进行了简要的分析。此外，对于解决密钥分发问题的 Diffie-Hellman 密钥协商协议也进行了介绍。

第 5 章数字签名。数字签名是实现网络认证的基础，介绍其概念、原理、作用、意义和现状。作为高效数字签名的重要手段——消息摘要也放在这一章，并通过著名的 PGP 加密和数字签名软件的实际操作来全面运用前五章所讲解的内容。

第 6 章公钥构架。PKI 作为公钥体制最重要的应用，读者需了解其定义和组成、体系结构、原理和功能，本章重点对 PKI 体系中的 CA 和数字证书的格式与标准进行了介绍，并通过对 Outlook 证书的配置来帮助读者加深对 PKI 的理解。

第 7 章数字认证。数字认证是通过数字证书的形式来完成的，本章详细介绍数字证书的申请与安装步骤，特别是数字证书的使用方法，包括设置服务器证书和客户身份认证以及数字证书的撤销等。本章设置 4 个项目，内容涵盖数字证书的申请与管理、用户申请管理和数字证书加密与签名使用。

第 8 章数字加密与应用实例是读者体验区，选择中国工商银行电子银行认证系统和广州市数字证书管理中心作为实例，介绍中国工商银行的 U 盾和口令卡两种安全措施。还介绍了广州市数字证书管理中心较为完善的数字证书设置系统，并带领读者体验数字证书在网上税务和网上社会保障两个领域的具体应用。

本书图文并茂，描述与操作并重，实例丰富，以项目作为引导，并在每章之后附有综合练习供读者巩固所学知识。本书适合高职高专学校信息、计算机、电子商务和通信等专业的学生作为信息安全类课程的教材使用，也可供计算机技术人员和计算机爱好者参考。

限于编者的学识，加之编写时间有限，书中难免存在欠妥之处，望广大读者提出宝贵的意见和建议。

编　者

2008 年 8 月

# 开始之前

“密码技术与应用”是信息安全技术及相关专业的一门主干专业课程。课程按照现代密码技术的应用和必要的理论基础来进行内容的组织，以培养学生运用密码技术进行数据安全通信和建立安全认证能力为核心。通过本课程的学习，使学生理解并掌握信息安全的基本需求和目标，掌握对称加密体制和非对称加密体制的原理与特点，在此基础上，认识数字签名与 PKI 认证系统，并能够据此创建自己的安全认证手段，提供安全通信服务，从而建立“需求—原理—应用”的关系，达到理论联系实际，为进一步学习其他课程和进入信息系统安全的相关工作岗位打下基础。

本课程的开发以职业分析为基础，以就业方向为导向，在充分征询行业专家、专业教师和信息安全岗位一线人士的建议的基础上，对计算机信息系统和网络的安全维护与管理、计算机网络安全体系设计与实现、信息安全及应用软件开发等专业化方向进行了分析，确立信息安全管理员（师）、信息安全工程师、程序员、信息安全专员（主管）等岗位的需求，并据此分析各个工作岗位所承担的工作项目，将其进一步分解为若干工作任务。在此基础上，为各项工作任务确立所需技能和知识，形成密码技术与应用的职业能力需求分析，成为课程内容设置和构建的基础。

本教材尽量采用浅显易懂的文字来说明教学内容，并使用大量图表来形象化地表述各种复杂的原理，使学生不必在具备完备理论的基础上掌握密码技术的原理。本教材以项目为载体，以工作任务为导向，在每一章的结尾均设置多个实训项目，教师可根据不同的实践条件进行项目驱动教学，据此作为能力培养的目标，从而使学生能够明白现代密码技术的作用范围，提高应用密码技术分析和解决问题的能力。

# 目录

# 第1章

# 信息安全需求与目标

随着社会信息化进程的不断深入和网络技术的快速发展，网络化已经深入社会活动的各个层面，信息化的普及及信息资源最大程度的共享正在成为各种组织发展的重要目标之一。21世纪是信息的时代，信息日渐成为一种重要的战略资源，信息技术改变着人们的工作和生活方式，社会信息化已经成为当今世界发展的主要潮流，信息产业正成为支柱型产业，信息的获取、处理和安全保障能力成为一个国家综合国力的重要象征。当前，一方面信息技术产业欣欣向荣，处于空前繁荣的发展阶段，而另一方面，危害信息安全的事件时有发生，信息安全的形势变得越来越严峻。各种形式的攻击和破坏、计算机犯罪、计算机恶意代码（如病毒）的侵袭等，已经成为危害信息安全的主要威胁。与此同时，基于计算机网络的电子政务、电子商务和电子金融等应用正在广泛兴起，产生了与信息流相伴随的资金流、物流等大量敏感信息，这些应用对信息安全都提出了更高的要求，所以，信息安全作为一门学科，其发展越来越受到人们的关注。

## 1.1 信息安全现状

世界主要工业国家每年因计算机犯罪所蒙受的经济损失令人吃惊，据美国联邦调查局的调查报告显示，美国每年因计算机犯罪所造成的经济损失高达1 700多亿美元，远远超过普通经济犯罪所带来的经济损失。据美国的一项调查报告宣称，有40%的被调查者承认在他们供职的机构中曾发生过信息安全事件。我国的计算机犯罪案例也在逐年上升，例如，近几年我国的网络银行屡屡发生金融欺诈事件。

黑客入侵已成为危害计算机网络和信息安全的经常性、多发性事件，国内外都曾发生过严重的黑客入侵事件。

2000年2月7日起的一周内，黑客对许多网站发动大规模的攻击，著名的美国雅虎、亚马逊、eBay等八大网站相继被攻并导致服务器瘫痪，造成直接经济损失12亿美元。

2001年5月1日前后发生了一场中美网络黑客大战。双方互相攻击对方的计算机网站，都遭受了很大的损失。这一事件留给人们的思考是发人深省的。

2003年1月25日13时30分到19时30分的6个小时内，北美洲、欧洲和亚洲的Internet站点全部陷入瘫痪和半瘫痪状态，其原因至今尚不清楚。

据美国联邦调查局的估算，大型计算机网络每被攻破一次所造成的经济损失为50亿美元，而银行数据中心的一台计算机每停机一秒钟所造成的损失为5 000美元。

除了金融信息系统外，政治、军事等重要的信息系统也是不法分子攻击的重点对象。德国的

几名青年曾攻入美国五角大楼和北约的计算机数据库。美国通用动力公司的一名软件设计师所设计的逻辑炸弹破坏了太空导弹数据库,致使数据库中的数据无法恢复,造成无法弥补的损失。被称为美国头号黑客的 Kevin Mitnick 15 岁时就闯入北美空中防务指挥系统主机,翻阅美国所有的核弹头资料,并与美国联邦调查局的特工恶作剧,简直令人难以置信。后来他又向美国圣地亚哥超级计算机中心、摩托罗拉公司、Novell 公司、SUN 公司及芬兰诺基亚公司的计算机系统发动攻击,盗窃各种程序和数据,价值高达 4 亿多美元。

社会的信息化导致第三次军事革命,信息战、网络战成为新时期的作战方式,数字化部队和数字化战场随之诞生。早在 1995 年 1 月,美国国防部就成立了信息战执行委员会,1995 年海湾战争期间,美国成功地对伊拉克发动了信息战。战争刚一开始,美国便激活了埋藏在伊拉克计算机系统中的病毒,并用电子干扰机对伊拉克的防空及通信系统实施电子干扰,致使该国计算机系统和通信系统陷入瘫痪,只能处于被动挨打的地位。在科索沃战争期间,美国也曾发动信息战袭击南斯拉夫的计算机系统。在 2003 年的伊拉克战争中,美国的信息战和电子战的优势就更加明显。最近美国又成立网络作战司令部,统一部署和指挥意在维护美国利益的网络作战。

过去被认为是科学幻想的计算机病毒,现在已经活生生地出现在人们面前,对计算机系统的安全构成极大威胁。1988 年 11 月 3 日,美国康奈尔大学一年级研究生罗特·莫里斯编制的称为蠕虫的计算机病毒通过因特网大面积传播,致使 6 000 台 UNIX 工作站和小型机被感染,直接经济损失达 6 000 万美元。据有关部门统计,目前计算机病毒的类型已增至上万种,而且还在高速增加。中国台湾人编制的 CIH 病毒是世界上第一个直接攻击计算机主板的病毒,曾在我国和东南亚地区多次发作,造成重大的经济损失。随着移动通信技术的迅速发展,手机的使用越来越普及,最近又出现了手机病毒。与计算机病毒作斗争是一项长期的任务,目前反病毒技术已发展到很高的水平。我国的反病毒技术处于世界先进水平,随着反病毒技术的提高,人们对计算机病毒已不像最初那样恐慌。但是,计算机病毒仍然是非常令人厌恶的,其传播和发作都将消耗大量的计算机资源,重者将造成不可估量的损失。过去,大多数计算机病毒的编制者只是为了炫耀自己的技术,而现在却更多地是为了获取经济和政治方面的利益,而且呈现群体作案的特点。这一变化是人们必须认真思考和严密防范的。

面对严重危害计算机和网络信息安全的各种威胁,必须采取有力措施确保计算机和网络的信息安全。特别是中美黑客网络大战等事件,让人清醒地认识到,为了确保国家的安全,必须建立我国自己的信息安全体系。

虽然我国在信息安全技术方面整体落后于美国等发达国家,但在信息安全领域的许多方面有自己的特色。如在密码技术、计算机病毒防治、软件加密等方面,我国都有一定程度的自主创新,可信计算是近年来发展起来的一种信息安全新技术,它已经在世界范围内形成热潮。建立自主、可信的信息安全体系正是信息安全发展的终极目标。

## 1.2 信息安全概述

信息安全这一概念所涵盖的范围比较广,大到国家军事、政治情报等的机密安全,小到企业信息系统的正常运行,预防青少年对不良信息的浏览,防止个人信息的泄露,等等。网络环境下

的信息安全体系是保证信息安全的关键所在，包括计算机安全操作系统、安全协议、安全机制（数字签名、信息认证、数据加密等），其中任何一个安全漏洞都足以导致全局安全受到严重威胁。信息安全服务至少应该包括在支持信息网络服务的基本理论之中，以及基于新一代信息网络体系结构的网络安全服务体系结构之中。信息安全是指网络的硬件、软件及其系统中的数据受到保护，不会出于偶然的或者恶意的原因而遭到破坏、更改、泄露，系统能够连续、可靠、正常地运行，信息服务不会中断，等等。

信息安全是一门涉及计算机科学、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综合性学科。从广义上来说，凡是涉及网络信息的保密性、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安全的研究内容。

ITU－T X.800 标准将“网络安全”（network security）在逻辑上分别进行定义，即安全攻击（security attack）是指损害机构所拥有信息的安全的所有行为；安全机制（security mechanism）是指用于检测、预防安全攻击或者恢复系统的机制；安全服务（security service）是指采用一种或多种安全机制以抵御安全攻击、提高机构的数据处理系统安全和信息传输安全的服务。

为了能够有效地了解用户的安全需求，选择合适的安全产品和策略，有必要建立一些系统的方法来进行网络安全防范，网络安全防范体系的科学性、可行性是其顺利实施的有力保障。图1－1给出了基于 DISSP 扩展的三维安全防范技术体系框架结构。第一维是安全服务，给出了8种安全属性（ITU－T X.800－199103－I）。第二维是系统单元，给出信息网络系统的组成。第三维是协议层次，给出并扩展了国际标准化组织的开放系统互连参考模型（OSI/RM）。

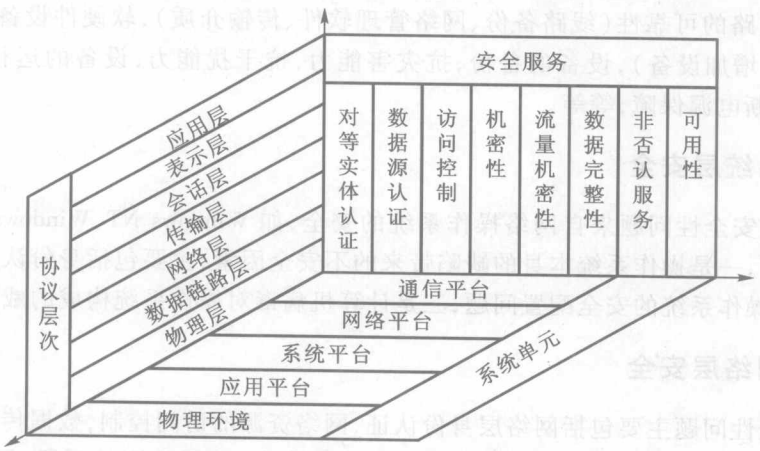


图1－1　三维安全防范技术体系框架结构

框架结构中的每一个系统单元都对应于某个协议层次，需要采取多种安全服务才能保证该系统单元的安全。网络平台需要有网络节点之间的认证和访问控制；应用平台需要有针对用户的认证和访问控制，需要保证数据传输的完整性、保密性，需要有抗抵赖和审计的功能，需要保证应用系统的可用性和可靠性。针对一个信息网络系统，如果在各个系统单元都有相应的安全措施来满足其安全需求，则认为该信息网络是安全的。

全方位的、整体的网络安全防范体系也是分层次的，不同层次反映不同的安全问题。根据网络的应用现状和网络的结构，可将安全防范技术体系的层次划分为物理层安全、系统层安全、网

络层安全、应用层安全和安全管理，如图 1－2 所示。

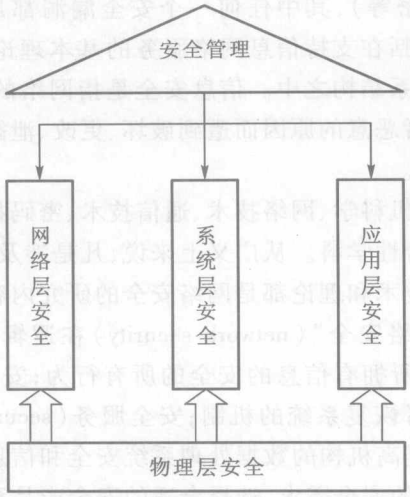


图 1－2　网络安全防范技术体系的层次

### 1.2.1　物理层安全

物理环境的安全性包括通信线路的安全、物理设备的安全、机房的安全等。物理层的安全主要体现在通信线路的可靠性（线路备份、网络管理软件、传输介质），软硬件设备的安全性（替换设备、拆卸设备、增加设备），设备的备份，抗灾害能力，抗干扰能力，设备的运行环境（温度、湿度、烟尘），不间断电源保障，等等。

### 1.2.2　系统层安全

操作系统的安全性问题来自网络操作系统的安全，如 Windows NT、Windows 2000 等。主要表现在三个方面，一是操作系统本身的缺陷带来的不安全因素，主要包括身份认证、访问控制、系统漏洞等；二是操作系统的安全配置问题；三是计算机病毒对操作系统构成的威胁。

### 1.2.3　网络层安全

网络的安全性问题主要包括网络层身份认证，网络资源的访问控制，数据传输的保密性与完整性，远程接入的安全，域名系统的安全，路由系统的安全，入侵检测的手段，网络设施防病毒，等等。

### 1.2.4　应用层安全

应用的安全性问题主要由提供服务所使用的应用软件和数据的安全性产生，包括 Web 服务、电子邮件系统、域名系统等。此外，还包括计算机病毒对系统造成的威胁。

### 1.2.5　安全管理

安全管理包括安全技术和设备的管理、安全管理制度、部门与人员的组织规则等。管理的制

度化极大地影响着整个网络的安全，严格的安全管理制度、明确的部门安全职责划分、合理的人员配置都可以在很大程度上降低其他层次的安全漏洞。

## 1.3 信息安全目标

通俗地说，网络信息安全与保密主要是指保护网络信息系统，减少其潜在的危险，使其不受威胁、不出事故。从技术的角度来说，网络信息安全与保密的目标主要体现在系统的保密性、完整性、可控性、可靠性、可鉴别性、不可抵赖性等方面。

### 1.3.1 可靠性

可靠性是网络信息系统能够在规定的条件下和规定的时间内完成规定功能的特性。可靠性是系统安全最基本的要求之一，是所有网络信息系统建设和运行的目标。网络信息系统的可靠性测度标准主要有三种：抗毁性、生存性和有效性。

抗毁性是指系统面对人为破坏时的可靠性。比如，部分线路或节点失效后，系统是否仍然能够提供一定程度的服务。增强抗毁性可以有效地避免因各种灾害（战争、地震等）造成大面积瘫痪的事件。

生存性是指系统在随机破坏下的可靠性。生存性主要反映随机性破坏和网络拓扑结构对系统可靠性造成的影响。这里，随机性破坏是指系统部件因为老化等而造成的自然失效。

有效性是一种基于业务性能的可靠性。有效性主要反映在网络信息系统的部件失效的情况下，满足业务性能要求的程度。比如，网络部件失效虽然未引起连接性故障，但是却造成质量性能指标下降、平均延时增加、线路阻塞等现象。

可靠性主要表现在硬件可靠性、软件可靠性、人员可靠性、环境可靠性等方面。硬件可靠性最为直观和常见。软件可靠性是指在规定的时间内，程序成功运行的概率。人员可靠性是指人员成功地完成工作或任务的概率，人员可靠性在整个系统可靠性中扮演着重要的角色，因为系统失效的大部分原因是人为差错造成的。人的行为要受到生理和心理的影响，受到其技术熟练程度、责任心和品德等素质方面的影响。因此，人员的教育、培养、训练和管理以及合理的人机界面设计是提高可靠性的重要方面。环境可靠性是指在特定的环境内，保证网络成功运行的概率。这里的环境主要是指自然环境和电磁环境。

此外，可靠性还体现在可用性方面，可用性是网络信息系统面向用户的安全性能。网络信息系统最基本的功能是向用户提供服务，而用户的需求是随机的、多方面的，有时还包括时间上的要求。可用性一般用系统正常使用时间和整个工作时间的比值来度量。

### 1.3.2 可鉴别性

可鉴别性是网络信息可被授权实体访问并按需求使用的特性。即在需要网络信息服务时，允许授权用户或实体使用的特性，或者是在网络部分受损或需要降级使用时，仍然能够为授权用户提供有效服务的特性。

可鉴别性还应该满足以下要求：身份识别（如图 1－3 所示）与确认、访问控制（对用户的权限进行控制，相应权限只能访问特定的资源，防止或限制经由隐蔽通道的非法访问，包括自主访

问控制和强制访问控制)、业务流控制(利用均分负载方法,防止业务流量过度集中而引起网络阻塞)、路由选择控制(选择那些稳定、可靠的子网、中继线或链路等)、审计跟踪(把网络信息系统中发生的所有安全事件相关情况存储在安全审计跟踪之中,以便分析原因,分清责任,及时采取相应的措施。审计跟踪的信息主要包括:事件类型、被管理的客体的等级、事件时间、事件信息、事件回答以及事件统计等)。

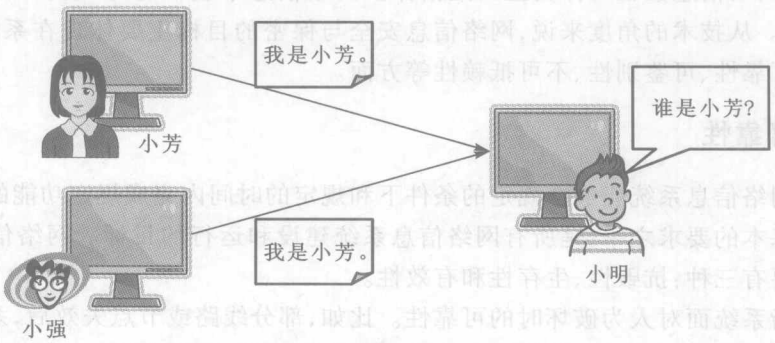


图 1-3　身份识别

### 1.3.3　保密性

保密性是网络信息不被泄露给非授权的用户、实体或过程,或供其利用的特性。即防止信息泄露给非授权的个人或实体,信息只为授权用户所使用的特性。保密性是在可靠性和可用性的基础之上,保障网络信息安全的重要手段(如图 1-4 所示)。

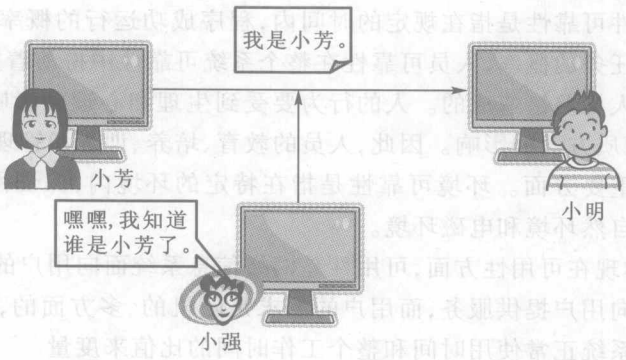


图 1-4　明文传输的危害——丧失保密性

常用的保密技术包括:防侦收(使对手侦收不到有用的信息)、防辐射(防止有用信息通过各种途径辐射出去)、信息加密(在密钥的控制下,用加密算法对信息进行加密处理,即使对手得到经过加密的信息也会因为没有密钥而无法读懂有效信息)、物理保密(通过各种物理方法,如限制、隔离、掩蔽、控制等措施,保护信息不会被泄露)。

### 1.3.4 完整性

完整性是指网络信息未经授权不能被改变的特性。即网络信息在存储或传输的过程中保持不被偶然或蓄意地删除、修改、伪造、乱序、重放、插入和丢失的特性。完整性是一种面向信息的安全性，它要求保持信息的原样，即信息的正确生成、存储和传输（如图 1－5 所示）。

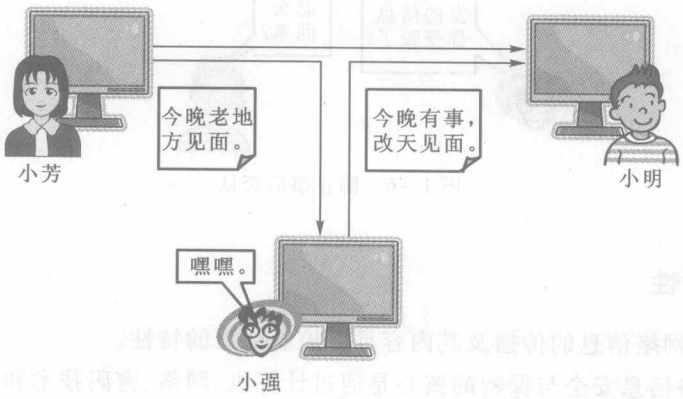


图 1－5　信息的完整性被破坏

完整性与保密性不同，保密性要求信息不被泄露给未经授权的人，而完整性则要求信息不致受到各种因素的破坏。影响网络信息完整性的主要因素包括：设备故障、误码（传输、处理和存储过程中产生的误码，定时的稳定度和精度降低而造成的误码，各种干扰源造成的误码）、人为攻击、计算机病毒等。

保障网络信息完整性的主要方法有以下几种。

（1）协议：通过各种安全协议，可以有效地检测出被复制的信息、被删除的字段、失效的字段和被修改的字段。

（2）纠错编码：由此实现检错和纠错的功能。最简单、最常用的纠错编码方法是奇偶校验法。

（3）密码校验和：这是抗篡改和防止传输失败的重要手段。

（4）数字签名：保障信息的真实性。

（5）公证：请求网络管理或中介机构证明信息的真实性。

### 1.3.5 不可抵赖性

不可抵赖性也称作不可否认性，在网络信息系统的信息交互过程中，确信参与者的真实同一性，即所有参与者都不可能否认或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否认已发送过信息，利用递交和接收证据可以防止收信方否认已经接收过信息（如图 1－6 所示）。

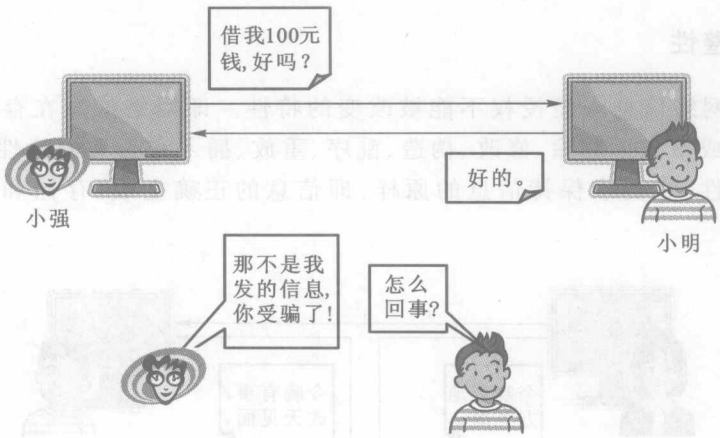


图 1-6　防止事后否认

### 1.3.6　可控性

可控性是指对网络信息的传播及其内容具有控制能力的特性。

概括地说，网络信息安全与保密的核心是通过计算机、网络、密码技术和安全技术，保护在公用网络信息系统中传输、交换和存储的消息的保密性、完整性、可控性、可靠性、可鉴别性、不可抵赖性等。

## 1.4　信息安全面临的威胁

因特网的安全隐患主要源于计算机网络的脆弱性、网络通信协议的缺陷、网络软件与网络服务的漏洞、网络结构的安全隐患和网络硬件的安全缺陷等几个方面。

### 1.4.1　计算机网络的脆弱性

计算机网络的脆弱性通常包括物理网络的脆弱性、过程网络的脆弱性以及通信链路的脆弱性三种。具体表现为：

（1）电磁辐射

计算机及其外围设备在进行信息处理时会产生电磁泄漏，即电磁辐射。现有的一些探测设备能够在 1 km 以外收集计算机站点的电磁辐射信息，并且能区分不同计算机终端的信息。

（2）搭线窃听

（3）串音

在有线通信链路中，由于电磁泄漏和信道间寄生参数的交叉耦合，当一个信道进行信息的传送时，会在另一个或多个相邻的信道中感应出信号或噪声，即串音。串音不但使网络内的噪声增加，被传输的信息发生畸变，而且会引起信息泄露。

在因特网中，最易被窃的是电子邮件信息。尽管电子邮件的传输通常仅仅是几分钟的事情，但它要经过许多中转主机节点，每经过一个节点就多了一次被黑客截取信息的机会。电子邮件