数字签名原理及技术

张先红　编著

机 械 工 业 出 版 社

本书系统地介绍了当前各项有代表性的数字签名技术。主要内容分为三部分：第一部分为基础部分，涉及密码学、数学基础和一些基础算法；第二部分详述了三种最典型的数字签名体制：RSA 签名、DSS 和 ECDSA 体制，然后介绍了其他典型的通用及有特殊用途的数字签名体制；最后一部分介绍了电子邮件和数字证书等数字签名的典型应用、数字签名的潜信道问题、数字签名的标准与数字签名法的相关内容。

本书适用于电子商务、电子政务、电子证券等系统的开发者，以及从事信息安全的科研、教学人员和信息安全专业的学生。

图书在版编目（CIP）数据

数字签名原理及技术/张先红编著 .—北京：机械工业出版社，2004.1
ISBN 7-111-13245-9

Ⅰ.数 … Ⅱ.张 … Ⅲ.电子计算机－密码术 Ⅳ.TP309.7

中国版本图书馆 CIP 数据核字（2003）第 096393 号

机械工业出版社（北京市百万庄大街 22 号 邮政编码 100037）
策划编辑：胡毓坚
责任编辑：孙 业 版式设计：张世琴 责任校对：张 媛
封面设计：鞠 扬 责任印制：路 琳
北京机工印刷厂印刷·新华书店北京发行所发行
2004 年 1 月第 1 版·第 1 次印刷
787mm×1092mm $^{1}/_{16}$·15.5 印张·384 千字
0 001—3 000 册
定价：28.00 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换
本社购书热线电话（010）68993821、88379646
封面无防伪标均为盗版

前　言

信息时代虽然带给我们无限商机与方便，但也充斥着隐患与危险。由于网络容易受到攻击，导致机密信息的泄露，轻则引发企业、部门工作陷于瘫痪而造成巨大的经济损失，重则危及国家、军事安全和社会稳定。当前，网络犯罪活动快速增加，各种网络安全隐患日益突出。网络犯罪正成为一个亟待解决的问题。由于信息已经成为代表综合国力的战略资源，网络业已渗透到人们日常生活的各个方面，所以信息安全已成为保证国民经济信息化建设健康有序发展的基础，直接关系到国家的安全，其影响重大。

网络安全技术众多，如防火墙、安全审计、入侵检测等等。本书介绍的数字签名技术是当前信息化建设中的关键安全机制之一。数字签名，是电子政务、电子商务、电子银行、电子证券等等系统必备的关键性技术，在日常的电子邮件中我们也经常使用，又如重庆去年启用的电子身份认证系统，其核心技术就是数字签名。

数字签名又有人称之为数字签字、电子签名、电子签章等。其提出的初衷就是在网络环境中模拟日常生活中的手工签名或印章；而要使数字签名具有与传统手工签名一样的法律效力，又催生了数字签名法律的出现。数字签名具有许多传统签名所不具备的优点，如签名因消息而异，同一个人对不同的消息，其签名结果是不同的；原有文件的修改必然会反映为签名结果的改变，原文件与签名结果两者是一个混合的不可分割的整体等。所以，数字签名比传统签名更具可靠性。

数字签名的特性及可抵御的网络威胁可以概括为身份鉴别，可辨别信源的真实性而防冒充；数据完整性保护，抵御数据的篡改或重排；不可抵赖性，信源事后不可否认以防其抵赖；一般还使用加密技术保护信息机密性，以防截听攻击；加入流水号等技术，可防重放攻击。特别是其身份鉴别、数据完整性和不可抵赖性在电子商务、电子政务等领域中有很重要的作用。

与传统签字或印章有根本不同，数字签名的基础是公钥密码学，通过数学的手段来达到传统签字的功能。简单地说，在公钥密码体制中，仅仅签名者自己掌握私钥，而其对应的公钥是公开的，那么签名者用自己的私钥变换数据（加密），其他人就可以利用签名者的公钥来逆变换数据（解密），因为利用其他

任何公钥都无法正确逆变换出该私钥变换后的数据，从而就可以鉴别该数据是谁进行的变换处理，亦即是谁的签名。

在本书中作者力求全面而系统地介绍当前数字签名的研究概貌。为了让没有学习过密码学的读者方便理解，加入了密码学、数学理论等部分基础知识。

本书的编写与出版得到了中国工程物理研究院科学技术基金（项目号20010667）的资助，同时本书也是作者长期从事信息安全研究工作的一个总结。

在本书的编写过程中，得到了相关领导和诸多老师的帮助与支持；特别是甄增振高工、张小东工程师和王宇同志的帮助，在此一并表示诚挚感谢。

由于信息安全技术发展很快，相关文献层出不穷。另受作者学识所限，以致想反映当前数字签名的研究概貌亦感力有未逮，书中错误和不妥之处在所难免，希望得到读者的指正。

编　者

目　录

第1章 概 述

由于网络的广泛普及与使用，其应用涉及到政府、军事、文教、商业、金融等诸多领域。如商业经济信息系统、政府机关信息系统、银行业务系统、证券业务系统、科研数据传输等，这些系统都涉及到机密信息的传输与存储。

如何保证这些机密信息不泄露，就是网络信息安全研究需要解决的问题。网络安全的目标应当满足：身份真实性、信息机密性、信息完整性、服务可用性、不可否认性、系统可控性、系统易用性、可审查性等等。数字签名技术是网络安全的重要手段之一，它可以保证信息完整性、鉴别发送者的身份真实性与不可否认性；再运用数字签名本身的基础技术如加密技术，可以保证信息机密性；如再运用审计日志的方法，可完成可审查性的功能。

数字签名是当前网络安全领域的研究热点。特别是在电子商务、电子银行、电子政务等应用领域，数字签名是其关键技术之一，在社会生活的各个领域也有极其广阔的应用前景。美国、欧盟分别在2000年前后，正式颁布了数字签名法律。

1.1 因特网

因特网（Internet）作为世界上最大的计算机网络，已经取得了极大的进步。越来越多的个人、商业组织、研究机构和政府机构都依赖于因特网进行通信和研究工作。但是，网络上的不可靠因素太多，受到攻击所造成的损失可能很大。个人隐私、商业机密、电子支票、乃至国家、军事机密都可能受到攻击。因特网安全问题越来越受到人们的关注。

1.1.1 因特网的发展简介

Internet最早来源于ARPA建立的ARPAnet，ARPA是美国国防部高级研究计划局（DARPA）的前身。该网于1969年投入使用，最初用于军事研究目的，要求该网络实现异种网之间的互联互通，网络必须能够经受住故障的考验而维持正常工作，一旦发生战争，当网络的某一部分因遭受攻击而失去工作能力时，网络的其他部分应当能够维持正常通信。由于ARPA大力鼓励分组交换技术的研究，该网的建立大大推动了分组交换技术的发展。

1972年，ARPAnet在首届计算机后台通信国际会议上首次与公众见面，并验证了分组交换技术的可行性。由此，ARPAnet成为现代计算机网络诞生的标志。

1980年，美国国防部把其研制的广域网网络体系结构和协议标准：TCP/IP协议簇加入到UNIX（BSD4.1版本）的内核中，随后该协议即成为UNIX操作系统的标准通信模块。内含TCP/IP的UNIX为当时许多大学的局域网建设提供了迫切需要的联网手段，也促使了UNIX在网络方面的成功。

1982年，Internet由ARPAnet、MILNET等几个计算机网络合并而成，作为Internet的早期骨干网。ARPAnet试验并奠定了Internet存在和发展的基础，较好地解决了异种机网络互联的一系列理论和技术问题。随后该网就分为了二部分：一是军方的MILNET，用于军

方的非机密通信；另一部分就是现在的因特网（Internet）。

蓬勃发展的其他局域网和广域网，也对 Internet 的进一步发展起到了重要的作用。例如美国国家科学基金会（NSF）建立的美国国家科学基金网 NSFnet。1986 年，它建立了供美国全国的科学家、工程师共享的六大超级计算机中心。为了这些超级计算机设施，NSF 建立了独立的基于 TCP/IP 协议簇的计算机网络 NSFnet。同时 NSF 帮助建立了很多地区网，并联入到 NSFnet。NSFnet 面向全社会开放，不仅仅供计算机研究人员、政府职员和政府承包商使用。由于 NSFnet 的巨大成功，1990 年，NSFnet 彻底取代了 ARPAnet 而成为 Internet 的主干网。

ARPAnet 最初建成时只有四个结点，1972 年只有 23 个结点，直到 1977 年 3 月总共只有 111 个结点。随着社会科技、文化和经济的发展，特别是计算机网络技术和通信技术的大力发展，人类社会从工业社会向信息社会过渡的趋势越来越明显，人们对信息的意识，对开发和使用信息资源的重视越来越加强，这些都强烈刺激了 NSFnet 和 ARPAnet 的发展，使联入这两个网络的主机和用户数目急剧增加。1988 年，由 NSFnet 连接的计算机数就猛增到 56000 台，此后每年更以 2 到 3 倍的惊人速度向前发展；1994 年，Internet 上的主机数目达到了 320 万台，连接了世界上的 35000 个计算机网络。现在，估计 Internet 的用户每月仍以 10％～15％的数目向前增长。今天的 Internet 已不再是计算机人员和军事部门进行科研的领域，而是一个开发和使用信息资源的覆盖全球的信息海洋。

1.1.2 因特网的广泛应用及高速增长的网络犯罪

在 Internet 上，按从事的业务分类包括了广告公司、航空公司、农业生产公司、艺术、导航设备、书店、化工、通信、计算机、咨询、娱乐、财贸、各类商店、旅馆等等 100 多类，覆盖了社会生活的方方面面。

1995 年，Internet 开始大规模应用在商业领域。当年，美国 Internet 业务的总营业额为 10 亿美元，1996 年达到 18 亿美元。提供联机服务的供应商也从原先像 America Online 这样的计算机公司发展到像 AT&T、MCI、Pacific Bell 等通信运营公司。目前全世界已有 200 多个国家和地区联入因特网。

由于商业应用产生的巨大需求，从调制解调器、光纤网到诸如 Web 服务器和浏览器的 Internet 应用市场都分外红火。

在 Internet 蓬勃发展的同时，其本身随着用户的需求的转移也发生着产品结构上的变化。1994 年，所有的 Internet 软件几乎全是 TCP/IP 协议，那时人们需要的是能兼容 TCP/IP 协议的网络体系结构；如今 Internet 重心已转向具体的应用，象利用 WWW 来做广告或进行联机贸易。Web 是 Internet 上增长最快的应用，其用户已从 1994 年的不到 400 万激增至 1995 年的 1000 万，Web 站的数目在 1995 年就达到三万个；到目前 Internet 用户可以说已经离不开 WWW 服务。

安全性问题是困扰 Internet 用户发展的一个主要因素。依据 Financial Times 曾做过的统计，平均每 20 秒钟就有一个网络遭到入侵。计算机犯罪已经成为普遍的国际性问题。计算机犯罪大都具有瞬时性、广域性、专业性、时空分离性等特点。通常计算机罪犯很难留下犯罪证据，这大大刺激了计算机高技术犯罪案件的发生。计算机犯罪案率的迅速增加，使各国的计算机系统、特别是网络系统面临着很大的威胁，并成为严重的社会问题之一。

例如，在 1989 年，三名德国黑客因涉嫌向前苏联出售军事机密而被捕，他们曾在两年多的时间里，侵入了北约及美国的计算机网络，从中窃取了诸多高度机密的信息。1996 年，美国中央情报局主页上的名称被改为了“中央笨蛋局（Central Stupidity Agency）”，而美国司法部（Department of Justice）则被改为了“非法部（Department of Injustice）”。

1995 年俄罗斯的一个黑客在英国被捕。他被控用笔记本电脑从纽约花旗银行非法转移至少 370 万美元到世界各地由他和他的同党控制的账户。

美国联邦调查局于 2001 年曾称，来自东欧的电脑黑客在最近数月中攻击了超过 40 个美国电子商务和银行网站，以期获得秘密的金融信息或实施敲诈。美国联邦调查局的分支部门——全国基础设施保护中心的调查人员称，盗窃信用卡的数量上升比例同在俄罗斯境内盗用信用卡的上升幅度相近。联邦调查局有关人员指出，他们的调查显示，在东欧，特别是在俄罗斯和乌克兰的几个有组织的黑客团体，成功地进入了美国电子商务电脑系统，从而导致成百上千台电脑成为牺牲品，此外，大约超过 100 万张信用卡号码被盗。美国联邦调查局目前正在全美二十个州进行四十起案件的调查工作。美国联邦调查局一改以往不对正在进行调查的案件进行评论的政策，因为他们相信尽管此举会影响其工作，但是却有助于提醒公众并加强他们的警惕性。联邦调查局称目前此种敲诈行为仍在发生，但是对具体细节则拒绝加以介绍，并指出这些案件中涉及美国本土以外的犯罪组织。

我国的网络犯罪也成激增之势。目前查获的国内网络犯罪主要包括：色情网站，网络贩卖盗版光碟，贩卖违禁、管制物品，网上销售赃物，网络诈欺，妨害名誉，入侵他人网站，电脑病毒，网络赌博，散播个人资料等等。

网络犯罪已经渗透到社会生活的方方面面，随着计算机的运用越来越广泛，网络犯罪正成为一个亟待解决的令人头痛的问题。

1.2 网络安全

网络安全从其本质上来讲就是网络上的信息安全。信息安全是对信息的保密性、完整性和可用性的保护。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安全的研究领域。网络安全包括物理安全、网络系统安全、数据安全、信息内容安全和信息基础设施安全等。

网络安全与我国的经济安全、社会安全和国家安全紧密相连。涉及到个人利益、企业生存、金融风险防范、社会稳定和国家安全等诸多方面，是信息化建设进程中具有重大战略意义的问题。目前网络安全的现状令人担忧，从技术到管理都处于落后、被动局面。

网络安全风险来源于内部脆弱性和外部威胁。内部脆弱性风险的防范属于主动控制范畴；外部威胁风险的防范属于被动控制范畴。必须全方位解析网络的脆弱性和威胁，才能构建网络的安全措施，确保网络安全。

1.2.1 因特网的安全脆弱性分析

由于 Internet 从建立开始就缺乏安全方面的总体构想和设计；TCP/IP 协议是在可信环境下为网络互联专门设计的，缺乏安全措施的考虑，所以必然导致因特网的安全脆弱。

从外部来说，由于因特网的日益普及，网络分布的广域性、网络体系结构的开放性、信

息资源的共享性和通信信道的共用性；用户的增多，黑客的涌现，发现的因特网安全漏洞越来越多；随着密码分析研究的发展，网络攻击手段的日渐丰富，使网络的安全脆弱性问题凸现，网络安全问题更趋严重化。

1. 从用户角度看安全脆弱性有如下体现：

（1）对信息被他人利用缺乏控制能力。由于系统本身的漏洞，或其他恶意或非恶意的程序，如病毒、网络传输等，都可能导致私有信息的泄露，让所有者失去其对信息的控制。

（2）对信息的泄露或不正当的接触与利用存在疑虑。由于网络上信息的易泄露，攻击者容易取得他人重要信息，而冒名该人进行网上活动，如进行电子交易等。

（3）对政府或组织以处理案件为由而截收信息的动机存在不信任感。例如，美国联邦调查局力图取得安装电话窃听设备的权利，又如美国政府提倡的密钥托管等，都造成用户的疑虑和不信任感。

（4）担心自己的计算机系统遭到外界的破坏，包括怀有敌意的破坏和收到大批有恶意的电子邮件广告等。

（5）最迫切需要使用时出现计算机系统故障，导致急需的信息无法取出。

（6）有关个人钱财、健康状况、购物习惯等隐私信息的大量暴露，如被一些数据统计公司等所持有、公布或泄露。

2. 从技术角度分析网络安全的脆弱性，可以列举如下：

（1）不设防的网络有上千个漏洞和后门。再从计算机软硬件看：机器设备、计算机软件、网络系统、甚至有些安全产品都是外国产品；计算机的操作系统几乎全部都采用美国的系统，计算机主机的 CPU 芯片也都是美国产品；目前使用的路由器、交换机等绝大部分也是国外产品；关键技术掌握在别人手里，安全得不到可靠保证。

（2）电磁辐射。电子设备工作过程都有电磁辐射产生。电磁辐射在网络中表现出两方面的脆弱性。电磁辐射物能够破坏网络中传输的数据，这种辐射的来源有两个：网络周围电子电气设备产生的电磁辐射和试图破坏数据传输而预谋的干扰辐射源；网络的终端、打印机或其他电子设备在工作时产生的电磁辐射泄露。即便使用不太先进的设备，在近处甚至较远处都可将这些数据、包括终端屏幕上显示的数据接收下来，并且重新恢复。

（3）线路窃听。可分为被动的无源线路窃听和主动的有源线路窃听。无源线路窃听通常是一种没有检测的窃听，它通常是为了获取网络中信息内容，是一种被动攻击。有源线路窃听是对信息流进行有目的的变形，能够任意改变信息内容，注入伪造信息、删除和重发原来的信息；也可以用于模仿合法用户，或通过干扰阻止和破坏信息传输。有源线路窃听属于主动攻击。

（4）串音干扰。串音的作用就是产生传输噪声，这些噪声能对网络上传输的信号造成严重的破坏。

（5）硬件故障。硬件故障势必造成软件中断和通信中断，甚至重要数据的丢失，带来重大损害。

（6）软件故障。通信网络软件一般用于建立计算机和网络的连接。程序里包含有大量的管理系统安全的部分，如果这些软件程序受到损害，则该系统就是一个极其不安全的网络系统，安全强度大大降低。

（7）人为因素。系统内部人员的非法活动，如系统操作员、工程技术人员和管理人员在

非法人员的教唆下，盗窃机密数据或破坏系统资源。利用制度不健全或管理不严盗窃存有机密数据的媒体，甚至直接破坏网络系统。

（8）网络规模。网络安全的脆弱性和网络的规模有密切关系。网络规模越大，其安全的脆弱性越大。资源共享与网络安全是一对矛盾，网络发展使资源共享加强，但导致安全问题愈加严重。

（9）网络物理环境。这种类型脆弱性是属于计算机设备防止自然灾害的破坏，比如火灾和洪水。也包括一般的物理环境的保护，象机房的安全门、人员出入机房的规定等。物理环境安全保护的范围不仅包括计算机设备和传输线路，也包括一切可以移动的物品，比如有打印数据的打印纸和装有数据和程序的磁盘等等。

（10）通信系统。通信系统始终是最为严重的脆弱性所在。对于一般的通信系统，获得存取权是相对简单的，并且机会总是存在的。一旦信息从生成和存储的设备发送出去，它就将成为对方分析研究的内容。

3. 从 TCP/IP 协议的安全脆弱性来分析，可以列举如下：

（1）IP 层。缺乏安全认证和保密机制（就是 IP 地址问题）。

（2）TCP/UDP 层。TCP 连接建立时的“三次握手”，仅仅考虑双方的有效连接，而忽略了安全性的考虑。TCP 连接能被欺骗、截取、操纵；UDP 易受 IP 源路由和拒绝服务的攻击。由于开始时建立 TCP/IP 协议时，是假定在可信环境下的通信，解决的是有效连接问题，所以造成上述安全隐患是在当时没有预料到的。

（3）应用层。应用层在认证、访问控制、完整性、保密性等很多安全问题上都存在安全隐患。如：Finger、FTP、Telnet、E－mail、DNS、SNMP、Web、Notes、Exchange、MIS、OA 等应用，有关它们漏洞的报告很多。

1.2.2 网络安全威胁的主要类型

网络安全潜在威胁形形色色，从不同角度看：有人为和非人为的、恶意的和非恶意的、内部攻击和外部攻击、被动和主动攻击等。对网络安全的威胁主要表现为：非授权访问、冒充合法用户、破坏数据完整性、干扰系统正常运行、利用网络传播病毒、线路窃听等方面。安全威胁主要利用以下途径来达到破坏的目的：系统存在的漏洞、系统安全体系的缺陷、使用人员的安全意识薄弱、管理制度的薄弱等。

网络威胁日益严重，网络面临的威胁五花八门，概括起来主要有以下几类。

（1）内部窃密和破坏。内部人员可能对网络系统形成下列威胁：内部涉密人员有意或无意泄密、更改记录信息；内部非授权人员有意无意偷窃机密信息、更改网络配置和记录信息；内部人员破坏网络系统等。

（2）截收。攻击者可能通过搭线或在电磁波辐射的范围内安装截收装置等方式，截获机密信息，或通过对信息流和流向、通信频度和长度等参数的分析，推出有用信息。它不破坏传输信息的内容。不易被查觉，属于被动攻击。

（3）非法访问。非法访问指的是未经授权而使用网络资源或以未授权的方式使用网络资源，它包括：非法用户如黑客进入网络或系统，进行违法操作；合法用户以未授权的方式进行操作。

（4）破坏信息的完整性。攻击可能从三个方面破坏信息的完整性：篡改——改变信息流

的次序、时序，更改信息的内容、形式；删除——删除某个消息或消息的某些部分；插入——在消息中插入一些信息，让收方读不懂或接收错误的信息。属于主动攻击类型。

(5) 冒充。攻击者可能进行下列冒充：冒充领导发布命令、调阅文件；冒充主机欺骗合法主机及合法用户；冒充网络控制程序套取或修改使用权限、口令、密钥等信息，越权使用网络设备和资源；接管合法用户，欺骗系统，占用合法用户的资源等等。

(6) 破坏系统的可用性。攻击者可能从下列几个方面破坏网络系统的可用性：使合法用户不能正常访问网络资源；利用特殊程序大量消耗系统资源；摧毁系统等。

(7) 重放。重放指的是攻击者截获并录制信息，然后在必要的时候重发或反复发送这些信息以扰乱或欺骗接受者，有的也称其为重演。

举例说明：梁上君在网上银行存有 $12000，现在他通过网络转账 $10000 到一个海外账户，同时他想办法获取该网上银行向海外银行转帐的数据包。然后他可以把这些数据包不断的重新发给该海外银行，以期从海外帐户上取得更多美元。当然，这一切只有在没有防重放攻击措施的情况下才会有效。

(8) 抵赖。从发信者和接收者两个角度看，可能出现下列抵赖行为：发信者事后否认曾经发送过某条消息；发信者事后否认曾经发送过某条消息的内容；接收者事后否认曾经接收过某条消息；接收者事后否认曾经接收过某条消息的内容。

(9) 流量分析攻击。根据分析通信双方通信流量的大小，以期获得相关信息。

(10) 其他威胁。对网络系统的威胁还包括计算机病毒、电磁泄漏、各种自然灾害（如水灾，火灾，地震等)、战争、失窃、操作失误等。

1.2.3 网络安全服务与机制

不安全的网络还不如没有网。一个不设防的网络，一旦遭到恶意攻击，将意味着一场灾难。对于网络的应用，需要居安思危、未雨绸缪，克服脆弱、抑制威胁，防患于未然。网络安全是对付威胁、克服脆弱性、保护网络资源的所有措施的总和，涉及政策、法律、管理、教育和技术等多方面的内容。网络安全是一项系统工程，针对来自不同方面的安全威胁，需要采取不同的安全对策。从法律、制度、管理和技术上采取综合措施，以便相互补充，达到较好的安全效果。管理是所有安全领域的重要组成部分，而技术措施是最直接的屏障，目前常用而有效的网络安全技术对策有如下几种。

(1) 加密。加密是所有信息保护技术措施中最古老、最基本的一种。加密的主要目的是防止信息的非授权泄漏。加密方法多种多样，在信息网络中一般是利用信息变换规则把可懂的信息变成不可懂的信息。既可对传输信息加密，也可对存储信息加密，把计算机数据变成一堆乱七八糟的数据，攻击者即使得到经过加密的信息，也不过是一串毫无意义的字符。加密可以有效地对抗截收、非法访问等威胁。现代密码算法不仅可以实现加密，还可以实现数字签名、鉴别等功能，有效地对抗截收、非法访问、破坏信息的完整性、冒充、抵赖、重演等威胁，因此，密码技术是网络信息安全的核心技术。

(2) 数字签名。数字签名机制提供了一种鉴别方法，以解决伪造、抵赖、冒充和篡改等安全问题。数字签名采用一种数据交换协议，使得收发数据的双方能够满足两个条件：接受方能够鉴别发送方所宣称的身份；发送方以后不能否认他发送过该数据这一事实。数据签名一般采用非对称加密（公钥密码）技术，发送方对整个明文进行加密变换，得到一个值，将

其作为签名。接收者使用发送者的公开密钥对签名进行解密运算，如其结果满足一定条件，则签名有效，证明对方身份是真实的。本书将专门对数字签名技术进行讲述。

（3）鉴别。鉴别的目的是验明用户或信息的正身。对实体声称的身份进行惟一的识别，以便验证其访问请求合法性、或保证信息来自或到达指定的源和目的。鉴别技术可以验证消息的完整性，有效地对抗冒充、非法访问等威胁。按照鉴别对象的不同，鉴别技术可以分为消息源鉴别和通信双方相互鉴别；按照鉴别内容的不同，鉴别技术可以分为用户身份鉴别和消息内容鉴别。鉴别的方法很多：利用鉴别码验证消息的完整性；利用通行字、密钥、访问控制机制等鉴别用户身份，防止冒充、非法访问；当今较佳的鉴别方法是数字签名。利用发送方单方数字签名，可实现消息源鉴别，访问身份鉴别、消息完整性鉴别。利用收发双方数字签名，可同时实现收发双方身份鉴别、消息完整性鉴别。

（4）访问控制。访问控制的目的是防止非法访问。访问控制是采取各种措施保证系统资源不被非法访问和使用。一般采用基于资源的集中式控制、基于源和目的地址的过滤管理以及网络签证等技术来实现。

（5）防火墙。防火墙技术是建立在现代通信网络技术和信息安全技术基础上的应用性安全技术，越来越多地应用于专用网络与公用网络的互联环境中。专用网络系统与因特网互联的第一道屏障就是防火墙。防火墙通过控制和监测网络之间的信息交换和访问行为来实现对网络安全的有效管理，其基本功能为：过滤进、出网络的数据；管理进、出网络的访问行为；封堵某些禁止行为；记录通过防火墙的信息内容和活动；对网络攻击进行检测和告警。

当然还有其他技术，如入侵检测、防病毒技术、安全审计、数据备份与恢复等等。本书将讨论数字签名技术的理论基础，算法原理以及相关的应用、标准、法律法规等问题。

1.3 数字签名的作用与用途

数字签名是实现电子交易安全的核心技术之一，它在实现身份认证、数据完整性、不可抵赖性等功能方面都有重要应用。尤其在密钥分配、电子银行、电子证券、电子商务和电子政务等许多领域有重要应用价值。

数字签名的实现基础是加密技术，其使用公钥加密算法与散列函数。常用数字签名算法有：RSA、DSS、ECDSA、ElGamal、Schnorr 等；还有一些用于特殊用途的数字签名，如盲签名、群签名、失败－终止签名等。

1.3.1 生活中的手写签字与印章

在平常生活中，使用手写签字与印章随处可见，如签署合同，办理证明等。手写签字与印章不论在个人、单位，乃至政府、军事、外交处理信件、商业契约文件、命令、条约等都常使用。如果在网络上实现签字和印章的电子化，其好处与优点是无疑的。

使用传统的手写签字与印章，其目的是：签署双方已经签署该文件，从而该文件能得到法律的认证、核准，可以在法律上生效，签署双方必须履行该文件上的规定的条款。

在网络环境的数字签名，使用公钥加密算法，以模拟手写签字与印章。按笔迹学理论，每个人的手写签字是不一样的，印章对每个实体（个人或单位等）也是惟一的，法律上不准其他实体仿造。在数字签名中，每个实体（个人或单位）有一个（或一组）秘密值，对应其

分配一个惟一的数字证书。用该秘密值签署文件，用对应的数字证书进行验证，就可以在网络环境中替代平常生活中的手写签字与印章。

数字证书，有的称为电子证书，它是网络上各个实体的网上身份证明，相当于我们的身份证。数字证书由具有权威性、可信任性、公正的第三方机构所颁发，通常由政府或政府授权的机构担当，这种第三方机构叫做认证机构（Certificate Authority），简记为 CA。比如生活中，就好象李五的证明（相当于数字证书）由西北大学计算机学院颁发，因为上面有计算机学院的印章，而计算机学院是由西北大学授权的，西北大学又是由更高一级单位授权的。CA 的建立也好象实际生活，一层一层地进行授权。

在生活中，有冒充签名的，有私刻单位印章的。而数字签名的引入，不可避免的也带来一些新问题，列举如下：

（1）需要立法机构对数字签名技术有足够的重视，并且在立法上加快脚步，迅速制定有关法律，以充分实现数字签名具有的特殊鉴别作用。这对应于信息安全中强调的管理的重要性，这单纯用技术方法是不可解决的。

（2）要求数字签名软件具有很高的普及性，如果发送方的信息已经进行了数字签名，那么接收方就一定要有数字签名软件才可处理。

（3）假设某人发送信息后脱离了某个组织，被取消了原有数字签名的权限，以往发送的数字签名在鉴定时只能在取消确认列表中找到原有确认信息，这样就需要鉴定中心结合时间信息进行鉴定，这需要鉴定中心的建立健全。

（4）基础设施的使用费用问题，是收费还是免费，这些都将影响到该技术的推广。

数字签名实际上使用了某种算法（公钥密码算法）变换了所需传输的信息，与传统的手工签字与印章有根本不同。手工签字是模拟的，因人而异，不同的人，其签字是不同的；数字签名是针对计算机处理的数据，即 0 和 1 的比特数据串，是因消息而异的，同一个人，对不同的消息，其签字结果是不同的。

书面手写签名中，签名与文件内容是彼此分离的；而数字签名中，签名是因消息而异的，也就是说签名与原有文件已经形成了一个混合的整体数据（虽然原文件和数字签名结果可以分开保存），原有文件的修改必然反映为签名的变化。所以，数字签名比传统手工签名更具可靠性。

1.3.2 数字签名原理简述

数字签名在具体实施时，首先发送方对信息施以数学变换，所得的信息与原信息惟一地对应；在接收方进行逆变换，得到原始信息。只要数学变换方法优良，变换后的信息在传输中就具有很强的安全性，很难被破译、篡改。这个发送方的变换过程就是签名，通常是一种加密措施；对应的逆变换过程就是对签名的认证，通常是一种解密措施。

有一种密码体制称为公钥密码，又叫非对称密码；密钥是由公开密钥和私有密钥组成的密钥对。简单地讲，数字签名就是用私有密钥进行加密，而认证就是利用公开密钥可以进行正确的解密。但是由于公开密钥无法推算出私有密钥，所以公示的公开密钥并不会损害私有密钥的安全；公开密钥无须保密，可以公开传播，而私有密钥必须保密。如此，某人用其私有密钥加密消息，能够用他的公开密钥正确解密，就可肯定该消息是某人签字的。因为其他人的公开密钥不可正确解密该加密过的消息，其他人也不可能拥有该人的私有密钥而制造出

该加密过的消息。

下面用一个具体的例子说明，以帮助读者理解。

【例 1-1】　李红申请获取了一个数字证书，数字证书里面保存了他的公开密钥——其中的 2 个数字　{5，119}，当然按规定，其他人也可以获得李红的公开密钥；同时他本人保存了只有他自己才拥有的私有密钥——也是一对数字　{77，119}。现在假设李红要对下述消息签名："Who am I?Bill Gates"。

首先把上述字符串转换为 ASCII 值为 V：{87 104 111 32 97 109 32 73 63 32 66 105 108 108 32 71 97 116 101 115}。

签名运算为：对上述 V 中每个值 v，运算：v^{77} mod　119。Mod 表示求余数的运算。

求出来的值为 M：{117 83 76 2 48 23 2 54 14 2 19 63 61 61 2 29 48 107 33 47}。

用字符表示为："uSL┐0┤┐6┐┐　!!? = =┐　0k！/"。是一串无意义的字符。

验证方使用公开密钥对 M 解密，如果结果有意义，就可初步断定该消息是经过李红签名的。解密算法，也就是验证算法如下：

对上述 M 中每个值 m，运算：m^5 mod　119。求出来的值为：

{87 104 111 32 97 109 32 73 63 32 66 105 108 108 32 71 97 116 101 115}。

用字符表示为："Who am I?Bill Gates"。

显然，只有相匹配的私有密钥与公开密钥才能完成上述工作，如其中任何一个密钥不对，验证结果将是一串乱码，签字不成立。实际的签名算法当然更为复杂，密钥数字更大，有完整性保护，防重放等功能。

1.3.3　数字签名可以抵御的威胁

数字签名机制作为保障网络信息安全的手段之一，可以解决伪造、抵赖、冒充和篡改问题。

数字签名的目的之一，就是在网络环境中代替传统的手工签字与印章，那么其可抵御哪些网络攻击？

(1) 防冒充（伪造）。其他人不能伪造对消息的签名，因为私有密钥只有签名者自己知道，所以其他人不可能构造出正确的签名结果数据。显然要求各位保存好自己的私有密钥，好象保存自己家门的钥匙一样。

可鉴别身份。由于传统的手工签字一般是双方直接见面的，身份自可一清二楚；在网络环境中，接受方必须能够鉴别发送方所宣称的身份。如例 1-1 所示，可鉴别身份：接收者使用发送者的公开密钥对签名报文进行解密运算，如其结果为明文，则签名有效，证明对方身份是真实的。

(2) 防篡改（防破坏信息的完整性）。传统的手工签字，假如要签署一本 200 页的合同，是仅仅在合同末尾签名呢？还是对每一页都签名？不然，对方会不会偷换其中几页？这些都是问题所在。而数字签名，如前所述：签名与原有文件已经形成了一个混合的整体数据，不可能篡改，从而保证了数据的完整性。

(3) 防重放。如 1.2.2 中所讲的梁上君之例，大做无本万利的事情是不可能的。在日常生活中，我向梁上君借了钱，同时写了一张借条给梁上君；当我还钱的时候，肯定要向他索回我写的借条撕毁，不然，恐怕他会再次挟借条要求我再次还钱。在数字签名中，如果采用

了对签名报文添加流水号、时戳等技术，可以防止重放攻击。

（4）防抵赖。前面讲了，数字签名可以鉴别身份，不可能冒充伪造，那么，只要保存好签名的报文，就好似保存好了手工签署的合同文本，也就是保留了证据，签名者就无法抵赖。以上是签名者不能抵赖，那如果接受者确已收到对方的签名报文，却抵赖没有收到呢？要防接受者的抵赖，在数字签名体制中，要求接受者返回一个自己签名的表示收到的报文，给对方或者是第三方，或者引入第三方机制。如此操作，双方均不可抵赖。

（5）机密性（保密性）。有了机密性保证，截收攻击也就失效了。手工签字的文件（如合同文本）是不具备保密性的，文件一旦丢失，文件信息就极可能泄露。数字签名，可以加密要签名的信息，例 1-1 中的密文“uSL┐0┤┐6┐┐!!?==┐0k!/”是不可理解的。当然，签名的报文如果不要求机密性，也可以不用加密。

由以上对比可知，数字签名比手工签字更具优越性。特别是在网络应用中，数字签名是进行身份鉴别与网上安全交易的通用实施技术。当然，网络环境还有很多其他威胁，要由其他专门技术解决，如防火墙技术、反病毒技术、入侵检测技术等。

1.3.4 数字签名的用途

在 1979 年 G.J.Simmons 就著文讨论过数字签名的应用。将数字签名运用于美苏两国的禁止核实验条约的验证工作。

双方允许把若干地震测试仪放入对方国家，地震测试仪把采集到的数据传送回本国分析，以验证对方是否进行了核实验。问题是双方互不信任，所以就得保证：收到的数据不是对方篡改后的；收到的数据也不是对方凭空伪造的；传送的数据仅仅只用于地震数据而不是其他信息。

要解决上述问题，就需要借用数字签名技术。因为经过数字签名的数据不可篡改，不可伪造。当然第三个问题，涉及到数字签名的潜信道问题，这在后续章节有详细讲述。

在网络应用中，凡是要解决伪造、抵赖、冒充、篡改与身份鉴别的问题，都可运用数字签名来处理。下面举几个例子：

网上银行通过因特网向客户提供信息查询、对账、网上支付、资金划转、信贷业务以及投资理财等金融业务。网上银行将对传统银行业带来巨变，有人估计：网上银行将使劳动生产率年均增长 54%。银行发放给你的 IC 卡，就存储了代表你身份的数字证书与其他信息，其交易过程就需要数字签名的支持。

电子商务能完成企业之间、企业与消费者之间在网上的商业交换活动。网上证券能在网上完成股票交易、网上证券信息服务、网上银行/证券转账业务等。这些业务需要身份鉴别、防篡改等功能，也要使用数字签名。

再看看电子政务。假如一个没有身份认证服务的电子政务系统，任何人都可随便签发文件散布，而不用担心事发后的追查，因为无法甄别出签字者，该电子政务系统的危害性可想而知。电子政务系统必须提供身份认证服务、权限控制服务、信息保密服务、数据完整性服务和不可否认服务。

我们平常的电子邮件，也常要求具有数字签名功能，比如流行的 PGP，就提供了简单的数字签名模块。

其实数字签名已经超出了手工签名的用途范围。比如，.NET 程序开发中，每个配件可

以有创建者的数字签名，同时相应的公开密钥也保存在配件中，其目的之一是为了标志一个配件的惟一身份。这样做的同时，带来的其他好处，就是可以防篡改；可防篡改功能也就是具有了判别是否被病毒感染等的功能。

数字签名应用前景非常广阔，为了规范和推广数字签名技术，世界各国纷纷颁布有关数字签名的标准和法律。与此同时，其他身份鉴别技术也得到较快的发展，如指纹识别，声纹识别，瞳孔识别等生物特征识别技术。