信息安全技术与教材系列丛书

密码学引论

张焕国　刘玉珍 / 编著

全国优秀出版社
武汉大学出版社

信息安全技术与教材系列丛书

国家自然科学基金项目（90104005，66973034）
国家863计划项目
国家密码发展基金项目
教育部博士点基金项目

密码学引论

张焕国　刘玉珍 / 编著

全国优秀出版社
武汉大学出版社

图书在版编目(CIP)数据

密码学引论/张焕国,刘玉珍编著.—武汉：武汉大学出版社,2003.10
信息安全技术与教材系列丛书
ISBN 7-307-04009-3

Ⅰ.密… Ⅱ.①张… ②刘… Ⅲ.密码—理论 Ⅳ.TN918.1

中国版本图书馆 CIP 数据核字(2003)第 067166 号

责任编辑：黄金文　　责任校对：刘　欣　　版式设计：支　笛

出版发行：**武汉大学出版社**　(430072　武昌　珞珈山)
(电子邮件：wdp4@whu.edu.cn　网址：www.wdp.whu.edu.cn)
印刷：湖北省黄冈日报社印刷厂
开本：787×980　1/16　　印张：16.5　　字数：317 千字
版次：2003 年 10 月第 1 版　　2003 年 10 月第 1 次印刷
ISBN 7-307-04009-3/TN・14　　定价：26.00 元

信息安全技术与教材系列丛书

编　委　会

序 言

21世纪是信息的时代，信息成为一种重要的战略资源。信息科学成为最活跃的学科领域之一，信息技术改变着人们的生活和工作方式，信息产业成为新的经济增长点。信息的安全保障能力成为一个国家综合国力的重要组成部分。

当前，以Internet为代表的计算机网络的迅速发展和“电子政务”、“电子商务”等信息系统的广泛应用，正引起社会和经济的深刻变革，为网络安全和信息安全开拓了新的服务空间。

世界主要工业化国家中每年因利用计算机犯罪所造成的经济损失远远超过普通经济犯罪。内外不法分子互相勾结侵害计算机系统，已成为危害计算机信息安全的普遍性、多发性事件。计算机病毒已对计算机系统的安全构成极大的威胁。社会的信息化导致新的军事革命，信息战、网络战成为新的作战形式。

总之，随着计算机在军事、政治、金融、商业等部门的广泛应用，社会对计算机的依赖越来越大，如果计算机系统的安全受到破坏将导致社会的混乱并造成巨大损失。因此，确保计算机系统的安全已成为世人关注的社会问题和计算机科学的热点研究课题。

信息安全事关国家安全，事关经济发展，必须采取措施确保信息安全。

发展信息安全技术与产业，人才是关键。培养信息安全领域的专业人才，成为当务之急。2001年经教育部批准，武汉大学创建了全国第一个信息安全本科专业。到2003年，全国设立信息安全本科专业的高等院校增加到20多所。2003年经国务院学位办批准武汉大学建立信息安全博士点。

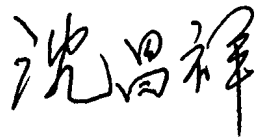
为了增进信息安全领域的学术交流、为信息安全专业的大学生提供一套适用的教材，武汉大学组织编写了这套《信息安全技术与教材系列丛书》。这套丛书涵盖了信息安全的主要专业领域，既可用做本科生的教材，又可作为工程技术人员的技术参考书。

我觉得这套丛书的特点是内容全面、技术新颖、理论联系实际，努力反映信息安全领域的新成果和新技术。在我国信息安全专业人才培养刚刚起步的今天，这套丛

书的出版是非常及时的和十分有益的。

我代表编委会对丛书的作者和广大读者表示感谢。欢迎广大读者提出宝贵意见，以使丛书能够进一步修改完善。

中国工程院院士，武汉大学兼职教授



2003 年 7 月 28 日

前 言

21 世纪是信息的时代，信息成为一种重要的战略资源，信息技术改变着人们的生活和工作方式，信息产业成为新的经济增长点。信息的安全保障能力成为一个国家综合国力的重要组成部分。

当前，信息技术与产业的发展正处于空前繁荣的阶段。以 Internet 为代表的计算机网络的迅速发展和广泛应用，正引起社会和经济的深刻变革。Internet 已经成为我们生活和工作中的一个不可分割的组成部分。基于计算机网络的“电子政务”、“电子商务”和“电子金融”正在兴起，它们的兴起在政务、商务和金融领域引起了一场革命。然而，由于 Internet 的开放性和无政府状态，使 Internet 成为一个不安全的网络。这就使 Internet 不能适应电子政务、电子商务和电子金融等系统对信息安全的要求。网络安全和信息安全已经成为发展电子政务、电子商务和电子金融的主要技术瓶颈。

世界主要工业化国家中每年因利用计算机犯罪所造成的经济损失远远超过普通经济犯罪造成的损失。在我国利用计算机犯罪的案例也在迅速上升。

“黑客”入侵已成为危害计算机网络安全和信息安全的普遍性、多发性事件。

过去被认为是科学幻想的计算机病毒，现已活生生地呈现在我们的面前，对计算机系统的安全构成极大的威胁。

社会的信息化导致新的军事革命，信息战、网络战成为新的重要作战形式，数字化部队和数字化战场已经诞生。在 1995 年的海湾战争和 2003 年的伊拉克战争期间，美国成功地对伊拉克发动了信息战。

总之，随着计算机在军事、政治、金融、商业等部门的广泛应用，社会对计算机的依赖越来越大，如果计算机系统的安全受到破坏将导致社会的混乱并造成巨大损失。因此，确保计算机系统的安全已成为世人关注的社会问题和计算机科学的热点研究课题。

信息安全事关国家安全，事关民族兴衰，事关经济发展，必须采取措施确保信息安全。

我国政府十分重视信息安全技术和产业的发展，先后在成都、上海和武汉建立了信息安全成果产业化基地。

2001 年经教育部批准，武汉大学创建了全国第一个信息安全本科专业。2003 年经国务院学位办批准，武汉大学创建了信息安全博士点。

信息系统的硬件结构安全和操作系统安全是确保信息安全的基础，密码技术是关键技术。

为了增进信息安全技术特别是密码技术的学术交流，我们编写了这本抛砖引玉之作。

本书是作者在武汉大学计算机学院长期从事信息安全教学和科研的基础上写成的。其研究工作得到国家自然科学基金项目(90104005,66973034)、国家863计划项目(2002AA141051)、国家密码发展基金和教育部博士点基金(20020486046)的资助。作者试图从理论和实际相结合的角度较系统地介绍密码学的基本理论和实际应用。既介绍国内外的前沿研究成果，又介绍具体的实用技术；既介绍国外学者的研究成果，又介绍国内学者的研究成果。尽管作者有以上初衷，但因学术水平和篇幅所限，仍有许多密码学的理论与技术没能介绍，而且所述内容也会有不妥和错误之处。对此，作者恳请读者的理解和批评指正，并于此先致感谢之意。

本书共分八章。第一章，概论；第二章，密码学的基本概念；第三章，分组密码；第四章，序列密码；第五章，公开密钥密码；第六章，数字签名；第七章，认证；第八章，密钥管理。

本书的第七章由刘玉珍编写，其余由张焕国编写，并由张焕国对全书进行统编。

作者衷心感谢给予作者指导、支持和帮助的所有领导、专家和同行。

张焕国　刘玉珍

于珞珈山

目 录

第一章 概 论

21 世纪是信息的时代、知识经济的时代。信息成为社会发展的重要战略资源，信息技术改变着人们的生活和工作方式。信息产业成为新的经济增长点。社会的信息化已成为当今世界发展的主要潮流。信息的获取能力和信息的保障能力成为一个国家综合国力和经济竞争力的重要组成部分，因此成为世界各国竞力攀登的制高点。

随着计算机在军事、政治、金融、商业等部门的广泛应用，社会对计算机的依赖越来越大，如果计算机系统的安全受到破坏将导致社会的混乱并造成巨大损失。因此，确保计算机系统的安全已成为世人关注的社会问题和计算机科学的热点研究课题。

当前，以 Internet 为代表的计算机网络的迅速发展和广泛应用，正引起社会和经济的深刻变革，极大地改变着人们的生活。Internet 已经成为我们生活中的一个不可分割的组成部分。基于计算机网络的崭新的政务形式“电子政务”、崭新的商务形式“电子商务”和崭新的金融形式“电子金融”正在兴起，它们的兴起在政务、商务和金融领域引起了一场革命。对此，发展我国的电子政务、电子商务和电子金融已成为建设具有中国特色社会主义强国的不可回避的选择。

然而，目前影响电子政务、电子商务、电子金融应用的主要技术障碍是网络安全和信息安全问题。由于 Internet 的开放性和无政府状态，使 Internet 成为一个不安全的网络。这就使 Internet 不能适应电子政务、电子商务和电子金融等系统对信息安全的要求。

世界主要工业国家中每年因利用计算机犯罪所造成的经济损失令人吃惊，据美国 FBI 的调查报告，美国每年因利用计算机犯罪所造成的经济损失就高达 1 700 多亿美元，远远超过普通经济犯罪所造成的经济损失。据美国的一项调查报告，有 40% 的被调查者承认在他们的机构中曾发生过利用计算机犯罪的事件。在我国，利用计算机犯罪的案例也在迅速上升。

“黑客”入侵已成为危害计算机网络和信息安全的普遍性、多发性事件，国内外都屡屡发生严重的“黑客”入侵事件。

2000 年 2 月 7 日起的一周内，“黑客”对 Internet 网站发动了大规模的攻击，著名的美国雅虎、亚马逊、伊贝等 8 大网站相继被攻瘫痪，造成直接损失 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，双方都有很大的损失。这一事件留给我们的思考将是令人深省的。

2003 年 1 月 25 日 13 时 30 分到 19 时 30 分的 6 个小时内，北美、欧洲和亚洲的

Internet 全部陷入瘫痪或半瘫痪状态，其原因至今尚不清楚。

据美国 FBI 的估计，大型计算机网络每被攻破一次所造成的损失为 50 亿美元，而一个银行的数据中心的计算机每停机一秒钟的损失为 5 000 美元。

除了金融信息外，政治、军事等重要数据也是不法分子攻击的重点。德国几名青年曾攻入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设计的逻辑炸弹破坏了太空导弹数据库，致使电脑数据库的数据无法恢复，造成无法弥补的损失。英国、法国和韩国也发生过类似事件。

社会的信息化导致第三次军事革命，信息战、网络战成为新的重要作战形式，数字化部队和数字化战场已经诞生。美国早就提出了信息战的概念。1995 年 1 月美国国防部成立“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，致使计算机和通信系统瘫痪，使伊拉克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前南斯拉夫的电脑系统。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。美国情报部门利用“黑客”窃取情报是世人皆知的事。

过去被认为是科学幻想的计算机病毒，现已活生生地出现在我们的面前，对计算机系统的安全构成极大的威胁。1988 年 11 月 3 日美国康耐尔大学的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 Internet 网大面积传播，致使6 000 台 UNIX 工作站和小型机被传染，直接经济损失达6 000万美元以上。据有关统计，目前计算机病毒已增至6 000多种，而且还在继续高速度增加。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硬件的病毒，曾在国内和东南亚地区多次大范围传染发作，造成重大经济损失。随着 Internet 的迅速发展和广泛应用，目前计算机病毒也进入了 Internet 时代，主要通过 Internet 进行传播。美国军方早就出钱资助军用计算机病毒的研究。随着移动通信的迅速发展，手机的使用越来越普及，最近又出现了手机病毒。在国内，计算机病毒的传染现象也很严重，特别是大中小学的公用实验室的微机几乎都被计算机病毒传染过。在国内流行的计算机病毒除了由国外传入外，还有一些国内不法分子编制的国产计算机病毒。随着计算机病毒的出现，人们便开始和计算机病毒作斗争。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讨厌的，它们的传染发作，都将消耗大量的计算机资源，重者将造成重大损失。

面对如此严重危害计算机信息安全的种种威胁，必须采取措施确保计算机信息安全。特别是美国袭击我驻前南斯拉夫大使馆和中美“黑客”大战等事件，使我们清醒地认识到，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上落后于美国等发达国家，但我国在信息安全领域中的某些方面有自己的特色。如在密码技术、计算机病毒防治、软件加密等方

面我国都有自己的特色。我国政府已将信息安全技术和产业的发展列为优先发展领域。因此可以相信,我国的信息安全技术和产业将会得到迅速的发展。

国际标准化组织 ISO 在其网络安全体系设计标准(ISO 7498 - 2)中定义了计算机网络系统的五大安全服务功能:身份认证服务、访问控制服务、数据加密服务、数据完整性服务和不可否认服务,比较全面地描述了计算机系统安全的内涵。

从另一个角度可将计算机系统安全划分为计算机系统的设备安全和计算机系统的信息安全。对计算机设备的任何损坏都危害计算机设备的安全,如火灾、水灾、雷击、霉变等都可能导致计算机设备的损坏。计算机设备的损坏将危害计算机信息安全。即使计算机系统的设备没有受到损坏,其信息安全也可能已经受到危害。由于危害计算机信息安全的行为在很多情况下并不留下痕迹,因此常常在信息安全已经受到危害的情况下,用户还不能发现。而对计算机设备安全的损害,用户一般都能直接发现。

本书主要讨论信息安全,信息安全又称为数据安全。

确保数据安全(Data Security)就是要采取措施保护数据,使之免受未授权的泄露、篡改和毁坏。数据安全性主要包括数据的秘密性(Secrecy)、数据的真实性(Authenticity)和数据的完整性(Integrity)三个方面。所谓秘密性就是该知道的就让其知道,不该知道的就不能让其知道。使数据免受未授权的泄露,即确保数据的秘密性。所谓真实性就是数据真实无伪,使数据免受未授权的篡改,即确保数据的真实性。所谓完整性就是数据正确无误、完整不缺,使数据免受未授权的毁坏,即确保数据的完整性。

要确保计算机信息安全,必须采取措施,必须付出代价,这代价就是资源,时间资源或空间资源。其安全措施主要包括法律措施、教育措施、管理措施和技术措施等。

确保信息安全是一个系统工程,必须综合采取各种措施才能奏效。一个系统只有所有子系统都是安全时才是安全的,而只要有一个子系统不安全则整个系统就不安全。虽然某种措施对付某种危害可能更有效,但是没有一种措施能全面解决计算机信息安全问题。特别应当强调的是,绝不能忽视法律、教育、管理措施,在许多情况下它们的作用甚至大于技术措施。

确保信息安全的技术措施包括信息系统的硬件结构安全、操作系统安全、数据库安全、网络安全、密码技术、病毒防治技术、信息隐藏技术、数字权益保护技术等。在这些众多的技术措施中,信息系统的硬件结构安全和操作系统安全是确保信息安全的基础,其他都是关键技术。

本书讨论信息安全的关键技术——密码技术。

密码技术是一门古老的技术,大概自人类社会出现战争便产生了密码(Cipher)。由于密码长期以来仅用于政治、军事、公安、外交等要害部门,其研究本身也只限于秘密进行,所以密码被蒙上神秘的面纱。在军事上,密码成为决定战争胜负的重要因素之一。有些军事评论家认为,盟军在破译密码方面的成功,使第二次世界大战提前几

年结束。

然而,随着计算机和通信技术的迅速发展和普及应用,出现了电子政务、电子商务、电子金融等重要的应用信息系统。在这些系统中必须确保数据的安全保密,因此密码技术有了更广泛的应用空间。

密码技术的基本思想是伪装信息,伪装就是对数据施加一种可逆的数学变换。伪装前的数据称为明文(Plaintext),伪装后的数据称为密文(Ciphertext)。伪装的过程称为加密(Encryption),去掉伪装恢复明文的过程称为解密(Decryption)。加解密要在密钥(Key)的控制下进行。将数据以密文的形式存储在计算机的文件中或送入网络信道中传输,而且只给合法用户分配密钥。这样,即使密文被非法窃取,因不法分子没有密钥而不能得到明文,从而达到确保数据秘密性的目的。同样,因为不法分子没有密钥也不能伪造出合理的明密文,因而篡改数据必然被发现,从而达到确保数据真实性的目的。与能够检测发现篡改数据的道理相同,如果密文数据中发生了错误或毁坏也将能够检测发现,从而达到确保数据完整性的目的。

密码的发展经历了由简单到复杂,由古典到近代的发展历程。在密码发展的过程中,科学技术的发展和战争的刺激都起了巨大的推进作用。

1946 年电子计算机一出现便用于密码破译,使密码进入电子时代。

1949 年商农(C. D. Shannon)发表了题为《保密系统的通信理论》的著名论文,把密码置于坚实的数学基础之上,标志着密码学作为一门学科的形成。

然而对于传统密码,通信的双方必须预约使用相同的密钥,而密钥的分配只能通过其他安全途径,如派专门信使等。在计算机网络中,设共有 n 个用户,任意两个用户都要进行保密通信,故需要 $n(n-1)/2$ 种不同的密钥,当 n 较大时这个数字是很大的。另一方面,为了安全要求密钥经常更换。如此大量的密钥要经常地产生、分配和更换,其困难性和危险性是可想而知的,而且有时甚至不可能事先预约密钥,如企业间想通过通信网络来洽谈生意而又要保守商业秘密,在许多情况下不可能事先预约密钥。因此,传统密码在密钥分配上的困难成为它在计算机网络环境中的应用的主要障碍。

1976 年 W. Diffie 和 M. E. Hellman 提出公开密钥密码(Public Key Cryptosystem)的概念,从此开创了一个密码新时代。公开密钥密码从根本上克服了传统密码在密钥分配上的困难,特别适合计算机网络应用,而且实现数字签名容易,因而特别受到重视。目前,公开密钥密码已经得到广泛应用,在计算机网络中将公开密钥密码和传统密码相结合已经成为网络加密的主要形式。在国际上研究的比较充分,而且公认比较安全的公开密钥密码有,基于大整数因子分解困难性的 RSA 密码和基于有限域上离散对数问题困难性的 ElGamal 密码、椭圆曲线密码等。

1977 年美国颁布了数据加密标准 DES(Data Encryption Standard),这是密码史上的一个创举。DES 算法最初由美国 IBM 公司设计,经国家保密局评测,颁布为标准。DES 开创了向世人公开加密算法的先例。它设计精巧、安全、方便,是近代密码成功

的典范。它成为商用密码的世界标准,为确保数据安全作出了重大贡献。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,标志着密码的设计与分析达到了新的水平。1998 年底美国政府宣布不再支持 DES,DES 完成了它的历史使命。但是,由于 DES 已经制成各种计算机软件和硬件产品并得到广泛应用,因此 DES 的使用不可能立即停止。普遍认为 DES 还会继续使用一段时间,其中 3 重 DES 已得到美国政府和许多国际组织的认可。

早在 1984 年底,美国总统里根就下令美国保密局研制一种新密码,准备取代 DES。经过 10 年的研制和试用,1994 年美国颁布了密钥托管加密标准 EES(Escrowed Encryption Standard),这是密码史上的又一个创举。EES 的密码算法被设计成允许法律监听的保密方式。即如果法律部门不监听,则加密对于其他人来说是计算上不可破译的,但是经法律部门允许可破译密码进行监听。如此设计的目的在于既要保护正常的商业通信秘密,又要在法律部门允许的条件下可破译监听,以阻止不法分子利用保密通信进行犯罪活动。而且 EES 只提供芯片不公开算法,这标志着美国密码政策发生了改变,由公开征集转向秘密设计,由公开算法转向算法保密。和 DES 一样,EES 也在美国社会引起激烈的争论。商界和学术界对不公布算法只承诺安全的做法表示不信任,强烈要求公开算法并取消其中的法律监督。迫于社会的压力,美国政府曾邀请少数密码专家介绍算法,企图通过专家影响民众,然而收效不大。科学技术的力量是伟大的。1995 年美国贝尔实验室的年轻博士 M. Blaze 攻击 EES 的法律监督字段,伪造 ID 获得成功。于是,美国政府宣布仅将 EES 用于话音加密,不用于计算机数据加密,并且后来又公开了加密算法。于是美国政府于 1997 年又开始公开征集新的数据加密标准算法 AES。

1994 年美国颁布了数字签名标准 DSS(Digital Signature Standard),这是密码史上的第一次。数字签名就是数字形式的签名盖章。它是确保数据真实性的一种重要措施。没有数字签名,诸如电子政务、电子金融、电子商务等系统是不能实用的。由于美国在计算机科学技术方面的领先地位,DSS 实际上成为一种国际标准。许多国际标准化组织都已将 DSS 颁布为数字签名标准。一些国家已经颁布了数字签名法,从此数字签名有了法律依据。我国也颁布了自己的数字签名标准,也在研究数字签名的相应法律。

1997 年美国宣布公开征集高级加密标准 AES(Advanced Encryption Standard),以取代 1998 年底停止的 DES。经过三轮筛选,最终选出一个算法作为 AES。第一轮筛选,从应征的 21 个算法中选出 15 个算法作为 AES 候选算法。第二轮筛选,从第一轮筛选出的 15 个算法中再选出 5 个候选算法。第三轮筛选,从第二轮筛选出的 5 个算法中最终选出 1 个候选算法作为 AES。2000 年 10 月 2 日美国政府正式宣布选中比利时密码学家 Joan Daemen 和 Vincent Rijmen 提出的一种密码算法 Rijndael 作为 AES。2001 年 11 月 26 日,美国政府正式颁布 AES 为美国国家标准(编号为 FIST PUBS 197)。这是密码史上的又一个重要事件,世界各国都高度重视这一事件。