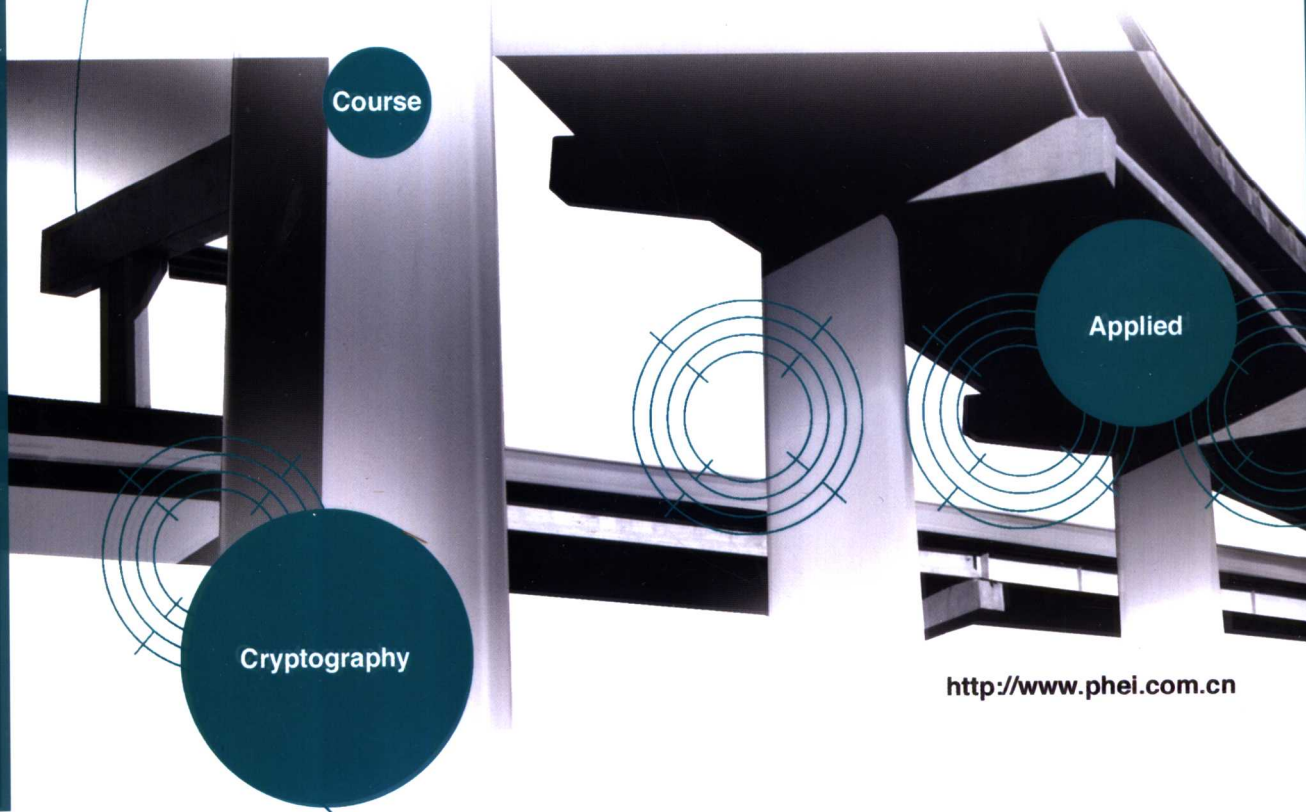
高等学校电子信息类教材

应用密码学教程

胡向东　魏琴芳　编著



http://www.phei.com.cn

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY

高等学校电子信息类教材

应用密码学教程

胡向东　魏琴芳　编著

電子工業出版社
Publishing House of Electronics Industry
北京 • BEIJING

内 容 简 介

本书是作者根据多年的教学和科研工作实践，在学习、总结众多国内外有关网络信息安全和应用密码学文献基础上，特别从教学适用性角度，遵从学习规律编写而成。本书全面介绍了应用密码学的基本概念、基本理论和典型实用技术，专门为教学编排、设计。全书共 14 章，语言简练，内容重点突出，算法经典实用，逻辑性强，便于读者花少量时间尽快掌握应用密码学的精髓。本书最后介绍的应用密码学在电子商务支付安全、数字通信安全和工业网络控制安全这三个典型领域的应用方法和技术，也是本书的一大亮点。

本书可作为高等院校密码学、信息安全、通信工程、计算机、信息管理、电子商务、检测技术、控制理论与控制工程等专业高年级本科生和研究生教材，也可供从事网络和通信信息安全相关领域应用和设计开发的研究人员、工程技术人员参考。

图书在版编目（CIP）数据

应用密码学教程 / 胡向东，魏琴芳编著. —北京：电子工业出版社，2005. 1
高等学校电子信息类教材
ISBN 7-121-00524-7

I. 应… II. ①胡… ②魏… III. 密码-理论-高等学校-教材 IV. TN918.1

中国版本图书馆 CIP 数据核字（2004）第 110318 号

责任编辑：刘志红　特约编辑：张　莉
印　　刷：北京天竺颖华印刷厂
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编 100036
经　　销：各地新华书店
开　　本：787×1092　1/16　印张：18.75　字数：480 千字
印　　次：2005 年 1 月第 1 次印刷
印　　数：5 000 册　定价：28.00 元

凡购买电子工业出版社的图书，如有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系。联系电话：（010）68279077。质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

前　言

随着通信和计算机技术的快速发展，以及经济全球化应用的推动，互联网表现出广泛的覆盖性（包括地域覆盖性、应用领域的覆盖性、使用人群的覆盖性）、使用的方便性、信息传递的快捷性和运作的低成本特性，人们对信息网络的依赖程度越来越大，各种新兴的网络应用层出不穷，并相互推动。移动通信、电子商务、电子政务、企业信息化、“三金工程”等与社会发展、人们生产、生活息息相关领域的安全问题，越来越成为全社会关注的焦点，并成为制约网络应用发展的主要瓶颈之一。没有安全就没有应用，没有应用就没有发展，提高全社会的网络信息安全意识和基本专业知识是保障我国信息化建设健康、稳步、快速发展的前提和基础。

应用密码学作为实现网络信息安全的核心技术，在保障网络信息安全的应用中具有重要的意义，而对典型密码学算法的掌握又是快速实现信息安全的捷径。在各种网络应用迫切呼唤信息安全的背景下，作者根据自己多年的教学和科研工作实践，在学习、总结众多国内外有关网络信息安全和应用密码学文献基础上，特别针对教学工作需要和学习规律完成了本书的撰写工作。在编写过程中，作者力求本书能体现以下特色。

可读性　在内容安排上力求先进实用，由浅入深、循序渐进、逻辑严密、前后呼应；在语言表达上力求通俗易懂、文笔流畅、言简意赅，通过必要的实例和典型的算法为读者快速地掌握应用密码学的核心概念、方法和技术提供了便利。

简明性　全书在内容安排上力求层次清晰、结构合理、主次分明、重点突出，论述上既简明扼要，又系统全面。

实用性　在讲清应用密码学基本概念的同时，力求对对称密码体制（包括序列密码）、非对称密码体制的基本技术、典型密码算法的基本工作原理及其应用方法进行较系统、深入的介绍。

典型性。本书不求面面俱到，力争帮助读者快速入门，并掌握密码学的核心内容，因此在内容取舍、密码算法的选取和例题设置等方面都体现出广泛的代表性和典型性。

适于自学。本书的编排从教学适用性出发，特别重视读者对应用密码学知识的系统理解和有针对性地重点掌握，在内容体系结构、语言表达、内容选取、举例及应用等方面都做了特别的考虑，适于自学。

本书全面介绍了应用密码学的基本概念、基本理论和典型实用技术。内容涉及网络信息安全概述、密码学基础、古典密码、密码学数学引论、对称密码体制、非对称密码体制、HASH函数和消息认证、数字签名、密钥管理、序列密码、密码学与电子商务支付安全、密码学与数字通信安全、密码学与工业网络控制安全、密码学的新进展——量子密码学等。从教学的角度考虑，在每章末都给出了适量的思考题和习题以便读者巩固知识之用。

本书特色鲜明，根据教材的需要进行编排和设计，语言简练、内容先进实用、逻辑性强；

举例典型、紧扣内容、易于接受；可读性好、系统性强、适合自学；内容重点突出、算法经典实用，便于读者花少量的时间尽快掌握应用密码学的精髓。本书最后以电子商务支付安全、数字通信安全和工业网络控制安全三个典型领域的信息安全应用为例，分析了应用密码学在这三个典型领域的应用方法和技术，这也是本书的一大亮点。

本书简明、实用，符合素质教育的要求，在掌握密码学基础知识的同时，对锻炼读者的独立思考和动手能力特别有用，有助于读者掌握密码学的基本理论，并培养密码学的工程技能。教师可在32~56学时内讲解全部或选讲部分内容，还可以配以适当的上机教授让学生动手实践，在有限的时间内快速掌握应用密码学的核心内容，提高学习效率。

本书可作为高等院校密码学、信息安全、通信工程、计算机、信息管理、电子商务、检测技术、控制理论与控制工程等专业高年级本科生和研究生教材，也可供从事网络和信息安全相关领域应用和设计开发的研究人员、工程技术人员参考。

本书由重庆邮电学院自动化学院胡向东副教授组织编写，第3、4、10、12章由重庆邮电学院通信与信息工程学院魏琴芳老师编写，胡向东负责其余章节的编写和全书的统稿。作者要特别感谢参考文献中所列各位作者，包括众多未能在参考文献中一一列出的作者，正是因为他们在各自领域的独到见解和特别的贡献为作者提供了宝贵的资料和丰富的写作源泉，使作者能够在总结教学和科研工作成果的基础上，汲取各家之长，形成一本具有自身特色的应用密码学教程。

在本书编写过程中，重庆邮电学院自动化学院王平教授、鲜继清副教授、重庆邮电学院信息安全重点实验室等都提供了大力支持，在此表示衷心的感谢。蔡军、谢颖、张开碧等老师和高旸、徐笑尘、易明华、余刚等研究生参与了部分资料的收集、整理和书稿的校对工作，在此对他们付出的辛勤劳动表示深深的感谢。

本书另配有相应的CAI课件。如有需要，请与作者取得联系。

应用密码学是一门内容广泛、发展迅速的学科，对本书的编写是作者在此领域的一次努力尝试，限于作者的水平和学识，书中难免存在疏漏和错误之处，诚望读者不吝赐教，以利修正，让更多的读者获益。联系电子邮件：huxd@cqupt.edu.cn。

作　者

2004年8月

受重庆市教委科技研究项目（040510）资助

受重庆邮电学院

控制理论与控制工程博士点
模式识别与智能系统硕士点

建设项目资助

目　录

第1章 绪 论

1.1 网络信息安全概述

1.1.1 网络信息安全问题的由来

随着通信与计算机网络技术的快速发展和公众信息系统（包括计算机互联网、移动通信网、磁卡系统等）商业性应用步伐的加快，当数据通信和资源共享等网络信息服务功能广泛覆盖于各行各业及各个领域，网络用户来自各个阶层与部门，人们对网络环境和网络信息资源的依赖程度日渐加深时，网络信息的安全隐患就越来越明显地突现出来，在网络中存储和传输的大量数据需要保护，因为这些数据对于所有者来说可能是敏感数据（如个人的医疗记录、信用卡账号、登录网络的口令，或者企业的战略报告、销售预测、技术产品的细节、研究成果、人员的档案等）。这些数据在存储和传输过程中都有可能被盗用、暴露、篡改和伪造。除此之外，基于网络的信息交换还面临着身份认证和防否认等安全需求。这些问题被公认为是21世纪公众信息系统发展的关键。

目前，作为数据通信和资源共享的重要平台——互联网是一个开放系统，其具有资源丰富、高度分布、广泛开放、动态演化、边界模糊等特点，安全防御能力非常脆弱，而攻击却易于实施，并且难留痕迹。随着网络技术及其应用的飞速发展，黑客袭击事件不断发生并逐年递增，网络安全引起了世界各国的普遍关注。就我国而言，目前，我国信息化建设已进入高速发展阶段，电子政务、电子商务、网络金融、网络媒体等正在兴起，这些与国民经济、社会稳定息息相关的领域急需信息安全保障。

1.1.2 网络信息安全问题的根源

产生网络信息安全问题的根源可以从三个方面分析：自身缺陷、开放性和人的因素。

1. 网络自身的安全缺陷

网络自身的安全缺陷主要是指协议不安全和业务不安全。

导致协议不安全的主要原因：一方面是Internet从建立开始就缺乏安全的总体构想和设计，因为Internet起源的初衷是方便学术交流和信息沟通，并非商业目的。Internet所使用的TCP/IP协议是在假定的可信环境下，为网络互连而专门设计的，本身缺乏考虑安全措施。TCP/IP协议的IP层没有安全认证和保密机制（只基于IP地址进行数据包的寻址，无认证和保密）。在传输层，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。另一方面，协议本身可能会泄露口令、连接可能成为被盗用的目标、服务器本身需要读写特权、密码保密措施不强等。

业务的不安全主要表现为：业务内部可能隐藏着一些错误的信息；有些业务本身尚未完善，难于区分出错原因；有些业务设置复杂，一般非专业人士很难完善的设置。

2. 网络的开放性

网络的开放性主要表现为：业务基于公开的协议；连接是基于主机上的社团彼此信任的原则；远程访问使远程攻击成为可能。在电脑网络所创造的特殊的、虚拟的空间，网络犯罪往往十分隐蔽，有时可能会留下蛛丝马迹，但更多的时候是无迹可寻。

3. 人的因素

人是信息活动的主体，是引起网络信息安全问题最主要的因素，可以从以下三个方面来理解。

1）人为的无意失误

人为的无意失误主要是指用户安全配置不当造成的安全漏洞，包括用户安全意识不强、用户口令选择不当、用户将自己的账号信息与别人共享、用户在使用软件时未按要求进行正确的设置。

2）黑客攻击

这是人为的恶意攻击，是网络信息安全面临的最大威胁。在英文中，黑客有两个概念：Hacker 和 Cracker。Hacker 是这样一类人，他们对钱财和权利蔑视，而对网络本身非常专注，他们在网上进行探测性的行动，帮助人们找到网络的漏洞，可以说他们是这个领域的绅士。但是 Cracker 不一样，他们要么为了满足自己的私欲，要么受雇于一些商业机构，具有攻击性和破坏性。他们修改网页，窃取机密数据，甚至破坏整个网络系统。因其危害性较大，Cracker 已成为网络安全真正的，也是主要的防范对象。这类人闯入计算机网络系统盗取信息，故意破坏他人财产，使服务器中断。他们对电脑非常着迷，自认为比他人聪明，因此，随心所欲地闯入某些信息禁区，开玩笑或恶做剧，甚至干出违法的事。他们把此看做一种智力挑战，好玩、刺激可能是他们最初的动机，但当有利可图时，很多人往往抵制不住诱惑而走上犯罪的道路。信息战也是黑客开展攻击的一个非常重要的缘由。

3）管理不善

对网络信息系统的严格管理是避免受到攻击的重要措施。据统计，在美国，90%以上的 IT 企业对黑客攻击准备不足，75%~85%的网站都抵挡不住黑客的攻击。美色和财物通常成为间谍猎取机密性信息的致胜法宝。总之，管理的缺陷也可能导致系统内部人员泄露机密，被一些不法分子获取以制造可乘之机。

1.1.3 网络信息安全的重要性和紧迫性

随着全球信息基础设施和各个国家信息基础的逐渐形成，计算机网络已经成为信息化社会发展的重要保证，网络深入到国家的政府、军事、文教、企业等诸多领域，许多重要的政府宏观调控决策、商业经济信息、银行资金转账、股票证券、能源资源数据、科研数据等重要信息都通过网络存储、传输和处理，所以，难免会吸引各种主动或被动的人为攻击。例如，信息泄露、信息窃取、数据篡改、计算机病毒等。同时，通信实体还面临着诸如水灾、火灾、地震、电磁辐射等方面的考验。

关于网络信息安全的意义，从大的方面说，网络信息安全关系到国家主权的安全、社会

的稳定、民族文化的继承和发扬等；从小的方面说，网络信息安全关系到公私财物和个人隐私的安全。因此，必须设计一套完善的安全策略，采用不同的防范措施，并制定相应的安全管理规章制度来加以保护网络的安全。

近年来，计算机犯罪案件数量急剧上升，计算机犯罪已经成为一个普遍的国际性问题。据美国联邦调查局报告，计算机犯罪是商业犯罪中最大的犯罪类型之一，每笔犯罪的平均金额为45000美元，每年计算机犯罪造成的经济损失高达500亿美元。任何一个计算机犯罪案件的发生都具有无边界性、瞬时性、突发性、动态性、隐蔽性的特点。通常一个计算机犯罪案件可在很短时间内完成，并且往往很难获取犯罪者留下的证据，这大大刺激了计算机高技术犯罪案件的发生。计算机犯罪率的迅速增加，使各国的计算机系统面临着威胁，并成为严重的社会问题之一，人们已经清醒地认识到计算机系统的脆弱性和不安全性。

1.2 密码学在网络信息安全中的作用

在现实世界中，安全是一个相当简单的概念。例如，房子门窗上要安装足够坚固的锁以阻止窃贼的闯入；安装报警器是阻止入侵者破门而入的进一步措施；当有人想从他人的银行账户上骗取钱款时，出纳员要求其出示相关身份证明也是为了保证存款安全；签署商业合同时，需要双方在合同上签名以产生法律效力也是保证合同的实施安全。

在数字世界中，安全以类似的方式工作着。机密性就像大门上的锁，它可以阻止非法者闯入用户的文件夹读取用户的敏感数据或盗取钱财（如信用卡号或网上证券账户信息）。数据完整性提供了一种当某些内容被修改时可以使用户得知的机制，相当于报警器。通过认证，可以验证实体的身份，就像从银行取钱时需要用户提供合法的身份（ID）一样。基于密码体制的数字签名具有防否认功能，同样有法律效力，可使人们遵守数字领域的承诺。

以上思想是密码技术在保护信息安全方面所起作用的具体体现。密码是一门古老的技术，但自密码技术诞生直至第二次世界大战结束，对于公众而言，密码技术始终处于一种未知的保密状态，常与军事、机要、间谍等工作联系在一起，让人在感到神秘之余，又有几分畏惧。信息技术的迅速发展改变了这一切。随着计算机和通信技术的迅猛发展，大量的敏感信息常通过公共通信设施或计算机网络进行交换，特别是Internet的广泛应用、电子商务和电子政务的迅速发展，越来越多的个人信息需要严格保密，如：银行账号、个人隐私等。正是这种对信息的机密性和真实性的需求，密码学才逐渐揭去了神秘的面纱，走进公众的日常生活中。

密码技术是实现网络信息安全的核心技术，是保护数据最重要的工具之一。通过加密变换，将可读的文件变换成不可理解的乱码，从而起到保护信息和数据的作用。它直接支持机密性、完整性和非否认性。当前信息安全的主流技术和理论都是基于以算法复杂性理论为特征的现代密码学的。从Diffie和Hellman发起密码学革命起，该领域最近几十年的发展表明，信息安全技术的一个创新生长点是信息安全的编译码理论和方法的深入研究，这方面具有代表性的工作有数据加密标准DES、高级加密标准AES、RSA算法、椭圆曲线密码算法ECC、IDEA算法、PGP系统等。

今天，在计算机被广泛应用的信息时代，由于计算机网络技术的迅速发展，大量信息以

数字形式存放在计算机系统里，信息的传输则通过公共信道。这些计算机系统和公共信道在不设防的情况下是很脆弱的，容易受到攻击和破坏，信息的失窃不容易被发现，而后果可能是极其严重的。如何保护信息的安全已成为许多人感兴趣的迫切话题，作为网络安全基础理论之一的密码学引起人们的极大关注，吸引着越来越多的科技人员投入到密码学领域的研究之中。

密码学尽管在网络信息安全中具有举足轻重的作用，但密码学绝不是确保网络信息安全的惟一工具，它也不能解决所有的安全问题。同时，密码编码与密码分析是一对矛和盾的关系，俗话说："道高一尺，魔高一丈"，它们在发展中始终处于一种动态的平衡。在网络信息安全领域，除了技术之外，管理也是非常重要的一个方面。如果密码技术使用不当，或者攻击者绕过了密码技术的使用，就不可能提供真正的安全性。

1.3 密码学的发展历史

密码学的发展历程大致经历了三个阶段：古代加密方法、古典密码和近代密码。

1.3.1 古代加密方法（手工阶段）

源于应用的无穷需求总是推动技术发明和进步的直接动力。存于石刻或史书中的记载表明，许多古代文明，包括埃及人、希伯来人、亚述人都在实践中逐步发明了密码系统。从某种意义上说，战争是科学技术进步的催化剂。人类自从有了战争，就面临着通信安全的需求，密码技术源远流长。

古代加密方法大约起源于公元前 440 年出现在古希腊战争中的隐写术。当时为了安全传送军事情报，奴隶主剃光奴隶的头发，将情报写在奴隶的光头上，待头发长长后将奴隶送到另一个部落，再次剃光头发，原有的信息复现出来，从而实现这两个部落之间的秘密通信。

密码学用于通信的另一个记录是斯巴达人于公元前400年应用Scytale加密工具在军官间传递秘密信息。Scytale 实际上是一个锥形指挥棒，周围环绕一张羊皮纸，将要保密的信息写在羊皮纸上。解下羊皮纸，上面的消息杂乱无章、无法理解，但将它绕在另一个同等尺寸的棒子上后，就能看到原始的消息。

我国古代也早有以藏头诗、藏尾诗、漏格诗及绘画等形式，将要表达的真正意思或"密语"隐藏在诗文或画卷中特定位置的记载，一般人只注意诗或画的表面意境，而不会去注意或很难发现隐藏其中的"话外之音"。

由上可见，自从有了文字以来，人们为了某种需要总是想法设法隐藏某些信息，以起到保证信息安全的目的。这些古代加密方法体现了后来发展起来的密码学的若干要素，但只能限制在一定范围内使用。

传输密文的发明地是古希腊，一个叫 Aeneas Tacticus 的希腊人在《论要塞的防护》一书中对此做了最早的论述。公元前 2 世纪，一个叫 Polybius 的希腊人设计了一种将字母编码成符号对的方法，他使用了一个称为 Polybius 的校验表，这个表中包含许多后来在加密系统中非常常见的成分，如代替与换位。Polybius 校验表由一个 5×5 的网格组成（如表 1-1 所示），网格中包含 26 个英文字母，其中 I 和 J 在同一格中。每一个字母被转换成两个数字，第一个