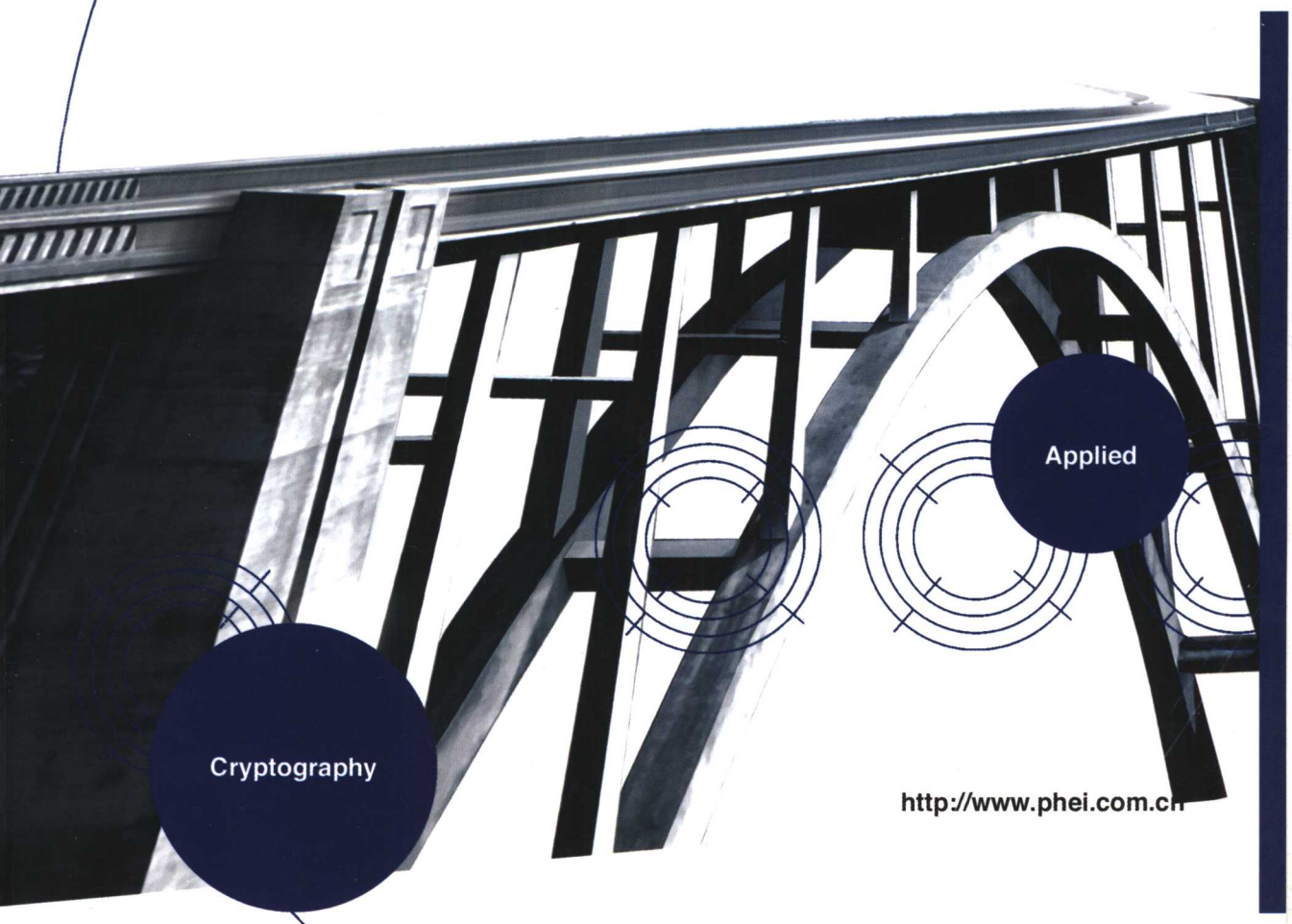
高等教育“十一五”国家级规划教材

应用密码学

胡向东　魏琴芳　编著　　王晓京　主审



http://www.phei.com.cn

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY

高等教育“十一五”国家级规划教材

应用密码学

胡向东　魏琴芳　编著

王晓京　主审

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

内 容 简 介

本书兼具专著和教材的双重属性，是作者从事多年的应用密码学相关教学和科研工作实践的结晶。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。全书共 15 章，内容涉及密码学基础、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、量子密码；书中还介绍了应用密码学在电子商务支付安全、数字通信安全、工业网络控制安全和无线传感器网络感知安全这四个典型领域的应用方法和技术。语言简练，内容重点突出，逻辑性强，算法经典实用；突出的特色是将复杂的密码算法原理分析得透彻深入，便于读者花少量的时间尽快掌握应用密码学的精髓。

本书可作为高等院校密码学、应用数学、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、系统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 / 胡向东等编著. —北京：电子工业出版社，2006.11
ISBN 7-121-03226-0

Ⅰ. 应… Ⅱ. 胡 Ⅲ. 密码-理论 Ⅳ. TN918.1

中国版本图书馆 CIP 数据核字（2006）第 119168 号

责任编辑：刘志红　　唐　霞
印　　刷：北京丰富彩艺印刷有限公司
装　　订：北京中新伟业印刷有限公司
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
开　　本：787×1092、1/16　印张：22.25　字数：541 千字
印　　次：2006 年 11 月第 1 次印刷
印　　数：5000 册　　定价：32.00 元

凡所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；邮购电话：（010）88254888。

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。

服务热线：（010）88258888。

序

随着信息化在全球的发展，互联网、电信网、广播电视网正在走向融合，计算机、通信、数码电子产品也朝着 3C 融合的方向发展，人们的社会生活对网络的依赖越来越大，信息及信息系统的安全与公众利益的关系日益密切。当人类面对外界时，人身安全是第一需求，人们需要相互传授安全防范的经验和技能。当人类步入信息社会之时，我们不难发现信息安全还是我们的第一需求，而且现在比过去任何时候都更需要普及信息安全的意识和知识。只有当这种意识和知识为工程技术人员真正掌握，并为公众所接受，整个社会的信息安全才有可靠的保障。

自 50 多年前香龙的“保密通信的信息理论”一文问世以来，密码学逐步从经验艺术走上了严谨科学的道路，成为了当今社会信息安全技术的坚实基石。不了解密码学，也很难真正驾驭信息安全。另一方面，互联网等当代信息技术领域提出的一系列信息安全新课题（其中许多还是有趣的科学问题和严肃的社会问题），反过来又推动着密码学不断深入发展和广泛应用，使密码学洋溢着生机和魅力。

密码学及其应用是跨学科的交叉研究领域，其成果和思想方法的意义已经不限于数学，甚至也不仅仅限于信息安全。国外从 20 世纪 70 年代起，密码和编码理论及技术逐渐成为许多工程学科的基础课程。事实上，它们不仅对理工科学生的训练有益，法律、管理等文科的学生也能从中吸收到思想和心智的知识养分。

现代密码学的确是建立在数学理论的基础之上的，但使用它的人绝不限于数学家，当代工程技术人员对它的需求也许更为迫切，它的应用和发展更需要普及和深入到越来越多的交叉领域中去。为了能够达到精确、简洁、优美的目的，密码学常常需要从形式化的数学层面来刻画；同时密码学也需要人们从工程应用的角度来理解它，甚至需要从逻辑常识和宽广的知识背景来介绍它和思考它，才能领会它的精髓，丰富它的内涵，灵活它的使用。

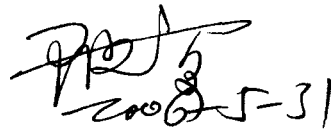
然而由于历史原因，适合工程技术人员的密码学中文教程相对较少，现代密码学的抽象形式使许多其他专业背景的人对它望而生畏，这就妨碍了它精妙思想和方法的普及。今天，网络安全等领域提出了越来越多的密码技术应用问题，客观上对应用密码学这种体裁的专著有了更广泛、更迫切的需要。

《应用密码学》使工科背景的读者多了一个选择，在一定程度上弥补了上述遗憾。这本

书的许多内容来源于作者在工程学科的密码学教学实践，注重从工程技术人员和学生易于接受的方式来介绍密码学的要领，不拘泥于细腻的理论证明和形式上的严谨。书中的一些重点章节还设置了许多有价值的具体实例，全书配有计算机 CAI 教学课件，这些对读者当不无裨益。针对当前网络安全的热点问题，作者在书中也适时地介绍了一些新的典型应用，抛砖引玉，使图书内容增色不少。

本书似也在追求一种信念：更多人的实践和思考有助于推动密码学的发展，多种风格、面向多种应用领域的应用密码学知识能够为密码学大厦添砖加瓦。读后有感，是为序。

中国科学院成都计算机应用研究所研究员、博导



前　言

随着通信和计算机技术的快速发展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、人们生产和生活息息相关领域的信息安全问题，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，凝聚自己多年的教学和科研工作实践成果，特别针对教学工作需要和学习规律完成了本书的编著工作。在本书编撰过程中，特别注重体现以下特色。

先进性。本书根据应用密码学的发展趋势，在讲清应用密码学基本概念的同时，力求对当前及未来具有很强应用前景的对称密码体制（包括序列密码）、非对称密码体制的典型密码算法的基本工作原理及其应用方法进行了系统、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，因此在密码算法的选取、例题设置和不同领域的应用方法等方面都体现出广泛的代表性和典型性。

易学性。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，在内容安排上力求层次清晰、结构合理、由浅入深、循序渐进、逻辑严密、前后呼应、主次分明、重点突出；在语言表达上力求文笔流畅、言简意赅、深入浅出、通俗易懂。

有趣性。科学是严谨的，但科学与生活并不是完全分离的，书中提供的部分背景知识增加了学习密码学的趣味性，有助于调节学习节奏，倡导和发现科学中孕育的和谐。

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。在结构上分为网络信息安全概述、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、密码学与无线传感器网络感知安全、密码学的新进展——量子密码学。每章末都给出了适量的思考题和习题作为巩固知识之用，并附有参考答案。为了方便使用，对于较高要求的部分用符号“*”标识。

本书兼具专著和教材的双重属性，突出的特色是将复杂的密码算法原理分析得透彻深入，便于读者花少量的时间尽快掌握应用密码学的精髓。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学进行动手实践，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、应用数学、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、系统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。

本书由重庆邮电大学胡向东教授组织编著，第 3，4，10，12 章由魏琴芳高工编著，胡向东负责其余章节的编著和全书的统稿。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资料的作者，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，形成一本体现自身价值、极具特色的应用密码学教材。

参加本书编写、CAI 课件和习题答案制作等工作的还包括重庆邮电大学自动化学院张毅、蔡军、张开碧、谢颖等老师；高旸、徐笑尘、易明华、余刚等研究生参与了部分资料的收集和整理工作；中科院成都计算机应用研究所的王晓京研究员对本书进行了认真细致的审阅并提供了宝贵的修改意见和建议；电子工业出版社的刘志红、康霞编辑为本书的高质量出版倾注了大量心血；在此对他们付出的辛勤劳动表示由衷的感谢。本书的编著出版受到高等教育“十一五”国家级教材规划建设项目、重庆市教委科技研究项目、重庆市科委自然科学基金计划项目和重庆邮电大学出版基金资助，并得到上海交通大学访问学者项目和江志斌教授的支持。

本书另配有相应的 CAI 课件，如有需要，请与出版社或作者联系免费索取，或从电子工业出版社华信教育资源网免费下载。

应用密码学是一门内容广泛、发展迅速的学科，对本书的编著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。我们的联系方式是：huxd@cqupt.edu.cn。

作　者

2006 年 9 月

读者调查表

尊敬的读者：

自电子工业出版社机电图书事业部开展读者调查活动以来，收到来自全国各地众多读者的积极反馈，他们除了褒奖我们所出版图书的优点外，也很客观地指出需要改进的地方。读者对我们工作的支持与关爱，将促进我们为您提供更优秀的图书。您可以填写下表寄给我们（北京万寿路 173 信箱机电图书事业部　邮编：100036），也可以发送电子邮件与我们取得联系（lzhmails@phei.com.cn），反馈您宝贵的建议和意见。我们将从中评出热心读者若干名，赠送我们出版的图书。谢谢您对我们工作的支持！

您的意见是我们创造精品的动力源泉！

姓名：_____性别：□ 男 □ 女　年龄：_____ 职业：_____

电话（手机）：_____ E-mail:_____

传真：_____ 通信地址：_____

邮编：_____

1. 影响您购买同类图书因素（可多选）：

□封面封底　□价格　□内容提要、前言和目录　□书评广告　□出版社名声

□作者名声　□正文内容　□其他_____

2. 您对本事业部图书的满意度：

从技术角度　□很满意　□比较满意　□一般　□较不满意　□不满意

从文字角度　□很满意　□比较满意　□一般　□较不满意　□不满意

从排版、封面设计角度　□很满意　□比较满意　□一般　□较不满意　□不满意

3. 您选购了我们哪些图书？主要用途？

_____

4. 您最喜欢我们出版的哪几本图书？请说明理由。

_____

5. 您所教课程主要参考书？请说明书名、作者、出版年份、定价、出版社。

_____

6. 目前教学您使用的是哪本教材？（请说明书名、作者、出版年、定价、出版社）有何优缺点？

_____

7. 您的相关专业领域中所涉及的新专业、新技术包括：

_____

8. 您感兴趣或希望增加的图书选题有：

_____

9. 您是否需要我们定期给您邮寄相关出版信息：　□是　　□否

邮寄地址：北京海淀区万寿路 173 信箱机电图书事业部　　邮编：100036

电话：010－88254473　E-mail: lzhmails@phei.com.cn　　联系人：刘志红

电子工业出版社机电图书事业部

机电图书事业部

机电图书事业部作为电子工业出版社主要业务部门，主要负责机械、电子、自动控制类图书的选题策划、开发、出版及营销工作。

在讲究高速度、高品质的信息时代，机电图书事业部秉承着“严谨、求实、高效、创新”的经营理念，不断整合资源，调整出版方向，增强事业部核心竞争能力，并且力求依托优秀的机械电子类图书产品、强大的专业技术力量以及优质高效的服务赢得读者的最高满意度。

目前，我们已经组织出版了包括机械设计师手册、机电一体化技术、CAD/CAM 工程应用及高等院校十一五机械类教材等系列丛书。技术“新”、内容“实”、质量“精”是机电图书事业部精品图书最大特色，也期待着能与您携手共迎机遇和挑战。

新书介绍

一、微机电系统技术与应用丛书			
7121018578	微弱信号检测技术	29.80	2005
7121019167	微惯性技术	39.80	2005
7121030314	微系统封装原理与技术	32.00（估）	2006
二、机电一体化技术丛书			
7121028921	嵌入式车载信息系统开发与应用（含光盘 1 张）	39.00	2006
7121024403	PLC 机电控制系统应用设计技术	32.00	2006
7121029286	机电一体化技术	29.80	2006
三、CAD/CAM/CAE 工程应用丛书			
7121024845	ANSYS10.0 有限元分析理论与工程应用（含光盘 1 张）	43.00	2006
7121027852	SolidWorks2006 完全学习手册——图解COSMOSWorks（含光盘 1 张）	43.00	2006
7121029030	ANSYS 高级工程应用实例分析与二次开发（含光盘 1 张）	48.00	2006
即将上市	UGNX4.0 数控加工实例教程（含光盘 1 张）	32.80（估）	2006
即将上市	UGNX4.0 机械设计实例教程（含光盘 1 张）	38.00（估）	2006
即将上市	AutoCAD2006 建筑图绘制实例教程（含光盘 1 张）	35.00（估）	2006
即将上市	AutoCAD2006 机械图绘制实例教程（含光盘 1 张）	35.00（估）	2006
四、机械设计师手册			
7121027909	机械设计师手册（上册） **（重点推荐）**	99.80	2006
7121027917	机械设计师手册（中册） **（重点推荐）**	99.80	2006
7121027925	机械设计师手册（下册） **（重点推荐）**	99.80	2006
五、高等院校十一五机械类统编教材			
7121030063	机械工程控制基础	21.00	2006
7121027267	画法几何基础及机械制图习题集	19.80	2006
7121027250	画法几何基础及机械制图	35.00	2006
六、其他			
7121030292	数控加工设备控制系统维修技术大全 **（重点推荐）**	89.00	2006
7121020181	机械设计习题与解答	19.80	2006

电子工业出版社机电图书事业部地址：
北京市万寿路 173 信箱电子工业出版社华信大厦 1017 室
邮　　编：100036　　电话：010-88254473
欢迎投稿：lzhmails@phei.com.cn

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY

反侵权盗版声明

举报电话：（010）88254396；（010）88258888

传　　真：（010）88254397

E-mail：　dbqq@phei.com.cn

通信地址：北京市万寿路 173 信箱

　　电子工业出版社总编办公室

邮　　编：100036

目　录