重庆市普通高等教育本科“十二五”规划教材

重点大学信息安全专业规划系列教材

应用密码学（第3版）

胡向东 魏琴芳 胡蓉 编著

清华大学出版社

重庆市普通高等教育本科“十二五”规划教材

重点大学信息安全专业规划系列教材

应用密码学（第3版）

胡向东 魏琴芳 胡蓉 编著

清华大学出版社
北京

内 容 简 介

本书属重庆市普通高等教育本科“十二五”规划教材，第1版为普通高等教育“十一五”国家级规划教材。本书全面介绍了密码学的基本概念、基本理论和典型实用技术。全书共13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、杂凑算法和消息认证、数字签名、密钥管理、序列密码、密码学的新进展、中国商用密码算法标准和密码学应用与实践。本书突出的特色是深入浅出地分析复杂的密码算法原理，详解中国商用密码算法标准，并结合实例介绍密码学的典型应用，重点培养学生的密码学工程实践技能。

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、物联网工程、智能电网信息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。尤其适合对学习密码学感到困难的初学者。

图书在版编目(CIP)数据

应用密码学/胡向东，魏琴芳，胡蓉编著. —3版. —北京：清华大学出版社，2014
重点大学信息安全专业规划系列教材
ISBN 978-7-302-36044-5

Ⅰ. ①应… Ⅱ. ①胡… ②魏… ③胡… Ⅲ. ①密码－理论－高等学校－教材 Ⅳ. ①TN918.1

中国版本图书馆CIP数据核字(2014)第066006号

责任编辑：付弘宇　李　晔
封面设计：常雪影
责任校对：梁　毅
责任印制：宋　林

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦A座　　邮　　编：100084
社 总 机：010-62770175　　邮　　购：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质 量 反 馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课 件 下 载：http://www.tup.com.cn，010-62795954

印 装 者：北京国马印刷厂
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张**：24.25　　**字　　数**：603千字
版　　次：2006年11月第1版　2014年7月第3版　　**印　　次**：2014年7月第1次印刷
印　　数：1～2000
定　　价：44.50元

产品编号：058496-01

INTRODUCTION

出版说明

由于网络应用越来越普及，信息化的社会已经呈现出越来越广阔的前景，可以肯定地说，在未来的社会中，电子支付、电子银行、电子政务以及多方面的网络信息服务将深入到人类生活的方方面面。同时，随之面临的信息安全问题也日益突出，非法访问、信息窃取，甚至信息犯罪等恶意行为导致信息的严重不安全。信息安全问题已由原来的军事国防领域扩展到整个社会，因此社会各界对信息安全人才有强烈的需求。

信息安全本科专业是2000年以来结合我国特色开设的新的本科专业，是计算机、通信、数学等领域的交叉学科，主要研究确保信息安全的科学和技术。自专业创办以来，各个高校在课程设置和教材研究上一直处于探索阶段。但各高校由于本身专业设置上来自于不同的学科，如计算机、通信和数学等，在课程设置上也没有统一的指导规范，在课程内容、深浅程度和课程衔接上，存在模糊不清、内容重叠、知识覆盖不全面等现象。因此，根据信息安全类专业知识体系所覆盖的知识点，系统地研究目前信息安全专业教学所涉及的核心技术的原理、实践及其应用，合理规划信息安全专业的核心课程，在此基础上提出适合我国信息安全专业教学和人才培养的核心课程的内容框架和知识体系，并在此基础上设计新的教学模式和教学方法，对进一步提高国内信息安全专业的教学水平和质量具有重要的意义。

为了进一步提高国内信息安全专业课程的教学水平和质量，培养适应社会经济发展需要的、兼具研究能力和工程能力的高质量专业技术人才。在教育部相关教学指导委员会专家的指导和建议下，清华大学出版社与国内多所重点大学共同对我国信息安全人才培养的课程框架和知识体系，以及实践教学内容进行了深入的研究，并在该基础上形成了“信息安全人才需求与专业知识体系、课程体系的研究”等研究报告。

本系列教材是在课程体系的研究基础上总结、完善而成，力求充分体现科学性、先进性、工程性，突出专业核心课程的教材，兼顾具有专业教学特点的相关基础课程教材，探索具有发展潜力的选修课程教材，满足高校多层次教学的需要。

本系列教材在规划过程中体现了如下一些基本组织原则和特点。

(1) 反映信息安全学科的发展和专业教育的改革,适应社会对信息安全人才的培养需求,教材内容坚持基本理论的扎实和清晰,反映基本理论和原理的综合应用,在其基础上强调工程实践环节,并及时反映教学体系的调整和教学内容的更新。

(2) 反映教学需要,促进教学发展。教材要适应多样化的教学需要,正确把握教学内容和课程体系的改革方向,在选择教材内容和编写体系时注意体现素质教育、创新能力与实践能力的培养,为学生知识、能力、素质协调发展创造条件。

(3) 实施精品战略,突出重点。规划教材建设把重点放在专业核心(基础)课程的教材建设上;特别注意选择并安排一部分原来基础比较好的优秀教材或讲义修订再版,逐步形成精品教材;提倡并鼓励编写体现工程型和应用型的专业教学内容和课程体系改革成果的教材。

(4) 支持一纲多本,合理配套。专业核心课和相关基础课的教材要配套,同一门课程可以有多本具有各自内容特点的教材。处理好教材统一性与多样化,基本教材与辅助教材、教学参考书,文字教材与软件教材的关系,实现教材系列资源的配套。

(5) 依靠专家,择优落实。在制定教材规划时,依靠各课程专家在调查研究本课程教材建设现状的基础上提出规划选题。在落实主编人选时,要引入竞争机制,通过申报、评审确定主编。书稿完成后认真实行审稿程序,确保出书质量。

繁荣教材出版事业,提高教材质量的关键是教师。建立一支高水平的、以老带新的教材编写队伍才能保证教材的编写质量,希望有志于教材建设的教师能够加入到我们的编写队伍中来。

重点大学信息安全专业规划系列教材

联系人:魏江江 weijj@tup.tsinghua.edu.cn

FOREWORD

前言

本书属重庆市普通高等教育本科“十二五”规划教材，第 1 版是普通高等教育“十一五”国家级规划教材。已先后被东华大学、上海交通大学、中山大学、贵州大学、黑龙江大学、西南科技大学、桂林电子科技大学、烟台大学、解放军信息工程大学、海军大连舰艇学院、北京工业大学、南京工业大学、湖北工业大学、安徽师范大学、杭州师范大学、曲阜师范大学、成都东软信息技术职业学院等国内数十所高校选用。

该教材经过十余年的教学实践，积累了较丰富的教学经验，其间经历三次改版，紧跟技术和应用的发展，遵从教学目标的递进。目前，国内外的信息技术及其应用得到了快速发展，特别是随着移动互联网、物联网、云计算技术的兴起及其层出不穷的应用推动，信息技术的覆盖领域和影响范围得以极大的拓展，正快速地改变着人们的工作模式和生活习惯；与此同时，新出现的信息安全问题如影随形，如美国“棱镜”计划的曝光为每一个信息服务的提供者和使用者都敲响了警钟，信息安全需求与日俱增，越来越多的人认识到信息安全的重要性，密码学保障信息安全的基础性地位得以突显，且密码学已深入人们日常生产生活的方方面面，掌握密码学是对信息安全类专门人才的基本要求，了解密码学已成为普通民众保护自身利益和隐私的一种基本需求。

为了更好地适应国内信息安全和密码学教学需要，更有效地展现密码学的核心内容与典型应用，在收集学生和教师等广大读者意见的基础上，结合新的教学目标定位与国内信息安全应用需求，对《应用密码学》第 2 版的内容进行了系统优化与全面梳理，在充分保留其“易学性”、“有趣性”、“先进性”、“典型性”、“工程性”等特色基础上，新版进一步强化了密码学的工程实践、“本土特色”与生活体验，使现代密码学原理、方法和工程应用结合更加紧密；首次全面引入中国国家商用密码算法标准的介绍，精选并更新了贴近生产生活实际的密码学典型应用案例，以便读者结合国情了解中国密码算法的发展与应用现状，增强读者对密码应用的现实感和信息安全的紧迫性，强化信息安全意识。书中涉及的多个具有代表性的密码算法已完成 C 语言实现和测试，能容易地动手实践。提供的导学表和交流与微思考项目有助于对学生学习的引领和目标导向，并训练其“学思交融”的学习模式，积极实践“授人以

渔”的教学要求和写作定位。

“学而不思则罔，思而不学则殆”

本书以密码故事开篇，全面介绍了密码学的基本概念、基本理论和典型实用技术；重点介绍密码学原理和密码学应用与实践。全书共13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、杂凑算法和消息认证、数字签名、密钥管理、序列密码、密码学的新进展、中国商用密码算法标准以及密码学应用与实践。每一章首先给出引领学习的导学表，内容包括本章的知识单元与知识点、能力点、重难点和学习要求；根据需要设置交流与微思考项目；除第0章外，每章末都给出了适量的习题作为巩固知识之用，并在附录中给出了部分习题的参考答案。

教师可在48~56学时内讲解全部或选讲部分内容，还可以配以适当的机时进行动手实践，在有限的时间内使学生快速掌握密码学的核心内容，提高学习效率。本书另配有相应的PPT教学课件、章后习题参考答案(完全版)和两个密码故事的视频资料，如果需要，请与出版社或编著者联系索取。

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、物联网工程、智能电网信息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管理、应用和设计开发的研究人员、工程技术人员参考。尤其适合对学习密码学感到困难的初学者。

本书由胡向东教授组织编写并题写书名，第3、4、10、13章由魏琴芳、胡蓉编著，胡向东负责其余章节的编著与全书的统稿；研究生牟海明完成了部分算法的仿真测试。韩恺敏、许宏如、成勇、秦晓鹏、王凯、徐慧芬、贾子漠、刘竹林、熊文韬、王鹏、唐飞、王瑞、赵润生、程利娜、陈国军、林家富等研究生参与了资料的整理、图表的绘制、教学课件和习题答案的制作等，胡尔婉设计制作了习题云图标。要特别感谢参考文献中所列的各位作者，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编著者提供了宝贵的资料和丰富的写作源泉，使我们能够在总结教学和科研工作成果的基础上，汲取各家之长，形成一本定位明确、适应需求、颇具特色并广受欢迎的密码学教材。清华大学出版社的工作人员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。本书的编著出版得到重庆市高等教育教学改革研究重大课题(1201004)和一般课题(113029)的指导，同时得到了国家自然科学基金项目(61170219)、重庆市基础与前沿研究计划项目(cstc2013jcyjA40002)和重庆市高等学校优秀人才支持计划项目(渝教人〔2011〕65号)的资助。

密码学地位特殊、内涵丰富、应用广泛、发展迅速，对本书的修订是我们在此领域的第三番努力尝试。限于编著者的水平和学识，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。联系方式：huxd@ cqupt.edu.cn。

编者著

2014年1月

CONTENTS

目录

开篇　密码学典故

上篇　密码学原理

下篇 密码学应用与实践

开篇　密码学典故

CHAPTER 0

密码故事　　第0章

知识单元与知识点

➢ 信息隐藏、密码、加密、解密、破译、换位、代替、摩斯电码等概念；

➢ 历史与现实工作、生活中的密码学应用。

能力点

◇ 初步建立密码学的基本概念；

◇ 初步认识密码学在工作、生活中的意义；

◇ 初步理解密码学的重要性。

重难点

■ 重点：密码学的基本概念与作用。

■ 难点：对破译方法与过程的认识。

学习要求

√ 了解密码学的相关概念；

√ 通过案例了解关于密码学的典型应用；

√ 建立学习密码学的浓厚兴趣。

密码学是一门古老而年轻的科学。密码学经历了几千年的演化与发展，形成了丰富的内涵，并得到了广泛的应用。密码学起源于信息隐藏，就是为了达到机密信息不被非授权地获知的目的而采取的某种手段或方式。现代密码学主要基于数学或物理的方法进行某种变换来实现。密码学曾经高深莫测、讳莫如深，主要用于国家外交或军事等重要领域；现在密码学与百姓的平常生活和工作息息相关，已成长为网络信息安全的基石。密码学在长期的发展过程中衍生出了许多或惊险刺激、或温婉动人的故事。为了激发出读者浓厚的兴趣进而学好这门课程，我们就从“讲故事”开始吧。