重点大学信息安全专业规划系列教材

现代密码学（第2版）

许春香 李发根 汪小芬 禹勇 聂旭云 编著

清华大学出版社

重点大学信息安全专业规划系列教材

现代密码学（第2版）

许春香 李发根 汪小芬 禹勇 聂旭云 编著

清华大学出版社
北京

内 容 简 介

本书系统介绍了密码学的基本知识，包括古典密码、流密码、分组密码、Hash 函数、公钥密码、数字签名、密码协议、可证明安全性理论、基于身份的密码体制、无证书密码体制和密码学的新方向。

本书内容全面、概念准确、语言精练，力求使用简单的语言来描述复杂的密码学算法和安全性分析问题。本书既可作为信息安全、计算机、通信工程等专业本科生和研究生的教材，也可以作为密码学和信息安全领域的教师、科研人员与工程技术人员的参考书。

图书在版编目(CIP)数据

现代密码学/许春香等编著. --2 版. --北京：清华大学出版社，2015
重点大学信息安全专业规划系列教材
ISBN 978-7-302-37043-7

Ⅰ. ①现… Ⅱ. ①许… 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 143077 号

责任编辑：付弘宇　李　晔
封面设计：傅瑞学
责任校对：时翠兰
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 刷 者：北京富博印刷有限公司
装 订 者：北京市密云县京文制本装订厂
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　张**：12　　**字　数**：294 千字
版　　次：2008 年 11 月第 1 版　2015 年 1 月第 2 版　　**印　次**：2015 年 1 月第1 次印刷
印　　数：1～2000
定　　价：25.00 元

产品编号：039746-01

丛书编委会

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

PREFACE

丛书序

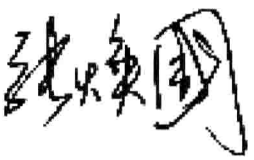
随着信息技术与产业的快速发展，信息和信息系统已经成为现代社会中最为重要的基础资源之一。人们在享受信息技术带来的便利的同时，诸如黑客攻击、计算机病毒泛滥等信息安全事件也层出不穷，信息安全的形势是严峻的。党的十八大明确指出：要“高度关注海洋、太空、网络空间安全”。加快国家信息安全保障体系建设，确保我国的信息安全，已经成为我国的国家战略。而发展我国信息安全技术与产业对于确保我国信息安全具有重要意义。

信息安全作为信息技术领域的朝阳产业，亟须大量的高素质人才。但与此相悖的是，目前我国信息安全技术人才的数量和质量远远不能满足社会的实际需求。因此，培养大量的高素质、高技术信息安全专业人才已成为我国本科高等工程教育领域的重要任务。

信息安全是一门集计算机、通信、电子、数学、物理、生物、法律、管理和教育等学科知识为一体的交叉型新学科。探索该学科的培养模式和课程设置是信息安全人才培养的首要问题。为此，电子科技大学计算机科学与工程学院信息安全专业的专家学者和工作在教学一线的老师们，以我国本科高等工程教育人才培养目标为宗旨，组织了一系列信息安全的研讨活动，认真研讨了国内外高等院校信息安全专业的教学体系和课程设置，在进行了大量前瞻性研究的基础上，启动了系列教材的编写工作。该套系列教材由《信息安全概论》、《计算机系统与网络防御技术》、《PKI 原理与技术》、《网络安全协议》、《信息安全数学基础》、《密码学基础》等构成。全方位、多角度地阐述信息安全技术的原理，反映当代信息安全研究发展的趋势，突出实践在高等工程教育人才培养中的重要性，为该套丛书的最大特点。

感谢电子科技大学信息安全专业的老师们为促进我国高等院校信息安全专业建设所付出的辛勤劳动，相信这套教材一定会成为我国高等院校信息安全人才培养的优秀教材。同时希望电子科技大学的教师们继续努力，培养

出更多、更优秀的信息安全人才,编写出更多、更好的信息安全教材,为推动我国信息安全事业的发展做出更大的贡献。



2013年8月2日

张焕国　教授
武汉大学计算机学院
空天信息安全与可信计算教育部重点实验室

FOREWORD

前言

密码学可以划分为古典密码学和现代密码学。古典密码学可以追溯到古罗马时期，而现代密码学主要是在第二次世界大战以后发展起来的。

本书分为13章，主要讨论现代密码学，为读者掌握和应用现代密码技术打下基础，但为了使读者全面了解密码学的历史，本书在第3章也简单介绍了古典密码学。学习现代密码学并不需要先学习古典密码学作为基础，但熟悉古典密码学对理解现代密码学是有帮助的，建议有兴趣的读者阅读古典密码学的相关著作。

第4~8章介绍现代密码学的基础体系，包括流密码、分组密码、Hash函数、公钥密码和数字签名。这个体系又可以分为三个环节：流密码是一个环节，分组密码是一个环节，其余部分属于一个环节。这三个环节联系并不紧密，不能认为前面环节是后面环节的基础，读者在阅读本书时需要注意这个特点。

在本书介绍的基础体系中，流密码技术环节主要讨论序列的随机性、线性移位寄存器以及两个普遍使用的流密码算法RC4和A5；分组密码技术环节主要讨论分组密码的工作模式，第一代公开的、完全说明实现细节的商用密码算法DES，国际数据加密算法IDEA，高级加密标准AES以及我国官方公布的第一个商用密码算法SMS4；第三个环节主要讨论RSA、ElGamal公钥密码、Rabin公钥密码、椭圆曲线公钥密码算法和RSA数字签名等数字签名算法以及MD5和SHA等Hash函数。

密码协议是应用上述基础体系中的密码技术所构建的协议，第9章主要讨论几种常用的密码协议。

第10章介绍密码体制可证明安全性理论，包括公钥加密体制的安全概念及其证明方法、数字签名体制的安全概念及其证明方法和几种具体的可证明安全的密码体制。

第11章介绍基于身份的密码体制，包括双线性配对、基于身份的加密体制、基于身份的签名体制、基于身份的密钥协商协议和基于身份的签密体制。

第12章讨论无证书密码体制，包括无证书加密体制、无证书签名体制、

无证书密钥协商协议和无证书签密体制。

第13章介绍密码学的新方向,包括量子密码学、变量公钥密码、基于格的公钥密码和DNA密码学。

本书可以作为信息安全专业、计算机专业、通信工程专业本科生和研究生的教材,也可以作为密码学和信息安全领域的教师、科研人员与工程技术人员的参考书。在作为本科生教材时,可以只讲授前9章内容;在作为研究生教材时,可以将后4章内容也作为讲授内容。

本书是在笔者编写的《现代密码学》(电子科技大学出版社,2008年11月出版)的基础上修订而成的。主要修订的部分为数学基础、古典密码、Hash函数、可证明安全性理论、基于身份的密码体制和无证书密码体制。

衷心感谢郝玉洁等老师,她们的大力推动是本书写作的动力,最后衷心感谢电子科技大学计算机学院的领导和同事们在本书编写期间给予的支持和帮助。

编者

2014年4月

于电子科技大学

CONTENTS

目录

CHAPTER 1

第1章 引 言

21世纪是信息的时代，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。在信息时代的今天，任何一个国家的政治、军事和外交都离不开信息，经济建设、科学发展和技术进步同样离不开信息，社会的信息化已经成为当今世界发展的潮流。计算机和网络技术的快速发展，使得整个社会的信息化程度愈来愈高，拥有更多的信息意味着在竞争中抢占先机。然而，现代信息技术是一把双刃剑，它一方面给人们带来了巨大的利益，另一方面又给人们带来了潜在的威胁。Internet的出现和发展为人类交换信息，促进科技、文化、教育和生产的发展，提高人们的生活质量提供了极大的便利。然而，正是因为Internet的开放性和无政府性，给不法分子以可乘之机，他们经常试图窃取重要情报、倾泻信息垃圾、进行网络诈骗、散发破坏性信息等。因此，信息安全已经成为世界各国共同关注的一个重要问题。所谓信息安全，是指保护信息及信息系统在信息存储、处理和传输过程中不被非法用户访问或修改，而且对合法用户不会拒绝服务，其核心内容是保护信息的机密性和认证性。

密码技术是保证信息安全的核心技术，密码学能为信息安全提供关键理论和技术支持，在信息安全领域中占有极其重要的地位。本书系统介绍了密码学的体系结构、基础知识以及在信息安全中发挥着重要作用的各种密码理论和技术。

1.1 密码学的发展历史

密码学，这门古老而年轻的科学，是信息安全的核心技术。回顾密码学的发展，如同翻开一本内容丰富、充满传奇色彩的故事书。人类对密码的研究和应用已有几千年的历史，从4000年前的古埃及到上个世纪的两次世界大战，密码学一直扮演着极其重要的角色。

古罗马的凯撒大帝第一次将密码术应用到人类实践中。当时，凯撒大帝利用传信兵与前线的将军们通信，为了防止传信兵中途被抓或者篡改信件，