

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。

本书封面贴有清华大学出版社防伪标签,无标签者不得销售。

版权所有,侵权必究。侵权举报电话:010-62782989 13701121933

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

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个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

P R E F A C E

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,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

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

目录

第 1 章 引言	1
1.1 密码学的发展历史	1
1.2 密码学基本概念	2
1.2.1 保密通信系统	3
1.2.2 密码体制分类	3
1.2.3 密码攻击	4
习题	5
第 2 章 数学基础	6
2.1 数论基础	6
2.1.1 整除与同余	6
2.1.2 欧几里得除法	8
2.1.3 一次同余式与中国剩余定理	9
2.1.4 二次剩余	10
2.2 近世代数基础	12
2.2.1 群	12
2.2.2 环和域	13
2.2.3 指数与原根	13
2.3 计算复杂性理论	14
2.3.1 图灵机	14
2.3.2 问题的计算复杂性分类	16
习题	17
第 3 章 古典密码	18
3.1 置换密码	18
3.2 代替密码	18

3.2.1	单表代替密码	19
3.2.2	多表代换密码	22
习题	24
第4章	流密码	25
4.1	基本概念	25
4.1.1	一次一密与流密码	25
4.1.2	流密码的思想	26
4.1.3	流密码结构	26
4.2	序列的随机性	27
4.3	密钥流生成器	28
4.4	线性反馈移位寄存器	29
4.5	两个流密码算法	32
4.5.1	流密码算法 RC4	32
4.5.2	流密码算法 A5	34
习题	35
第5章	分组密码	36
5.1	分组密码的基本原理	36
5.2	分组密码的工作模式	38
5.3	数据加密标准	40
5.3.1	DES 的历史	40
5.3.2	DES 算法	41
5.3.3	DES 的安全性	46
5.3.4	多重 DES	47
5.4	高级加密标准	48
5.4.1	AES 的基本运算单位	48
5.4.2	AES 算法	50
5.4.3	AES 的安全性	55
5.5	SMS4	56
5.5.1	术语说明	56
5.5.2	轮函数 F	56
5.5.3	SMS4 算法	57
5.5.4	密钥扩展算法	58
5.6	IDEA	59
5.6.1	IDEA 算法	59
5.6.2	IDEA 的安全性	61
习题	61

第 6 章 Hash 函数	62
6.1 Hash 函数的概念	62
6.1.1 Hash 函数的性质	62
6.1.2 迭代型 Hash 函数的一般结构	63
6.1.3 Hash 函数的应用	63
6.2 MD5	64
6.2.1 算法描述	64
6.2.2 MD5 的压缩函数	66
6.3 SHA	68
6.3.1 SHA-1	68
6.3.2 SHA-2	72
6.4 基于分组密码的 Hash 函数	75
6.5 Hash 函数的分析方法	76
习题	77
第 7 章 公钥密码	79
7.1 公钥密码的基本概念	79
7.1.1 公钥密码体制的原理	79
7.1.2 公钥密码体制的要求	81
7.2 RSA 公钥密码	82
7.2.1 算法描述	82
7.2.2 RSA 的安全性	84
7.3 ElGamal 公钥密码	85
7.3.1 算法描述	85
7.3.2 ElGamal 的安全性	86
7.4 Rabin 公钥密码	86
7.5 椭圆曲线公钥密码	87
7.5.1 实数域上的椭圆曲线	87
7.5.2 有限域上的椭圆曲线	88
7.5.3 椭圆曲线密码体制	89
习题	91
第 8 章 数字签名	92
8.1 数字签名的基本概念	92
8.2 RSA 数字签名	93
8.3 ElGamal 数字签名	94
8.4 数字签名标准	95
8.5 其他数字签名	96

8.5.1	基于离散对数问题的数字签名	96
8.5.2	基于大整数分解问题的数字签名	99
8.5.3	具有特殊用途的数字签名	100
习题	102
第9章	密码协议	104
9.1	密钥分配	104
9.1.1	Needham-Schroeder 协议	105
9.1.2	Kerberos	106
9.2	密钥协商	107
9.2.1	Diffie-Hellman 密钥交换协议	107
9.2.2	端到端协议	108
9.3	秘密共享	109
9.3.1	Shamir 门限方案	109
9.3.2	可验证秘密共享	110
9.3.3	无可信中心的秘密共享	111
9.4	身份识别	112
9.4.1	身份识别的概念	112
9.4.2	Guillou-Quisquater 身份识别方案	112
9.5	零知识证明	113
9.6	签密	115
习题	116
第10章	可证明安全性理论	117
10.1	可证明安全性理论的基本概念	117
10.1.1	公钥加密体制的安全性	117
10.1.2	数字签名体制的安全性	120
10.1.3	随机预言模型与标准模型	122
10.2	可证明安全的公钥加密体制	123
10.2.1	实际加密算法的安全性	123
10.2.2	RSA-OAEP	125
10.2.3	将 CPA 体制变成 CCA2 体制	127
10.3	可证明安全的数字签名体制	128
10.3.1	实际签名算法的安全性	128
10.3.2	RSA-PSS	129
习题	130
第11章	基于身份的密码体制	131
11.1	公钥认证方法	131

11.2	基于身份的加密体制	133
11.2.1	双线性配对	133
11.2.2	形式化模型	134
11.2.3	BF 方案	136
11.3	基于身份的签名体制	140
11.3.1	形式化模型	140
11.3.2	Hess 方案	142
11.3.3	CC 方案	143
11.4	基于身份的密钥协商协议	143
11.4.1	Smart 协议	143
11.4.2	Shim 协议	144
11.5	基于身份的签密体制	145
	习题	146
第 12 章	无证书密码体制	147
12.1	无证书加密体制	147
12.1.1	形式化模型	147
12.1.2	AP 方案	150
12.2	无证书签名体制	152
12.2.1	形式化模型	152
12.2.2	ZWXF 方案	155
12.3	无证书密钥协商协议	155
12.4	无证书签密体制	157
	习题	158
第 13 章	密码学的新方向	159
13.1	量子密码学	159
13.1.1	Bennett-Brassard 量子密钥分配协议	159
13.1.2	量子密码的应用与进展	160
13.2	变量公钥密码	161
13.2.1	多变量公钥密码体制的一般形式	162
13.2.2	MI 多变量公钥密码体制	162
13.2.3	彩虹: 多层油醋签名体制	164
13.2.4	多变量公钥密码体制的现状	166
13.3	基于格的公钥密码体制	166
13.3.1	数学背景	167
13.3.2	NTRU 公钥加密体制	169

13.4 DNA 密码学.....	170
13.4.1 DNA 计算.....	171
13.4.2 DNA 加密技术.....	172
13.4.3 DNA 密码发展的趋势.....	174
习题	175
参考文献.....	176

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,

凯撒采用了一种特殊的写信方式:将字母按顺序推后3位,即将字母A写为D,将字母B写为E,以此类推。信件写完后,凯撒将信件卷起,在封口滴上厚厚的蜡,在蜡未干以前,压上自己的私印。将军收到信件以后,首先检查蜡封是否完整,蜡印是否是凯撒的印章,然后才拆开信件,按照只有他和凯撒才知道的字母替换规律读信。在现在的密码学教科书上,我们仍然可以找到这种加密方法,即凯撒密码。

密码学在第二次世界大战期间也发挥了重要作用。1918年,为了保护银行通信安全,德国人 Arthur Scheribius 发明了第一台被称为 ENIGMA 的非手工编码密码机。第二次世界大战期间,这种密码机的加密通信能力被德国人用于军事,为德军在第二次世界大战初期的胜利起到了重要作用,让盟军大伤脑筋。后来,波兰人 Marian Rejewski 初步破解了 ENIGMA,随后,英国人 Alan Turing 更是终结了 ENIGMA,盟军随后开发了称为 Colossus 的机器。很多学者认为成功破解 ENIGMA 使得第二次世界大战提前一年结束。然而,密码学作为一门科学则仅仅是近60多年的事情。1948年,Shannon 发表了划时代的“通信的数学理论”,宣告了信息论的诞生。随后,Shannon 发表了著名的“保密系统的通信理论”一文,用信息论观点对信息保密问题做了全面的论述。该文将密码学的研究纳入了科学的轨道,同时,为对称密码学的构建提供了直接的理论基础。

为了解决对称密码系统中密钥分发和管理问题,1976年,Diffie 和 Hellman 在他们的经典论文“密码学的新方向”中提出了一种允许通信双方在不安全信道上安全地协商密钥的协议,即著名的 Diffie-Hellman 协议。在此基础上,他们提出了公钥密码学的概念。因此,这篇经典的论文成为密码学的研究和应用由传统走向现代的标志。虽然他们没有构造出一个具体的公钥密码系统,而只猜测其存在,但是他们的工作引起了密码学界的广泛关注。

1978年,Rivest、Shamir 和 Adleman 提出了著名的 RSA 公钥密码体制,这是第一个实用的公钥密码体制,由于他们的杰出贡献,他们获得了2002年的图灵奖。30多年来,虽然 RSA 公钥密码体制经历了风风雨雨,但是仍然是目前应用最为广泛的密码体制之一。随后,其他学者和研究人员基于其他的数学难题提出了大量的公钥密码算法。其中的代表方案有基于大整数分解问题的 Rabin 算法、基于离散对数问题的 ElGamal 算法以及近来受到广泛关注的基于椭圆曲线的密码算法等。

30多年来,公钥密码学的研究如雨后春笋,密码学研究者相继提出了一系列公钥密码算法,还提出了很多新的概念和应用,如数字签名、认证协议、基于身份的密码体制、数字签密等。在经历了几千年的历史后,密码学这门古老的艺术现在已经成为一门公开而活跃的学科。

1.2 密码学基本概念

密码学是主要研究通信安全保密的学科,它包括两个分支:密码编码学与密码分析学。密码编码学主要研究对消息进行变化,以保护信息在信道的传输过程中不被敌手窃取、解读和利用的方法;而密码分析学则恰恰相反,它主要研究如何分析和破译密码。这两个分支既相互对立,又相互促进。