普通高等教育“十一五”国家级规划教材

Springer

高·等·院·校·信·息·安·全·专·业·系·列·教·材

教育部信息安全类专业教学指导委员会与中国计算机学会教育专业委员会共同指导

Introduction to Cryptography: Principles and Applications

密码学导引：原理与应用

Hans Delfs, Helmut Knebl 著

肖国镇　张宁　译　　王育民　审

http://www.tup.com.cn

清华大学出版社

普通高等教育“十一五”国家级规划教材

Springer

高·等·院·校·信·息·安·全·专·业·系·列·教·材

Introduction to Cryptography: Principles and Applications

密码学导引：原理与应用

Hans Delfs, Helmut Knebl 著

肖国镇 张宁 译　　王育民 审

国家自然科学基金项目资助
(批准号：60473028)

清华大学出版社

北京

ISBN: 3-540-42278-1

图书在版编目(CIP)数据

密码学导引：原理与应用/德尔夫斯(Delfs, H.)，克内贝尔(Knebl, H.)著；肖国镇，张宁译. —北京：清华大学出版社，2008.1
(高等院校信息安全专业系列教材)
书名原文：Introduction to Cryptography: Principles and Applications
ISBN 978-7-302-15679-6

Ⅰ. 密… Ⅱ. ①德… ②克… ③肖… ④张… 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(2007)第 106277 号

责任编辑：张 民 李玮琪
责任校对：李建庄
责任印制：李红英

出版发行：清华大学出版社
http://www.tup.com.cn
c-service@tup.tsinghua.edu.cn
社 总 机：010-62770175
投稿咨询：010-62772015
地 址：北京清华大学学研大厦 A 座
邮 编：100084
邮购热线：010-62786544
客户服务：010-62776969

印 刷 者：北京市清华园胶印厂
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：185×230 **印 张**：17.75 **字 数**：364 千字
版 次：2008 年 1 月第 1 版 **印 次**：2008 年 1 月第 1 次印刷
印 数：1～4000
定 价：29.00 元

高等院校信息安全专业系列教材

编审委员会

出版说明

21世纪是信息时代，信息已成为社会发展的重要战略资源，社会的信息化已成为当今世界发展的潮流和核心，而信息安全在信息社会中将扮演极为重要的角色，它会直接关系到国家安全、企业经营和人们的日常生活。随着信息安全产业的快速发展，全球对信息安全人才的需求量不断增加，但我国目前信息安全人才极度匮乏，远远不能满足金融、商业、公安、军事和政府等部门的需求。要解决供需矛盾，必须加快信息安全人才的培养，以满足社会对信息安全人才的需求。为此，教育部继2001年批准在武汉大学开设信息安全本科专业之后，又批准了多所高等院校设立信息安全本科专业，而且许多高校和科研院所已设立了信息安全方向的具有硕士和博士学位授予权的学科点。

信息安全是计算机、通信、物理、数学等领域的交叉学科，对于这一新兴学科的培养模式和课程设置，各高校普遍缺乏经验，因此中国计算机学会教育专业委员会和清华大学出版社联合主办了“信息安全专业教育教学研讨会”等一系列研讨活动，并成立了“高等院校信息安全专业系列教材”编审委员会，由我国信息安全领域著名专家肖国镇教授担任编委会主任，共同指导“高等院校信息安全专业系列教材”的编写工作。编委会本着研究先行的指导原则，认真研讨国内外高等院校信息安全专业的教学体系和课程设置，进行了大量前瞻性的研究工作，而且这种研究工作将随着我国信息安全专业的发展不断深入。经过编委会全体委员及相关专家的推荐和审定，确定了本丛书首批教材的作者，这些作者绝大多数都是既在本专业领域有深厚的学术造诣、又在教学第一线有丰富的教学经验的学者、专家。

本系列教材是我国第一套专门针对信息安全专业的教材，其特点是：

① 体系完整、结构合理、内容先进。

② 适应面广：能够满足信息安全、计算机、通信工程等相关专业对信息安全领域课程的教材要求。

③ 立体配套：除主教材外，还配有多媒体电子教案、习题与实验指导等。

④ 版本更新及时，紧跟科学技术的新发展。

为了保证出版质量，我们坚持宁缺毋滥的原则，成熟一本，出版一本，并保持不断更新，力求将我国信息安全领域教育、科研的最新成果和成熟经验反映到教材中来。在全力做好本版教材，满足学生用书的基础上，还经由专家的推荐和审定，遴选了一批国外信息安全领域优秀的教材加入到本系列教材中，以进一步满足大家对外版书的需求。热切期望广大教师和科研工作者加入我们的队伍，同时也欢迎广大读者对本系列教材提出宝贵意见，以便我们对本系列教材的组织、编写与出版工作不断改进，为我国信息安全专业的教材建设与人才培养做出更大的贡献。

“高等院校信息安全专业系列教材”已于 2006 年初正式列入普通高等教育“十一五”国家级教材规划（见教高[2006]9 号文件《教育部关于印发普通高等教育“十一五”国家级教材规划选题的通知》）。我们会严把出版环节，保证规划教材的编校和印刷质量，按时完成出版任务。

2007 年 6 月，教育部高等学校信息安全类专业教学指导委员会成立大会暨第一次会议在北京胜利召开。本次会议由教育部高等学校信息安全类专业教学指导委员会主任单位北京工业大学和北京电子科技学院主办，清华大学出版社协办。教育部高等学校信息安全类专业教学指导委员会的成立对我国信息安全专业的发展将起到重要的指导和推动作用。“高等院校信息安全专业系列教材”将在教育部高等学校信息安全类专业教学指导委员会的组织和指导下，进一步体现科学性、系统性和新颖性，及时反映教学改革和课程建设的新成果，并随着我国信息安全学科的发展不断修订和完善。

我们的 E-mail 地址是：zhangm@tup.tsinghua.edu.cn；联系人：张民。

清华大学出版社

译者序

密码学的起源可以追溯到人类刚出现的时候。在人类开始研究如何通信的时候，同时也研究如何确保通信的机密，最先有意识地使用一些技术手段来加密信息的可能是公元前的古希腊人。他们使用的是一根叫 scytale 的棍子。送信人先将一张羊皮绕棍子螺旋形卷起来，然后把要写的信息按某种顺序写在上面，接着打开羊皮条卷，通过其他渠道将信送给收信人。如果不知道棍子的宽度（这里作为密钥）就不容易解密里面的内容的，但是收信人可以根据事先和写信人的约定，用同样的 scytale 的棍子将书信解密。后来，罗马的军队用凯撒密码（三个字母表轮换）进行通信。在随后的 19 个世纪里，人们发明了一些更为高明的加密技术，这些技术的安全性通常依赖于用户对它们的信任程度。19 世纪荷兰密码学家 Kerchoffs 提出了密码学的一个基本原则：密码系统的安全性应该完全依赖于密钥的安全性。1949 年，Shannon 发表了《保密通信的信息理论》，给密码学加上了科学的背景。同时 Shannon 证明了 Vernam 一次一密方案是当时唯一的无条件安全的密码体系。

20 世纪 70 年代，随着信息化进程的加快，信息安全和密码学越来越受到人们的重视，此时现代密码学已经初具模型。现代密码学的形成有两个标志性事件。首先，是美国国家标准局 NIST 公开征集数据加密标准，并于 1977 年确定 DES 为数据加密标准。此事件标志着公用密码算法标准的公开。DES 在超期服役近 20 年后，NIST 才开始进行高级加密标准（advanced encryption standard，AES）的研究，1999 年 8 月最后确定由比利时两位密码学家，Proton World International 公司的 Joan Daemen 博士和 Katholieke 大学（Leuven University）电机系的 Vincent Rijmen 博士所设计的 Rijdeal 算法作为 AES 的标准算法。从 DES 到 AES，公用密码的发展史开始有了一个标准模式：算法公开、方案公开征集以及公开论证。其次，是 Diffie 和 Hellman 于 1976 年发表了《密码学的新方向》，提出了公钥密码这个崭新的概念。公钥密码在信息安全中担负起密钥协商、数字签名、消息认证等重要角色，已成为最核心的密码算法。

现在的工业界和学术界对现代密码学的研究与应用都很重视，特别是近年来，许多高校都开办了信息安全相关专业，原来作为军事学的一个分支的密码学也开始成为信息安全专业本科生和研究生教育的一门重要课程。因此，我们翻译了这本国外优秀的密码学教科书。

本书的第 1 部分从第 1 章到第 4 章，介绍了密码学的基本概念，给出了对称密码和非对称密码的基础知识，适合初学者作为入门的教材。第 2 部分从第 5 章～第 10 章，从概率理论的角度出发，用了大量的篇幅介绍密码协议的分析方法和安全性证明过程。第 5 章介绍了一些基本的概率算法。第 6 章～第 8 章详细给出了概率理论在安全性分析上的应用。第 9 章和第 10 章结合以上各章的定义和定理，分析了加密和签名的可证明安全性，作者用严谨的语言讨论了各种加密和签名模型的安全性，给出安全性证明的基本概念、技巧和结论，阐明了基本概念及其相互关系。

本书可以用作教科书和参考书，适用于密码学的初学者和研究密码系统可证明安全性的专家学者。附录给出了基本的代数数论和概率论知识，大多数计算科学的学生都可以通过简单的学习掌握它们。希望学习完整证明理论的学生（和专家学者）可以通过本书的第 2 部分充分地学习可证明安全性的基本理论。本书给出的定义和定理都很精确，注解部分也详细地给出了读者可能在理解中出现的种种问题。各章后的习题能进一步帮助读者理解本章节的内容，十分有助于自学者在学习过程中掌握分析方法。

本书的作者 Hans Delfs 教授和 Helmut Knebl 教授长期从事密码编码和信息安全的教学以及科研工作，他们在 Regensburg 大学担任密码学教学期间完成了本书。

参加本书翻译的七位博士生对各自负责翻译的章节均比较熟悉。各部分分工如下：张宁负责翻译前言、目录、整理参考文献及第 3 章，陈智雄和辛向军共同翻译第 1、2 章和附录，卢明欣翻译第 4 章，汪晓芬翻译第 5，6 章，李胜强翻译第 7，8 章，陈原翻译第 9，10 章。张宁同学做了初校和文字风格的统一。最后由张宁同学统一整理和负责整部书的协调工作。有了这些同学的努力和合作，我们最后才能够顺利的出版本书的中文译本。再次感谢他们的工作。

我要特别感谢我的好友王育民教授，他以严谨负责的态度对本书做了详细的校对，给出了大量的修改意见，他为本书的出版付出的精力和心血是十分宝贵的。

虽然我们尽可能地完善此项翻译工作，但是有些地方的译文未必十分准确，甚至会有些错误，敬请读者批评和指正。

本书在翻译过程中受到了国家自然科学基金项目（编号：60473028）的资助，在此表示感谢。

西安电子科技大学 肖国镇

2007 年 10 月 于西安电子科技大学

原书序

随着电子通信的发展，信息安全在实际应用中越来越重要了。在世界上任何一个地方都可以公开接入计算机网络，在其中交换的消息要求保证完整性并保护消息不被复制。电子商务还需要法律范畴上的有效的数字签名以及安全的支付协议。现代密码学对所有的此类问题提供了解决的方案。

本书源于 Nurnberg 的 Georg-Simon-Ohm 应用科学大学计算机科学专业学生的课程，是给计算机科学、数学以及电子工程专业高年级本科生和研究生开设的密码学课程讲义。

本书的第 1 部分（第 1～4 章）从本科生的理解水平介绍了对称密码体制和非对称密码体制中的加密方案以及数字签名方案，还介绍了有关密码协议，比如，身份认证、电子选举以及电子现金。这一部分重点讨论模代数学和以模代数学为基础的非对称密码学。因为在这一部分中我们没有提及概率理论，所以对于一些非正式的定义（比如单向函数和抗碰撞的杂凑函数）我们给出了必要的介绍。

本书第 2 部分（第 5～10 章）的内容是说明如何使用概率理论精确解释诸如密码体制的安全性和函数的单向性这样的一些基本概念，并指出什么假设保证了公钥密码体制（比如 RSA）的安全性。这一部分涉及了一些更深入的课题，比如，单向函数的比特安全、计算上安全的伪随机发生器、密码体制的随机性和安全性之间的密切关系等问题。这一部分还给出了可证明安全的加密和签名体制的一些经典例子，同时，给出了它们的安全性证明。

虽然第 2 部分特别给出了数学构架和一些明确的定义，但是对一些必需的数学背景并没有介绍。对于数学和计算机科学专业刚起步的学生，学了基础的课程就足够他们理解本书。读者应该掌握代数的基本理论，比如，群、环、域的概念，还应该能理解附录中概率理论的基础知识。其中，附录 A 包含了理解密码方法必需的一些代数和数论结果。还有一些证明和推导，比如，基本的欧几里得算法和中国剩余定理；也包括了一些更深入的课题，比如，Legendre 符号和 Jacobi 符号以及概率素性检测等内容。附录 B 涵盖了

本书第2部分用到的所有概率和信息论方面的概念和结果。从数学难度的角度考虑，书中没有介绍椭圆曲线密码。本书通过介绍经典的密码体制，例如，整数集$\mathbb{Z}$的剩余类环$\mathbb{Z}_n$上的RSA体制，详细描述了公钥密码学的关键概念。

本书首先在第2章对经典的对称加密机制加以讨论。第3章详细讨论了公钥密码学的原理以及它们在加密和数字签名体制的应用。这一章对现在广为使用的著名的RSA、ElGamal和Rabin体制做了详细的介绍，分析了这几类加密和签名体制。这些体制的基本单向函数——模指数、模幂和模二次剩余函数——在本书的第2部分乃至整本书中都贯穿使用。第4章介绍了一些典型的密码协议，包括密码交换协议、身份认证协议、承诺系统、电子现金和电子选举系统。

后面几章的重点是对公钥密码学的关键概念和安全性给出了精确的定义。第5章用概率多项式算法模拟攻击。第6章研究了现代公钥密码学的安全性假设和它的基本模块单向函数。第7章特别详细分析了RSA函数、离散对数函数和Rabin函数。第8章解释了单向函数和符合密码学要求的计算安全的伪随机生成器间的紧密联系。第9章重点介绍了加密体制的可证明安全性。这些内容详细说明了随机性是安全的重点。我们从Shannon对信息理论工作所引出的可证明安全的经典想法出发，给出了很多最近对公钥加密机制的安全性分析结果的例子，同时，考虑了攻击算法的计算复杂度。本章还简单补充介绍了一个密码体制，这个体制的安全性可以用信息论方法证明，不需要任何问题的计算困难性假设(无条件安全方法)。最后，第10章讨论数字签名的安全等级，给出了一些签名体制，这些签名体制的安全性在标准假设(大整数分解)下即可证明，还给出了一个典型的安全性证明的全部过程。

除了第1章外，其他每一章最后都有习题，同时在本书的网页上提供了这些习题的答案，网址如下：http://cryptography.informatik.fh-nuernberg.de。

感谢校正此书的同事以及同学们，感谢他们提出的改进意见。特别感谢Jörg Schnwenk，Harald Stieber以及Rainer Weber。感谢Jimmy Upton提出的意见和建议，特别感谢Patricia Shiroma-Brockmann对本书的英文版本所做的校对审阅。最后，要感谢Spinger-Verlag的Alfred Hofmann，感谢他在此书编写和出版过程中的所给予的支持和帮助。

Hans Delfs，Helmut Knebl

Nürnberg 2001年12月

目录

第1部分　密码学的基本概念

第 2 部分 密码协议的分析方法和密码的安全性

第 1 部分

密码学的基本概念