ICSA Guide to Cryptography

信息安全技术丛书

ICSA密码学指南

(美) Randall K. Nichols 主编

吴世忠 郭涛 宋晓龙 等译

机械工业出版社
China Machine Press

信息安全技术丛书

ICSA密码学指南

（美） Randall K. Nichols 主编

吴世忠 郭涛 宋晓龙 等译

机械工业出版社
China Machine Press

本书详细介绍密码学在保护商业信息资源方面的应用，并详细描述了ICSA的信息安全产品认证过程。本书很好地将古典密码学历史和密码分析学结合到现代公钥密码产品领域，展现了密码分析学在先进计算机安全体系中的应用，探讨了生物学加密的前景，强调了密码安全产品在计算机系统中的正确实现。内容涉及过程、产品、协议、密钥管理、实现错误、产品认证等诸多方面。

本书面向信息技术的实践者，内容丰富，适合企业的CIO、网络管理人员、安全管理人员等专业人员阅读。

本书版权登记号：图字：01-2000-1723

图书在版编目（CIP）数据

ICSA密码学指南 /（美）尼科尔斯（Nichols, R. K.）主编；吴世忠等译. -北京：机械工业出版社，2004.5

（信息安全技术丛书）

书名原文：ICSA Guide To Cryptography

ISBN 7-111-14230-6

Ⅰ.I… Ⅱ.① 尼… ② 吴… Ⅲ.密码-理论 Ⅳ.TN918.1

中国版本图书馆CIP数据核字（2004）第037720号

机械工业出版社（北京市西城区百万庄大街22号 邮政编码 100037）

责任编辑：李 英

北京中加印刷有限公司印刷 · 新华书店北京发行所发行

2004年5月第1版第1次印刷

787mm × 1092mm 1/16 · 34.75印张

印数：0 001 - 4 000册

定价：55.00元

凡购本书，如有倒页、脱页、缺页，由本社发行部调换

本社购书热线：（010）68326294

译 者 序

近年来，我们已经在密码学领域翻译了大量的书籍，包括《应用密码学》、《密码编码和密码分析》、《密码学的理论和实践》、《密码学导引》（中译本均由机械工业出版社引进出版）等书。但在拿到本书的英文版后，我们有一种耳目一新的感觉。前面几本专著主要关注密码学本身，数学理论和密码算法比较多，普通读者阅读起来有一定难度。而本书风格迥异，作者以一个工程人员独特的视角，介绍了古典密码学的历史、公钥密码系统、各种密码算法、智能卡、IPSec、密码分析以及生物密码知识，内容由浅入深，叙述平实生动。因此，初看起来，本书的内容似乎有些零散，但是，当你细读下去，就会越来越觉得本书具有极大的实用价值。

本书是尼科尔斯先生关于密码学的第三本著作，在主编本书时，尼科尔斯先生在国际计算机安全联盟（ICSA，该公司已于2000年10月改名为TruSecure公司）担任密码学和生物方向的技术主管，对于整个信息安全领域的技术和产品具有全局把握，因此本书涵盖面非常广泛、几乎涉及信息安全领域所有的技术和产品。而且，作者在深入浅出地介绍深奥的密码学知识的同时，列举了大量现实生活中的例子，使得本书的行文活泼生动，一改传统密码学专著古板、深奥的风格，是一本不可多得的信息安全百科全书。因此，本书不仅适合于广大密码学、信息安全专业的学生阅读，也适合于网络安全从业人员参考。我们希望本书对于所有读者都有所裨益。

本书的翻译工作受到国家自然科学基金重大项目（90104033）的资助。

本书由吴世忠、郭涛、宋晓龙主持翻译，其他参与翻译工作的人员还有李寒梅、苏智睿、胡勇、李红阳、张展、李云雪、刘辉等，童俊、张晓东等同志在校稿和录入方面做了大量工作，在此一并表示感谢。

由于水平所限，翻译不妥或错误之处在所难免，敬请广大读者批评指正。

译 者

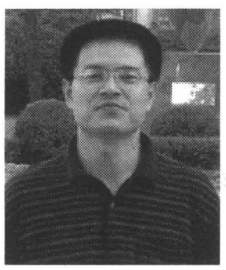
2004年2月

于中国信息安全产品测评认证中心

译者简介

吴世忠：博士、研究员，中国信息安全产品测评认证中心主任。现为全国信息安全标准化技术委员会副主任，中国信息产业商会信息安全产业分会理事长，《信息安全与通信保密》杂志主编。已公开出版文章百余篇，著有《信息系统的互连与互通》、《C3I系统的安全与保密》、《关贸总协定：中国准备好了吗？》、《首都信息化标准指南·信息安全与保密标准化体系》等专著五部和《应用密码学》、《密码编码和密码分析原理和方法》、《网络世界信息安全的真相》、《密码学的理论和实践》、《中文Windows2000的安全性》、《密码学导引》译著六部，同时还主持起草了防火墙、应用网关安全技术要求以及信息技术安全性评估准则等7项国家标准，并主笔撰写了与信息安全战略与技术发展有关的多篇专题报告。

郭涛：男，1974年9月出生，湖北宜昌人。2003年10月毕业于华中科技大学计算机学院，获得工学博士学位。中国信息安全产品测评认证中心高级研究人员，参加了多项国家重大科研项目。主要研究方向为信息安全技术、密码理论、安全测试技术、安全电子支付技术等；曾在《通信学报》、《高技术通讯》等刊物发表论文十几篇，译著有《密码学导引》。



宋晓龙：男，1970年9月出生。2000年5月毕业于中国人民解放军信息工程大学，获理学硕士学位；主要研究兴趣为密码算法与理论、密码分析和密码产品测试技术；曾在《通信学报》、《信息安全与通信保密》等刊物发表论文多篇，译著有《密码编码与密码分析原理和方法》和《密码学导引》。

作者简介

在编写本书的过程中，我们得到了许多同事的帮助，他们是不同领域中杰出的专家，为本书的出版做出了贡献。以下介绍本书的主要作者：

兰德尔·K. 尼科尔斯先生（Randall K. Nichols）

尼科尔斯先生是本书的主编，他是国际计算机安全联盟（International Computer Security Association，ICSA）密码学和生物统计学方面的技术主管，同时也是ICSA密码学和生物统计学产品联盟的资深密码技术主管。

本书是尼科尔斯先生关于密码学方面的第三本著作。尼科尔斯先生是密码分析学和古典密码学领域的专家，并已经编写了两本古典密码学教材，即古典密码学课程（《Classical Cryptography Course》）卷I和卷II，分别于1996年和1997年由Aegean Park出版社出版。尼科尔斯先生在密码学和计算机应用广泛的工程、建筑、咨询和化学工业领域担任过各种领导职位，在这方面拥有超过35年的管理经验。

尼科尔斯先生是COMSEC Solutions公司的总裁，COMSEC Solutions是一家在商业计算机安全领域中擅长密码对抗的咨询公司。尼科尔斯先生曾经担任美国密码学会（ACA）的主席和副主席，目前是ACA双月刊《密码学》（《The Cryptogram》）专家部的主编。尼科尔斯先生拥有Tulane大学的学士学位、德克萨斯A&M大学的硕士学位，以及休斯顿大学的MBA学位。

肖恩·阿博特先生（Shawn Abbott）

肖恩·阿博特先生是彩虹技术公司（Rainbow Technologies）的首席科学家，同时也是知识产权和因特网密码安全方面的专家。阿博特先生已经在五十多个会议上就关于如何使用硬件支持或攻击密码系统发表了演讲。阿博特先生不仅创立了作为CD-ROM加锁技术先驱的AND集团，还负责彩虹技术公司因特网安全集团产品的重要部分。阿博特先生还是国际软件公司（International Software）和Escrow公司的董事，以及Tragoes公司的顾问。

史蒂夫·彼得里先生（Steve Petri）

史蒂夫·彼得里先生是Litronic公司智能卡产品的项目总监。他带领一个由软件工程师组成的团队，并负责管理基于智能卡产品的跨平台产品线的技术开发工作，这些产品包括终端用户产品（NetSign、NetSign PRO）、软件开发者产品（CryptOS SDK、CryptOS SDK PRO、模板工具包），以及MIS管理产品（ProFile Manager）。彼得里先生是将先进的智能卡技术转化为真实产品方面的专家，而且他是工业界备受欢迎的演讲者。彼得里先生拥有普度大学的BSAAE学位和南加利福利亚大学的电子工程硕士（MSEE）学位。

玛丽·范·赞特女士（Mary van Zandt）

赞特女士是Sterling商业公司的市场总监，负责制定该公司安全产品的战略方向，这些安全产品对于安全保护电子商务的安全具有重要作用。该公司的产品可以用来解决各种安全问题，包括信息在传输或存储过程中的鉴别、访问、授权、完整性、机密性以及不可抵赖性。她在安

全、数据库、应用开发、专家系统以及数据仓库产品的市场方面拥有18年以上的经验，她曾经工作于Platinum Technology、Altai、Sybase、AICORP、Cap Gemini和惠普等公司。她于1982年获得Lake Forest大学的Lake Forest管理学院的MBA学位。

杰克·奥斯瓦尔德先生（Jack Oswald）

奥斯瓦尔德先生是RPK安全公司的总裁和CEO。他拥有12年以上的软件行业工作经验，其中包括10年的产品市场和产品管理。在1995年创建RPK公司之前，他领导一个小组制定了Borland公司全部的因特网战略，以及其早期采用Java技术的政策，并担任Borland公司的因特网产品部主任。他担任Borland公司的领先产品营销经理，负责管理Quattro Pro电子制表软件营销小组，还在多个高科技创业公司担任过市场总监。在他的职业生涯的早期，奥斯瓦尔德先生曾在一家小的家族式软件公司任职，该公司专注于数据库类产品。他拥有哈佛商学院MBA学位和Dartmouth学院的工程科学学位，擅长电子设计。

科林·苏塔先生（Colin Soutar）

科林·苏塔先生分别于1988年和1992年在苏格兰敦提市的敦提技术学院获得数学和物理学学士学位和物理学博士学位。1992年至1994年，他作为NRC研究助理在位于德克萨斯州休斯顿市的美国国家航空航天局（NASA）约翰逊空间中心工作，研究相关性在自动视觉系统中的应用。1994年，他开始在加拿大多伦多的Mytec技术公司工作，目前他是该公司的研发部总监。他已经参与编写了22部出版物，还拥有7项专利。

丹尼·罗贝格先生（Danny Roberge）

丹尼·罗贝格先生分别于1989年和1991年在加拿大蒙特利尔Ecole Polytechnique de Montreal学院获得物理工程方向的学士学位和硕士学位。1995年，他在加拿大魁北克省Laval大学的Centre d'Optique Photonique et激光实验室获得博士学位。1995年至1998年，他是Mytec技术公司的NSERC研究人员。他目前任职于加拿大蒙特利尔的Forensic技术公司。他的主要研究方向是图像处理与模式识别。

亚历克斯·斯托诺夫先生（Alex Stoianov）

斯托诺夫先生分别于1978年和1985年获得乌克兰基辅州立大学的无线电物理学和电子学的硕士学位以及物理学和数学博士学位。1978年至1993年，他在乌克兰的基辅州立大学的非线性光学系从事光折射及其相关现象的理论研究。从1994年起，他开始在Mytec技术公司从事光学处理、模式识别、指纹验证方面的研究。目前，他已经是该公司的高级研究人员。他发表了30多篇论文，并拥有多项专利。

勒内·吉尔罗伊女士（Rene Gilroy）

吉尔罗伊女士分别于1995年和1997年获得加拿大哈利法克斯市的Mount Saint Vincent大学的数学学士学位和加拿大滑铁卢大学的组合数学和优化学硕士学位。她的硕士论文的主题是DES和差分密码分析。她从1996年起在Mytec技术公司工作，从事生物加密算法的密码分析研究。她是多篇论文的合著者。

B. V. K. 维贾雅·库马尔先生（B. V. K. Vijaya Kumar）

库马尔先生分别于1975年和1977年获得印度坎普尔市的印度技术学院的电子工程学士学位和硕士学位，并于1980年在匹兹堡市获得卡耐基梅隆大学（CMU）的电子工程博士学位，然后

留在CMU电子和计算机工程系任教，目前，他是该系的教授。库马尔教授目前的研究方向是模式识别相关器的使用，并为数据存储系统开发高级信号处理方法。他已经编写或与人合著了五部书，拥有两项应用专利，在各种期刊和杂志上发表了二百多篇技术论文。库马尔教授是美国光学协会（Optical Society of American，OSA）和国际光学工程协会（International Society for Optical Engineering，SPIE）的会员。

香农·伯恩女士（Shannon Byrne）

香农·伯恩女士拥有商业学士、理学学士和理学硕士，是Paradata Systems公司的运营总监。她在面向对象编程和信息安全产品的软件开发方面拥有广阔的背景。她在1995年加入Paradata Systems公司之前，曾在Geovision、西门子、DMR Group以及Statistics Canada等公司工作。

戴维·什利克先生（David Slik）

戴维·什利克是Paradata Systems公司的顾问和前技术架构总监。他在最近四年中对电子商务系统进行了深入的研究。他已经开发了几个安全的软件商品分发系统，用于光盘和因特网数据的交付。

朱尔斯·普赖斯先生（Jules Price）

朱尔斯·普赖斯先生从1950年起就是ACA的密码高级研究人员，已经破译了1万多个密码。世界上只有少数人达到了这种水平，这意味着，他是75种不同的古典密码系统的专家。他还是一个专业工程师，作为副总裁、总工程师和项目经理，他曾经直接参与了许多数百万美元的大型项目，包括高速路、桥梁、大学、学校、医院和Shea体育场（纽约Mets队的主场）。他在构建规划和规范方面的丰富经验使得他对细节非常敏感。因为他的智慧，我们请他作为本书的主要编审。

哈特·W. 德格瑞菲特先生（Hart W. Degrafft）

德格瑞菲特先生有34年信息安全方面的经验，曾就职于美国国家安全局（National Security Agency，NSA）和美国国防信息系统局（Defense Information Systems Agency），曾是美国政府派驻NATO的代表，目前就职于SPARTA公司。他在政府部门和私营企业工作时，担任过多种技术、高级管理、任职和联络方面的职位。自从三年半前加入SPARTA公司，他担任过项目经理和首席工程师，开发用于电子数据交换、采购和旅游等商业领域的安全方案。他还在使用专家系统和Web技术的自动信息管理工具开发方面做过大量的工作。他拥有维吉尼亚技术大学的电子工程学士学位和马里兰大学的电子工程硕士学位。

米歇尔·E. 卡贝先生（Michel E. Kabay）

卡贝先生从十五岁就开始学习汇编语言。1976年，他已经在McGill大学学会了FORTRAN IV G语言，并获得了英国Dartmouth学院的应用统计学和无脊椎动物学专业的博士学位。在1979年以前，他是应用统计学领域的大学教授。他于1979年加入美国4GL和RDBMS编译小组，负责开发统计学语法，为命令语言中的统计函数编写解析算法、错误陷阱和代码。他于1980年加入惠普公司，成为性能方面的专家，并于1982年获得了系统工程师年度大奖。他是《Computer world》、《Network world》、《Computing Canada》、《Secure Computing Magazine》、《NCSA News》和一些贸易杂志的安全专栏的专栏作家。他于1997年获得CISSP（Certificated System Security Professional）专业资格。卡贝博士发表了170多篇关于运营管理和安全方面的论文，并由McGraw-Hill公司出版

了一部大学教材：《The NCSA Guide to Enterprise Security: Protecting Information Assets》。1991年，他加入美国国家计算机安全协会，义务担任教育主席和CompuServe NCSA论坛站长，并于1995年6月转为全职。他目前还是JINBU公司的总裁。

理查德·E. 史密斯先生（Richard E. Smith）

史密斯先生是《Internet Cryptography》一书的作者，该书由Addison Wesley出版，是美国销量最好的书籍之一。他是安全计算（Secure Computing）公司的首席信息安全架构师，他为美国的商业机构和包括NSA（美国国家安全局）在内的政府机构提供网络安全方面的咨询服务。他管理过很多有意义的项目，包括军方的网络防护系统和Sidewinder互联网防火墙。他是密码学和计算机安全领域的演说家、作家和培训大师。他拥有波士顿大学的电子工程学士学位和明尼苏达州立大学的硕士学位和博士学位。

蒂莫西·L. 特罗布里奇先生（Timothy L. Trowbridge）

特罗布里奇先生拥有普度大学的航空航天工程学士学位和科罗拉多州立大学的空间电子工程硕士学位。他在指挥、控制、通讯和智能系统（C3I）方面拥有18年的经验。他曾为两套指挥和操作系统开发过模拟和仿真软件，这些系统位于Cheyenne Mountain Complex，他还为美国空间指挥智能支撑系统进行系统工程研究。他是一位资深的研究人员，领导过卫星遥控遥测处理软件的开发，曾是两个研发项目（包括空间资产及其战术应用）的主要调查成员。他目前在位于美国科罗拉多州的Schriever空军基地的国家联合测试机构管理战争指挥和控制模拟软件的研发工作。

弗雷德里克·G. 汤普金斯先生（Frederick G. Tompkins）

汤普金斯先生是Unisys公司的信息安全顾问和项目副总监。他在人工智能、信息技术、工业安全和信息系统安全方面拥有超过30年的丰富经验。他是公认的信息安全策略和风险管理方面的权威。作为信息安全顾问，他的客户不仅包括商业机构，还包括州政府及联邦政府。作为Unisys公司的代表，他是美国总统的国家安全通讯顾问委员会网络组的成员。他最近为信息系统安全协会（Information Systems Security Association，ISSA）董事会服务，担任教育部长。他还是DataPro Reports公司信息安全领域的顾问。他是为战略中心和国际研究全球组织任务组服务的信息保障工作组的成员，美国工业安全协会的计算机安全委员会的主席。汤普金斯先生目前是网络可靠性和互操作性委员会的执行工作组的成员。此外，汤普金斯先生还是东密歇根大学的兼职教师，为研究生讲授信息安全风险管理课程。他拥有美国大学的技术管理学士学位和东密歇根大学的跨学科技术自由研究的硕士学位。

R. 凯文·亨特先生（R. Kevin Hunter）

亨特先生是Broken Rhythm Solutions LLC的总裁。他在管理和开发商业和军用软件以及通信系统应用方面拥有超过28年的经验。他拥有战略规划、项目规划、资源和项目管理、系统工程、安全工程、软件工程、计算机操作和质量保障等诸多领域的丰富经验。他帮助许多企业建立了软件开发、软件管理、安全系统开发和运行、网络管理控制方面的策略。他还拥有安全性合格评定、软件能力评估、管理审计方面的经验。他曾担任过安全指挥和控制系统、运营规划中心、信息管理系统和国际化系统等项目的总工程师。他拥有Regis大学的管理和计算机科学学士学位和菲尼克斯大学的MBA学位。

理查德·科满都先生（Richard Komando）

科满都先生是Krypto-Tech公司的总裁和CEO。他和Vinh C. Nguyen博士是Krypto-Tech公司的创建人，该公司为客户提供数据保密性方面的软件和硬件。除了有力地推动了多个计算机相关的创业公司的发展外，他还是美国使用强鉴别设备方面的首席系统工程师和国防自动化局的部门主管，也是一家财富五百强公司的自动化分析专家。他拥有Kings学院的学士学位和西佛罗里达大学的MBA学位。他在15年的时间里都积极参与计算机安全领域。

罗伊·佩雷拉先生（Roy Pereira）

佩雷拉先生是TimeStep公司的安全架构师。TimeStep公司是Newbridge的会员，专注于开发安全VPN解决方案，这些解决方案是网络安全领域的领先者。TimeStep的PERMIT企业级产品系列是符合IPSec的安全VPN方案，能够让用户把因特网当作私人网络使用。

在TimeStep公司，佩雷拉先生不但专注于安全和因特网的标准，也关注于产品发展方向、新技术、产品集成和产品管理。他在ANX和IETF很受尊敬，他是IETF的IPSec和IP压缩工作组的作者和很活跃的成员。在加入TimeStep公司之前，他已经创建了自己的软件开发公司，开发因特网服务器软件。他毕业于Carleton大学计算机科学系，已经在软件开发业拥有超过11年的经验，主要关注因特网协议、电讯协议、软件API和电子邮件系统等。

威廉·斯托林斯先生（William Stallings）

斯托林斯先生为帮助大家理解计算机网络和架构这个广阔领域的技术发展做出了特别的贡献，他在这些领域的不同方向编写了15个专题共32部专著。在该领域的过去二十年中，他曾经是技术投稿者、技术经理和几家高科技公司的总经理。目前，斯托林斯先生是独立顾问，他的客户包括计算机和网络的生产厂商和用户、软件开发公司以及领先的政府研究机构。

斯托林斯先生因为编写了许多优秀的计算机科学和工程教材，而多次获得教材和学术作者协会（Textbook and Academic Authors Association）颁发的Texty大奖：1998年，他因《操作系统：内在和设计原理》（《Operating Systems: Internals and Design Principles》，第三版，1998年由Prentice Hall出版）一书获得该奖；1997年，他因《数据和计算机通信》（《Data and Computer Communications》，第五版，1997年由Prentice Hall出版）一书获得该奖；1996年，他因《计算机组织和体系结构》（《Computer Organization and Architecture》，第四版，1996年由Prentice Hall出版）一书获得该奖。

他在从微型机到大型主机的各种不同计算机和操作系统上设计和实现了基于TCP/IP和OSI的协议套件。作为顾问，他曾为政府机构、计算机和软件商以及主要用户在网络软件和产品的设计、选择和使用上提供过建议。他还经常进行演讲，并撰写了大量的技术论文。他的新书《密码学和网络安全，原理和实践》（《Cryptography and Network Security，Principles and Practice》，第二版，1999年）已出版。斯托林斯先生拥有Notre Dame的电子工程学士学位和MIT的计算机科学博士学位。

序

从秘密的解密环到政府策略声明，把一些信息隐藏在其他信息中，或者从一些信息中发现所隐藏的信息，历来是对智力的一种挑战。密码学是一个非常迷人的领域，几乎每个孩子都玩过猜谜游戏，另一方面，密码学知识一直也是政府的最高级别秘密，用来保护政府最敏感的武器系统。古埃及法老坟墓上的墓志铭使用象形文字来象征尊严和权威，这种象形文字转换成密码，并逐渐演变成为装饰艺术或益智游戏。当密码学应用于军事和外交事务时，就是一件异常严肃的事情。毫不夸张地说，正是密码学的成败造就了许多战争的成败，从而改变了历史进程。也可以毫不夸张地说，现代历史正在由密码学的成败书写。

美国内战期间，麦克莱伦（McClellan）将军领导的联邦军队和罗伯特·E. 李（Robert E. Lee）将军领导的同盟军队在马里兰州华盛顿地区的夏普斯堡（Sharpsburg）附近进行了著名的安蒂他姆（Antietam）战役(1862年9月16至18日)。就在战役发生前几天，两名联邦士兵在他们的帐篷附近发现了一张纸，纸上的内容是李将军发布的进攻马里兰的详细计划的副本，该命令没有被加密。根据这张纸上的内容，麦克莱伦准确地得知李将军分散在各处的部队的位置，并抢在他们集结之前，越过南部山脉，从而重创了李的军队。

不可否认，李将军更加优秀，他比麦克莱伦更具想像力和魄力。在同等条件下战斗，李将军一定会取得胜利。如果他的那份被截获的命令得到了很好的加密处理，他肯定会尽快将他的军队集结在盖茨堡，并有充足的时间，利用有利地形，占据所有战略要地，重创曾经一度犹豫的麦克莱伦。如果南部军队取得了这场决定性战役的胜利，那么就有可能获得欧洲的外交承认，甚至取得北部各州选民的信任，进而影响林肯在1862年的选举，结束使用武力重建联邦的策略。如果真是这样，那么美国的历史就会被改写了。

密码学的成败塑造近代历史的另一个例子是1914年8月俄军在Tannenberg败给德军。俄军这次惨败的直接原因就是他们的通信被德军截获并利用。不可思议的是，俄军的通信全部是明文，因为俄军没有给战场指挥官配备密码和密钥。俄军因此不能在军队内部秘密协调相邻部队采取联合行动，更不要说让两支部队秘密地进行钳形进攻。在这场战役中，德军在俄军命令发送给俄军指挥官的时候进行窃听，而德军采用了安全的通信方式，这使得德军能够战胜两倍于自身的敌军——造成俄军几乎空前的崩溃。戴维·卡恩（David Kahn）在他的著作《密码破译者》(《The Codebreakers》)中写到："这是显而易见的，德军取得胜利的关键在于截获了俄军没有加密的通信"。战争的失败令人瞠目结舌，但是，就像安蒂他姆战役一样，更令人震惊的事情还远远不仅仅是战术上的胜负。回到这场战争，俄国的布尔什维克曾发起大规模的行动反对参与这场战争，这场战争使俄国蒙受了太大的财产损失和人员消耗。最终，就像多米诺骨牌一样，俄军在Tannenberg由于密码问题导致的失败最终结束了沙皇的统治，苏联出现在世界人民面前。

另一次重大的密码对抗是1942年与日本的中途岛战役。日本人想通过赢得中途岛战役，引诱和消灭珍珠港一役剩下的美军舰队，进而控制中太平洋，使夏威夷和美国西海岸成为日本人

的直接攻击目标。美国人将不得不集中力量保卫美国本土，而放任日本人向南长驱直入，孤立澳大利亚，进一步控制富饶的东南亚地区。

令美国人感到庆幸的是，日本人的通信不够安全，尽管他们书面强调了通信保密的重要性，实际操作和流程却是非常漫不经心。1942年，美国密码分析家破译了日军通信密码，进而知道了许多“联合舰队”的消息。结果，尼米兹（Nimitz）海军少将获知了日军准备采取偷袭方式进攻中途岛的计划，从而使日军的计划失败。盟军在中途岛的胜利阻止了日军的东进，使盟军在太平洋地区的战略地位从防守转为进攻，从而最终取得该地区战争的胜利，并赢得了整个战争。

世界现在又将注意力转移到了信息革命，以及恐怖主义、有组织的犯罪和毒品交易所带来的威胁。今天，我们所开发和使用的各种系统或多或少都采用了一些信息技术，完全脱离信息技术的系统是非常少见的。大坝的防洪闸门的远程遥控基于信息技术；高速公路的远程监控基于信息技术；汽车诸多性能的提高基于信息技术；工业流程的控制和管理基于高度复杂的信息技术。每一个基础设施，从空中交通管制、配电网到电话系统，无不基于信息技术或依赖于信息技术。一般来说，这些控制机制使用公共网之上的因特网协议。为提高效率，降低成本，现在都在强调异种系统间的互联互通，而信息技术使互联互通成为可能。一句话，信息技术无所不在。

遗憾的是，不断增加的互联互通也意味着不断增加的脆弱性。黑客、计算机罪犯、信息恐怖分子、甚至外国情报部门等各种不同形式的威胁也变得越来越复杂和广泛。另外，随之而来的挑战还包括在维护信息的保密性、完整性和可用性的同时，还需要为信息的内容、访问和基础设施提供保护，而所有这些保护都离不开密码技术。世界的互联为电子商务展现了广阔前景，将在世界范围内改变人们的生活方式，也将改变地理划分的不同团体之间的关系。推动电子商务发展的支撑技术还是密码技术，只有当在线达成的商务活动能够得到法律的认可，并且只有当公民能够确认在线交易不会损失他们的积蓄时，电子商务才能够被广泛接受。

电子商务的广阔前景依赖于现代计算机网络的速度和连通性，这些特性方便了商务交易，加快了现金的周转率，并使得我们更加富有。但是构成交易的数据交换必须是安全的，而这种安全的有效实现还是离不开密码技术。幸运的是，超过四千年的运用密码保护信息交易的经验为我们提供了随手可得的强有力的密码手段。公钥密码系统就提供了一个简单有效的方法，能够解决密钥管理过于复杂和昂贵的问题。为了能够最大限度地挖掘电子商务的潜力，我们需要广泛可用的高质量密码和支持密钥管理的基础设施。因此，问题的关键在于我们是否能够及时生产包含密码的软件和硬件产品。

对付恐怖分子、毒贩以及其他的犯罪分子的最有效的技术手段就是截获能够暴露他们的阴谋和计划的会话和消息。美国负责国家安全和法律事务的政府官员们有理由认为，广泛应用的加密将妨碍甚至消除他们截获犯罪消息的能力，并最终降低他们保护公共安全的能力。在长达一个世纪的时间里，他们已经习惯了相对容易地访问空间通信，他们提出强烈置疑，密码产品如果被别有用心的人不正当地使用，后果是非常危险的，密码产品的使用必须适当地与相应的立法相结合，允许负责国家安全事务的官员访问加密信息。更进一步讲，数字通信的复杂性和诸如带外信号等复杂交换技术的出现，已经大大增加了截获清晰话音传输的难度。面对技术的突飞猛进，政府采取的对策就是及时通过立法，使用合法手段获得对信息的访问。目前，已经

审查通过了相应法律，要求公共交换网络便于截获话音或数据通信，还要求密码技术的开发要与适当的暗门技术相结合，或者具备密钥托管或密钥恢复能力。

如果说这些措施还处在争议中，那绝对是一个保守的说法。针对密码技术立法，这绝对是个复杂的问题，因而早已成为技术专家们争论的核心。个人隐私的捍卫者丝毫不同情政府的立场和处境，强烈反对使用技术手段允许执法者和国家安全事务官员访问加密信息，甚至在法院的许可下。他们认为，这样的访问是一种权利滥用。同时，计算机行业的厂商们认为，如果用户知道美国生产的密码产品在安全性方面不如别人，那么，美国的计算机行业以及美国国家都将在国际市场丧失竞争力。他们认为政府要求访问机密信息以加强公共安全是一种误导。恐怖分子、毒贩和犯罪分子只要还有其他的安全产品可以选择（而它们确实无所不在），那么就绝对不会使用那些允许政府能够访问他们的通信的产品。现在是信息社会，无论是国家，还是企业和个人，都越来越依赖于信息技术。一方面，企业依赖计算机进行信息的产生、存储、处理和交换，并希望进入电子商务领域。另一方面，个人的工作、生活和娱乐也越来越依赖于信息技术，所以制定一个既能最好地服务于国家，又能够最大限度地满足企业和个人需求的密码策略就成为各方激烈争论的焦点。这一争论的结局将成为信息技术和密码技术的未来发展方针和路线，甚至有历史学家分析，未来历史将取决于这些决定。

兰德尔·K.尼科尔斯先生是本书的主编，他是美国密码学学会前任主席。在出版了两本关于古典密码学知识的专著后，尼科尔斯先生组织了密码学领域内的诸多杰出专家，共同合作编写了这本密码学领域的杰作，本书的内容几乎涵盖了密码学的所有方面，除了密码学的关键技术，还包括了密码学的数学渊源和社会影响。这本书深入浅出，既有广度，又有深度，各类读者都能从中获益。对密码学感兴趣的普通读者可以从中获得密码学知识的启蒙，了解密码学的技术和方法，看一看密码学如何帮助改变了历史的进程。信息安全领域的从业者或者准备进入信息安全领域的密码学爱好者更能从这本书中找到所需的专业知识。

Daniel J. Ryan
公司副总裁
Science Applications International Corporation
Julie J. C. H. Ryan
总裁
Julie Ryan, Inc.
http://www.julieryan.com

前　言

作为一门成熟的学科，密码学已经在商业领域取得广泛应用。企业在进行产品的全球推广，或者使用计算机网络实现全球通信和客户服务时，必须关注其资产和客户信息，防止受到各种各样的攻击。随着因特网发展成为主要的通信手段，这种关注也随之增多。保护存储在计算机中的信息或保护信息传输安全的最具性能价格比优势的方法就是采用密码技术。

密码学一度仅仅应用于政府和军队。现在，密码学已经广泛应用于科学、教育、生物测定、休闲、战略、战术等诸多领域和方向。尽管许多有远见的企业认识到密码学对保护其计算机信息资产安全的价值，但绝大多数的企业经理并未使用密码工具保护他们的计算机通信和数据库。随着经济全球化进程的加快，以及密码系统价格的降低，这种情况会逐步有所改变。

本书目标

本书的目的是为读者提供密码学在商业应用领域，尤其是在商业计算机安全系统方面的全貌。书中既有原理，也有实践，力图全面展现密码学作为保障计算机安全的战略和战术工具的益处，以及在商业舞台上的广泛应用。

本书深入探讨了正确采用密码措施所能够获得的商业价值，涵盖过程、产品、协议、密钥管理、实现错误、产品认证等诸多方面。

本书的目标读者不是技术专家，而是经理，并且特别针对销售商团队。本书详细阐述了密码学在保护商业信息资源方面的应用，并详细描述了ICSA的信息安全产品认证过程。本书很好地将古典密码学历史和密码分析学结合到现代公钥密码产品领域，展现了密码分析学在先进计算机安全系统中的应用，探讨了生物加密的前景，揭示了密码学在公共因特网上实现私人商务所面临的挑战，强调了密码安全产品在计算机系统中的正确实现。ICSA的信息安全产品认证是一个动态的过程，需要持续地评审相关的工业标准和当前的攻击方法，并将其应用于密码产品的测试中，以减少用户所面临的数字风险。最后，本书为读者提供了密码学应用于商业计算机系统方面的资源。

本书分为五个部分。第一部分展现现代密码系统的丰富历史基础，介绍代替密码和换位密码的历史渊源。密码学普遍性的原理在于任何一种语言（现存的和已经消失的）形式所表达的符号都能够被量化，并可用于开启密码学的宝藏。第二部分是对商业（公钥）计算机安全系统关键密码要求的阐述，包括单向函数、密码算法、因特网上的鉴别、密钥管理、硬件实现、数字签名以及CA认证机构。第三部分专门写给那些密码产品的销售商，讨论密码实现时所常犯的错误和ICSA的动态密码产品认证，还介绍ICSA在销售商认证和减少信息安全风险中的作用。第四部分阐述密码技术在保护计算机系统免受因特网攻击方面所起的重要作用。第四部分共有7章，是密码学实践的核心内容，是由这一领域里最优秀的几家企业组织编写的。这7章的内容各自独立，每一章都是一个独立的单元，包括了协议、智能卡、因特网密码、IPSec、电子商务以及基

于角色的密码系统。第五部分讨论密码分析、系统标识以及针对商业计算机系统所实施的攻击。这一部分还对生物识别技术结合密码技术的发展前景进行探讨。附录部分简单介绍椭圆曲线、复杂度理论和数论。

目标读者

本书是为信息技术的实践者编写的，企业的CIO、运营经理、网络经理、数据库经理、程序员、分析师以及EDI规划者之类的专业人士都可以从中找到有价值的内容。本书还可以作为计算机专业一年级的研究生教材、商业专业的计算机教材以及MBA教材。本书列出了大量的参考文献和URL，以便为那些需要深入了解某一内容的读者提供帮助。

本书的组织

本书内容以循序渐进的方式展开，其组织形式可以区分商用计算机系统密码保护的基本概念。对密码学的研究已经有几个世纪了，今天的成果是基于几百年的经验和教训取得的。在怀着极大的热情挖掘现代密码学的宝藏时，在试着理解现在的发展情况之前，有必要去了解密码学过去的历史和教训。本书各章组织如下:

第一部分：密码学发展史

该部分介绍古典密码学的基本原理，共有6章。

第1章：引言，本章介绍密码学历史上的主要成果和曾经影响了密码学发展的几个重要历史人物。

第2章：第一原则和概论，定义密码学在计算机系统方面的不同应用，例如，脆弱性、威胁、措施等；定义安全基础，例如，数据完整性、机密性、鉴别、不可抵赖性和标识；探讨密码学在保密和防泄漏等军事目标以外的成本效益和增值的商业目标；探讨因特网的飞速发展对保护隐私的影响。

第3章和第4章：历史上的密码系统I和II，定义普遍存在的基于语言学的密码原理；论述密码学的丰富历史；讨论简单的代替密码和换位密码系统；定义W. F. 弗雷德曼对密码系统的分析；介绍多码代替密码系统和同构（态）系统的知识；介绍基于外国语言的Xenocrypt密码以及现代语言和远古语言的分类；讨论Delastelle系统和分形原理。

第5章：代码和机器密码，介绍商业代码的起源；讨论战争期间机器密码的发展；探讨计算机是如何促进密码学发展的；介绍超级密码学知识。

第6章：数据加密标准（Data Encryption Standard，DES）和信息论，介绍古典密码学是如何转化到现代密码学的；深入介绍著名的DES算法、3DES和各种公钥密码术，并对实现进行讨论。

第二部分：商用密码系统

该部分介绍现代密码学的关键知识，共有6章。

第7章：公钥密码术（非对称密码），详细介绍对称密码和非对称密码术；讨论包括素数、大数、陷门函数、单向哈希函数在内的各种数学概念，以及它们在公钥系统中的重要性；详细介绍公钥密码系统的原理和背包问题。

第8章：算法，本章是核心的一章，覆盖了RSA算法、整数因式分解、离散对数，以及它们的椭圆曲线模拟等问题。

第9章：万维网中的标识、鉴别和授权，本章介绍因特网的标识和鉴别系统。

第10章：数字签名，本章介绍数字世界里的签名和鉴别，及其面临的挑战。

第11章：硬件实现，本章介绍实现密码功能的应用网关和专用芯片。

第12章：证书机构，本章介绍可信第三方（Trusted Third Party，TTP）和密钥恢复协议，讨论公钥证书、证书分发、证书撤销、认证实体分级等问题。

第三部分：实现和产品认证

在数字世界里的商务活动面临巨大的风险。第三部分介绍ICSA进行信息安全产品认证的目的，并介绍在产品测试中发现的实现错误。

第13章：实现错误，本章是重要的一章，覆盖与密码产品采购、安装、运行和连通性有关的多种实现错误；探讨实现密码对策时犯的错误；重点介绍红/黑分离、连接加密点对点局限、密钥和算法方面的问题。

第14章：ICSA产品认证，本章介绍ICSA密码产品联盟和ICSA密码产品认证的方法，阐述产品认证对产品安全性所起的作用。

第四部分：实用密码学

该部分的大多数材料是由ICSA密码产品联盟的资深管理代表提供的，共有6章，每一章都自成体系，代表了当今最先进的技术实现。

第15章：因特网密码学，本章涵盖用于保护因特网上的信息的所有重要协议。

第16章：安全：策略、隐私权和协议，本章探讨针对因特网的计算机安全问题，对攻击进行分类，并探讨密码产品所面临的法律问题。

第17章：智能卡，本章介绍智能卡技术，及其与密码学的关系。

第18章：IP安全和安全的VPN，本章介绍虚拟专用网（Virtual Private Network，VPN），以及相关的发展中的标准；具体介绍协议安全层、ISAKAMP、OAKLEY、密钥管理、鉴别、加密和路由配置。

第19章：电子商务系统中的密码学，本章介绍特定的用于满足电子商务安全目标的密码措施。

第20章：基于角色的密码学，本章介绍基于角色的密码学技术，这是一个与标准密码体系相对应的新选择。

第五部分：密码学的发展方向

该部分介绍密码学两个极具前景的发展方向：密码分析学和生物特征加密，共有两章。

第21章：密码分析和系统识别，本章讨论香农的信息概念、语言冗余、密码安全、操作因

素，以及针对对称加密的传统攻击；本章还讨论诸如蛮力攻击（使用蛮力搜索密钥）、拒绝服务攻击（DoS）、中间人等现代攻击；探讨使用特征向量区分密码系统和使用密钥串以解决攻击问题。

第22章：生物特征加密，本章介绍生物测定密码学，这是一个非常有意思的密码学发展方向，对加密和生物测定技术进行了很好的融合。

光盘[⊖]

本书所附带的光盘中包括了大量与密码产品（包括通过了ICSA认证的产品和未参加ICSA认证的产品）有关的论文和资料。

致谢

现代密码学所涵盖的内容已经远远超过了数学和密码分析学的范围，这也是我请求ICSA密码产品联盟及其所属成员的著名专家给予我包括高级技术资料在内的帮助的原因。帮助编写本书的密码学专家们都是密码学领域里最在行的、最受尊重的学者，读者可以从本书的各章内容中看到他们的专业智慧。另外，读者可以从本书开头的介绍中看到有关这些专家的专业和资格方面的介绍。

第8章的原始资料来源包括威廉·赖凯（William Raike，RPK国际公司的创始人）、杰克·奥斯瓦尔德（RPKUSA公司的CEO）和威廉·斯托林斯（他已经出版了22部安全方面的专著）所提供的资料。第9章的原始资料来源包括米歇尔·卡贝（ICSA的教育主管）所提供的资料。第10章包括理查德·科满都（KRYPTOTECH公司的CEO）提供的大量原始资料。第11章由肖恩·阿博特提供（RAINBOW TECHNOLOGIES公司的首席科学家），还包括从PKS'98收集来的资料。第12章是由哈特·德格瑞菲特（SPARTA公司的程序经理和总工程师）准备的。第13章是在弗雷德里克·汤普金斯（ICSA的前任策略分析主任，现在是UNISYS公司的信息安全顾问和副执行主任）的帮助下准备的。第15章由理查德·E. 史密斯（畅销书《Internet Cryptography》的作者，SECURE COMPUTING公司的首席信息安全架构师）提供。第16章是几个作者合作写成的，包括凯文·亨特（执行副总裁）、蒂莫西·特罗布里奇（BROKEN RHYTHM SOLUTIONS公司的总工程师，该公司的前身是DOXA ASSOCIATES）以及罗伊·佩雷拉（TIMESTEP公司的安全架构师）。第17章主要来自于史蒂夫·彼得里（LITRONICS公司的智能卡技术主任）。第18章是由TIMESTEP公司的罗伊·佩雷拉（安全领域的国际著名学者和IETF成员）提交的。第19章是由香农·伯恩（COO）以及PARADATA公司的戴维·什利克准备的。精彩的第20章由玛丽·范·赞特（STERLING COMMERCE公司的资深产品线经理）撰写。第22章采用了MYTEC技术公司的生物测定加密技术方面的材料，由科林·苏塔（首席科学家）、勒内·吉尔罗伊（资深密码学家）和卡内基梅隆大学的丹尼·罗贝格教授、亚历克斯·斯托诺夫、B. V. K. 维贾雅·库马尔撰写。我对于他们的能力、帮助和敬业精神非常感谢。在我们的集体努力下，本书是十分专业的。

⊖ 本翻译版图书不带光盘，原版图书所附光盘的内容可从以下网站下载：www.china-pub.com。——编辑注