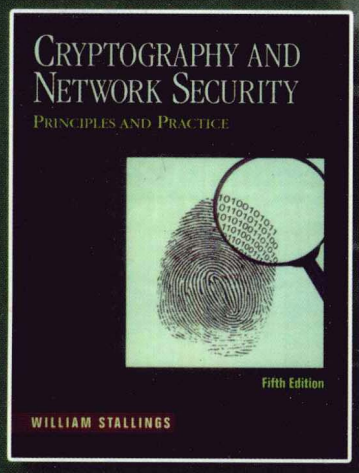
国外计算机科学教材系列

★William Stallings

PEARSON

密码编码学与网络安全
——原理与实践（第五版）

Cryptography and Network Security
Principles and Practice, Fifth Edition



[美] William Stallings 著

王张宜 杨 敏 杜瑞颖 等译
张焕国 审校

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

国外计算机科学教材系列

密码编码学与网络安全

——原理与实践(第五版)

Cryptography and Network Security

Principles and Practice, Fifth Edition

[美] William Stallings 著

王张宜 杨 敏 杜瑞颖 等译

张焕国 审校

電子工業出版社

Publishing House of Electronics Industry

北京 · BEIJING

内 容 简 介

本书系统介绍了密码编码学与网络安全的基本原理和应用技术。全书主要包括以下七个部分：对称密码部分讨论了对称加密的算法和设计原则；公钥密码部分讨论了公钥密码的算法和设计原则；密码学中的数据完整性算法部分讨论了密码学 Hash 函数、消息验证码和数字签名；相互信任部分讨论了密钥管理和认证技术；网络与因特网安全部分讨论了应用密码算法和安全协议为网络和 Internet 提供安全；法律与道德问题部分讨论了与计算机和网络安全相关的法律与道德问题。本书的第五版与第四版相比，书中的内容和组织结构都做了较大的调整，增加了许多新内容，并首次采用了在线内容和使用 Sage 计算机代数系统。

本书可作为研究生和高年级本科生的教材，也可以从事信息安全、计算机、通信、电子工程等领域的科技人员参考。

版权贸易合同登记号　图字：01-2011-6684

图书在版编目（CIP）数据

密码编码学与网络安全：原理与实践：第5版/（美）斯托林斯（Stallings，W.）著；王张宜等译.
北京：电子工业出版社，2012.1
国外计算机科学教材系列
书名原文：Cryptography and Network Security: Principles and Practice, Fifth Edition
ISBN 978-7-121-15250-4

I. ①密… II. ①斯… ②王… III. ①电子计算机-密码术-高等学校-教材 ②计算机网络-安全技术-高等学校-教材 IV. ①TP309.7 ②TP393.08

中国版本图书馆 CIP 数据核字（2011）第 241303 号

策划编辑：谭海平
责任编辑：李秦华
印　　刷：涿州市京南印刷厂
装　　订：涿州市桃园装订有限公司
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编　100036
开　　本：787×1092　1/16　印张：33.75　字数：1045 千字
印　　次：2012 年 1 月第 1 次印刷
定　　价：63.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

出 版 说 明

21世纪初的5至10年是我国国民经济和社会发展的重要时期，也是信息产业快速发展的关键时期。在我国加入WTO后的今天，培养一支适应国际化竞争的一流IT人才队伍是我国高等教育的重要任务之一。信息科学和技术方面人才的优劣与多寡，是我国面对国际竞争时成败的关键因素。

当前，正值我国高等教育特别是信息科学领域的教育调整、变革的重大时期，为使我国教育体制与国际化接轨，有条件的高等院校正在为某些信息学科和技术课程使用国外优秀教材和优秀原版教材，以使我国在计算机教学上尽快赶上国际先进水平。

电子工业出版社秉承多年来引进国外优秀图书的经验，翻译出版了“国外计算机科学教材系列”丛书，这套教材覆盖学科范围广、领域宽、层次多，既有本科专业课程教材，也有研究生课程教材，以适应不同院系、不同专业、不同层次的师生对教材的需求，广大师生可自由选择和自由组合使用。这些教材涉及的学科方向包括网络与通信、操作系统、计算机组织与结构、算法与数据结构、数据库与信息处理、编程语言、图形图像与多媒体、软件工程等。同时，我们也适当引进了一些优秀英文原版教材，本着翻译版本和英文原版并重的原则，对重点图书既提供英文原版又提供相应的翻译版本。

在图书选题上，我们大都选择国外著名出版公司出版的高校教材，如Pearson Education培生教育出版集团、麦格劳－希尔教育出版集团、麻省理工学院出版社、剑桥大学出版社等。撰写教材的许多作者都是蜚声世界的教授、学者，如道格拉斯·科默（Douglas E. Comer）、威廉·斯托林斯（William Stallings）、哈维·戴特尔（Harvey M. Deitel）、尤利斯·布莱克（Uyless Black）等。

为确保教材的选题质量和翻译质量，我们约请了清华大学、北京大学、北京航空航天大学、复旦大学、上海交通大学、南京大学、浙江大学、哈尔滨工业大学、华中科技大学、西安交通大学、国防科学技术大学、解放军理工大学等著名高校的教授和骨干教师参与了本系列教材的选题、翻译和审校工作。他们中既有讲授同类教材的骨干教师、博士，也有积累了几十年教学经验的老教授和博士生导师。

在该系列教材的选题、翻译和编辑加工过程中，为提高教材质量，我们做了大量细致的工作，包括对所选教材进行全面论证；选择编辑时力求达到专业对口；对排版、印制质量进行严格把关。对于英文教材中出现的错误，我们通过与作者联络和网上下载勘误表等方式，逐一进行了修订。

此外，我们还将与国外著名出版公司合作，提供一些教材的教学支持资料，希望能为授课老师提供帮助。今后，我们将继续加强与各高校教师的密切联系，为广大师生引进更多的国外优秀教材和参考书，为我国计算机科学教学体系与国际教学体系的接轨做出努力。

电子工业出版社

教材出版委员会

译 者 序

随着信息科学技术的高速发展和广泛应用，社会逐步信息化。在信息化社会中，通信、计算机和消费电子的结合，产生了 Internet、信息高速公路或全球信息基础设施(GII)，构成了人类生存的信息环境，即信息空间(Cyberspace)。在信息空间中，计算机和网络在军事、金融、工业、商业、人们的生活和工作等方面的应用越来越广泛，社会对计算机和网络的依赖越来越大，如果计算机和网络系统的信息安全受到破坏将导致社会的混乱并造成巨大损失。

我们应当清楚，人类社会中的安全可信与信息空间中的安全可信是休戚相关的。对于人类生存来说，只有同时解决了人类社会和信息空间的安全可信，才能保证人类社会的安全、和谐、繁荣和进步。

因此，确保信息空间、计算机和网络系统的信息安全成为世人关注的社会问题，并成为信息科学技术领域中的研究热点。

发展我国信息安全技术与产业的关键是人才，而培养人才的关键是教育。目前，我国许多大专院校都开设了信息安全专业或开设了信息安全课程，迫切需要一本合适的教科书。为此，电子工业出版社组织我们于 2006 年翻译出版了《密码编码学与网络安全——原理与实践(第四版)》这本优秀的教科书。这本书翻译出版后得到了广大读者的厚爱，许多著名大学都采用它作为教材，为我国信息安全人才培养和传播信息安全知识发挥了重要作用。

2010 年原书作者又出版了该书的第五版。在第五版中，作者对原书的内容和组织结构都做了较大的调整和更新。

1. 在书的组织结构方面做了如下调整：
   ① 在密码学方面增加了第三部分：密码学数据完整性算法。专门讨论密码算法中涉及数据完整性的内容，包括密码学 Hash 函数，消息认证码和数字签名。
   ② 增加了第四部分：相互信任。集中讨论了信息系统中的实体相互信任问题，包括密钥管理和用户认证。
   ③ 首次采用了在线内容，包括在线章和在线附录。将第六部分：系统安全、第七部分：法律与道德、附录 C 至附录 Q 放到网站上，读者可以上网阅读学习①。这样可以节约书的篇幅，降低书的成本。
   ④ 将伪随机数产生与序列密码集成为独立的一章。类似单独列章的还有传输层安全等。在以前的版本中，这些相关内容分散在各章中。这样将相关联的内容集成为一章，便于读者学习掌握。
2. 在内容方面进行了许多修改，并增加了一些新内容。如对于欧几里得算法、AES、分组密码工作模式、伪随机数、Hash 函数和消息认证码、密钥管理和分配、远程用户认证、IPsec 等内容进行了修改，并新增了 ElGamal 加密和数字签名、SHA-3、认证加密、联合身份认证、HTTPS、安全框架 SSH、域密钥身份认证邮件 DKIM、无线网络安全、法律与道德、在线附录、Sage 示例与问题等方面的新内容。

---

① 为使本书的中文版读者能读到原书的完整内容，特地翻译了原书的在线内容[第 20 章至第 23 章，以及附录 C 至附录 Q。这些内容的中文版已上载至华信教育资源网(http://www.hxedu.com.cn)，有兴趣的读者可免费下载]，从而为中文读者提供了一本完整的中文图书——编者注。

3. 作为对本书内容的补充，增加了 15 个附录。这些附录为感兴趣的读者提供了更深入、更广泛的补充材料。这是以前的版本中所没有的。

4. 首次使用开源免费的 Sage 计算机代数系统，使学生们能够亲手进行各种密码算法的实验。

为了使广大读者能够读到新版书，电子工业出版社又组织我们翻译出版了本书的第五版。

《密码编码学与网络安全——原理与实践》一书的作者 William Stallings 先后获得了 Notre Dame 电气工程学士学位和 MIT 计算机科学博士学位。他累计编写出版了 48 本计算机网络和计算机体系结构领域的书籍，在计算机网络和计算机体系结构的学术交流和教育方面做出了卓越的贡献。其中《密码编码学与网络安全——原理与实践》就是其中最成功的一本书籍。William Stallings 的著作不仅学术造诣很高，而且十分实用，先后 11 次获得美国教材和著作家协会（Textbook and Academic Authors Assiciation）颁发的优秀计算机科学教材奖。

本书系统地介绍了密码学与网络安全的基本原理和应用技术。全书主要包含以下七个部分。第一部分：对称密码，介绍了古典和现代对称密码算法，重点介绍数据加密标准（DES）和高级加密标准（AES）。此外，还讨论了伪随机数和流密码。第二部分：非对称密码，给出了数论基础、RSA 密码、椭圆曲线密码和其他公钥密码。第三部分：密码学中的数据完整性算法，介绍了密码学 Hash 函数、消息认证码和数字签名。第四部分：相互信任，介绍了密钥管理和密钥分配，以及用户认证协议。第五部分：网络与因特网安全，讨论了传输层安全、无线网络安全、E-mail 安全和 IP 安全等内容。第六部分：系统安全，讨论了非法入侵、恶意软件和防火墙技术。第七部分：法律与道德，讨论了与计算机和网络安全相关的法律和道德问题。

《密码编码学与网络安全——原理与实践（第五版）》一书内容丰富，讲述深入浅出，便于理解，尤其适合于课堂教学和自学，是一本难得的好书。本书可作为研究生和高年级本科生的教材，也可供从事信息安全、计算机、通信、电子工程等领域的科技人员参考。

本书的第一部分由杨敏和孟庆树翻译，第二部分由王后珍翻译，前言和第三部分由王张宜翻译，第四部分由陈晶翻译，第五部分由杜瑞颖翻译，第六部分和第七部分由彭国军翻译。

本书的附录 C、E、F、G、H、I 由杨敏翻译，附录 A、B、D、K、N、M 由王张宜翻译，附录 J 由王后珍翻译，附录 L 由陈晶翻译，附录 O、P、Q 由杜瑞颖翻译。全书由张焕国统稿和审校。研究生陈新姣、王丹、梁玉、郑美凤及叶青晟等参与了翻译书稿的整理工作。

由于译者的专业知识和外语水平有限，书中错误在所难免，敬请读者指正，译者在此先致感谢之意。

译者于武汉大学珞珈山

2011 年 8 月

符　号

符　号	表　达　式	意　义
D,K	D(K,Y)	用密钥 K 和对称算法解密密文 Y
D,PR_a	D(PR_a,Y)	用 A 的私钥 PR_a 和非对称算法解密密文 Y
D,PU_a	D(PU_a,Y)	用 A 的公钥 PU_a 和非对称算法解密密文 Y
E,K	E(K,X)	用密钥 K 和对称算法加密明文 X
E,PR_a	E(PR_a,X)	用 A 的私钥 PR_a 和非对称算法加密明文 X
E,PU_a	E(PU_a,X)	用 A 的公钥 PU_a 和非对称算法加密明文 X
K		密钥
PR_a		用户 A 的私钥
PU_a		用户 A 的公钥
MAC,K	MAC(K,X)	消息 X 的消息认证码,密钥为 K
GF(p)		阶为 p 的有限域,p 为素数。域定义为 Z_p 及其上的模 p 算术运算
GF(2^n)		阶为 2^n 的有限域
Z_n		小于 n 的非负整数集合
gcd	gcd(i,j)	最大公因子,整除 i 和 j 的最大正整数
mod	a mod m	a 除以 m 的余数
mod,≡	$a \equiv b \pmod m$	$a \bmod m = b \bmod m$
mod,≠	$a \neq b \pmod m$	$a \bmod m \neq b \bmod m$
dlog	$\mathrm{dlog}_{a,p}(b)$	以 a 为底 b 的对数,模 p 运算
ϕ	$\phi(n)$	欧拉函数,小于 n 且和 n 互素的正整数个数
Σ	$\sum_{i=1}^{n} a_i$	$a_1 + a_2 + \cdots + a_n$
Π	$\prod_{i=1}^{n} a_i$	$a_1 \times a_2 \times \cdots \times a_n$
|	$i \mid j$	i 整除得尽 j,即 i 除 j 的余数为零
|,|	$\lvert a \rvert$	a 的绝对值
‖	$x \Vert y$	级联 x 和 y
≈	$x \approx y$	x 约等于 y
⊕	$x \oplus y$	单位变量时是异或运算,多位变量时是按位异或
⌊,⌋	$\lfloor x \rfloor$	小于等于 x 的最大整数
∈	$x \in S$	元素 x 包含于集合 S
⟷	$A \longleftrightarrow (a_1, a_2, \cdots, a_k)$	整数 A 和整数序列(a_1,a_2,…,a_k)对应

前　言

在当前全球电子互联互通的时代，由于病毒、黑客、电子窃听和电子欺诈，使得安全性在任何时候都十分重要。第一，由于计算机系统的大量增加以及计算机系统通过网络互连，使得组织和个人越来越依赖于这些系统所存储和传输的信息。这也导致人们对如下的需求加深了认识：保护数据和资源不被泄露，保证数据和消息的真实性，保护系统不受基于网络的攻击。第二，密码和网络安全学科已经成熟，这样可开发出方便实用的应用软件来加强网络安全。由于这两种发展趋势，本书所讨论的内容就显得十分重要。

本书的目标

本书的目标是概述密码学与网络安全的原理和应用。本书的前两部分讨论密码学和网络安全技术，阐述网络安全的基本内容。其他部分讨论网络安全的实际应用，包括已经实现或正用于提供网络安全的实用应用软件。

因此本书涉及多个学科。特别地，要想理解本书讨论的某些技术的精髓，必须要有数论的基本知识和概率论中的某些结果。然而本书试图自成体系，不仅给出了必需的数论知识，而且让读者对这些知识有直观的理解。采用的方法是，在需要的时候才引入这些背景知识。这样有助于读者理解讨论这些知识的动机，作者认为这种方法比把所有的数学知识一次性全部放在本书开头要好。

本书适用对象

本书适合于学术和专业人员使用。作为教科书，本书可作为计算机科学、计算机工程、电气工程专业本科生密码编码学与网络安全方面课程的教材，学时为一学期。本书的内容包括了 IAS2 安全机制、NET4 安全和 IT311 里的材料（IAS2，NET4 是信息技术知识体系的两个核心领域，而 IT311 是密码学的高级教程）。这些材料都是 ACM/IEEE 计算机方向 2005 课程的讲授内容。

本书也可作为参考用书或作为自学教材。

本书的组织

本书由七个部分组成（概览全貌请见第 0 章）：

- 对称密码
- 公钥密码
- 数据完整性算法
- 相互信任
- 网络与因特网安全
- 系统安全
- 法律与道德

本书还针对教学的需要，提供了计算机代数系统 Sage 和大量图表使得表达更加清晰。每一章中都有关键术语表、课后习题、思考题、推荐读物和网站。本书还给出了术语表，常用的首字母缩略词表和参考文献。另外，对于教师还提供了试题库。

提供给学生的在线文档

对于本书的新版，我们提供了大量在线原始支持材料，包括如下类别：

- **在线章节**：为了减少本书（英文版）的篇幅和成本，书中的 4 个章节提供了 PDF 格式的电子文档，其中包括关于计算机安全的三章以及关于法律和道德的一章。在本书的目录中列出了这些章。
- **在线附录**：支持材料包含了本书正文中涉及的大量有趣的话题，但在本书（英文版）纸质印刷版中没有提供。我们为对此感兴趣的学生们提供了包含了这些话题的总计 15 个在线附录。在本书的目录中列出了这些附录。
- **家庭作业和答案**：为了帮助学生更好地学习和理解本书内容，我们提供了单独的一系列家庭作业和答案。这些能使学生们测试自己对于教材的掌握程度。
- **关键论文**：我们从专业文献中选择了 24 篇论文，其中许多是很难找到的。提供给读者进一步地阅读。
- **支持文档**：本书引用的其他各种类型的有用文档同时在线提供。
- **Sage 代码**：附录 B 中给出了示例的 Sage 源代码。如果学生们想要实现这些示例，可以以此作为参考。

购买本书（英文版）可提供读者 6 个月的在线材料访问权限。详见本书（英文版）扉页中的访问卡。

教学支持文档

对于教师，我们提供了下列材料：

- **答案手册**：对于每章末尾的思考题和习题的答案。
- **项目手册**：对于下面列出的所有项目的建议的任务分配方案。
- **PPT 幻灯片**：包含所有章节内容的幻灯片，适于讲课中使用。
- **PDF 文件**：本书中所有图和表的副本文档。
- **习题集**：按章的习题集。

在教师资源中心（IRC）中提供了所有的这些支持文档，可以通过 personhighered. com/stallings 或点击本书网站 WilliamStallings. com/Crypto/Crypto5e. html 中的“Book Info and More Instructor Resources”按钮访问 IRC。要想获取访问 IRC 的权限，请通过 pearsonhighered. com/educator/replocator/requestSalesRep. page 或者 Prentice Hall 的客服电话 1-800-526-0485 联系当地的 Prentice Hall 的经销商[①]。

教师和学生的 Internet 服务

本书的网站可给学生和教师提供支持，该网站链接一些相关的站点，并以 PDF（Adobe Acro-

① 为获取本书的教学支持文档，可参阅书后所附的《教辅申请表》——编者注。

bat)格式存储的本书中出现的图片、表格、幻灯片。该网站地址是 WilliamStallings. corn/ Crypto/ Crypto5e. html。更多的信息请参阅本书第 0 章。

本书第五版在网上新提供了一系列的家庭作业和答案。学生们能够对这些题目进行求解并检查答案是否正确,这些题目能够加深学生们对于所学内容的理解。

我们已经建立了一个邮件列表,方便使用本书的各位教师以及与本书作者之间互相交换信息、建议和问题。若发现印刷或其他错误,则在 WilliamStallings. com 可找到本书的勘误表。另外计算机科学专业学生资源网(WilliamStallings. com/StudentSupport. html)为计算机专业学生和专业人员提供了有关的文档、信息和链接。

项目和其他学生练习

对许多教师来说,密码学或信息安全课程的一个重要组成部分就是制定一个或一系列项目使得学生有机会亲手实践,以加深对本书中所学知识的理解。本书在很大程度上对该课程的讲授计划提供支持,包含了课程中一整套的项目组件。教师资源中心不仅包含如何布置和安排项目,而且还包括一系列涵盖本书内容的推荐教学项目:

- **Sage 项目**:下一节中详细介绍。
- **黑客项目**:本项目的目的是阐明入侵检测和预防的关键问题。
- **分组密码项目**:本实验对 AES 加密算法的操作过程进行跟踪,手工进行一轮的计算,并使用不同的分组密码工作模式进行计算。实验也包括 DES 算法。每种情况下都由在线(或离线下载)Java 小程序来实现 AES 或 DES 的运算。
- **实验室练习**:就本书中的概念进行编程和做实验的系列项目。
- **研究项目**:一系列指导学生研究 Internet 有关课题以及撰写研究报告的课外研究课题。
- **编程项目**:一系列涵盖大部分课程内容且可在任何平台上用任何适当的语言实现的程序设计项目。
- **安全评估实践**:用于检验已有组织机构的现有架构和实现的一系列活动。
- **书面作业**:每一章里推荐了一些书面作业。
- **课外阅读/报告作业**:每一章在参考文献中都包含有论文列表,可让学生阅读并写出简短报告。具体细节请参见附录 A。

Sage 计算机代数系统

本书第五版新增的一项最重要的内容就是使用 Sage 实现密码算法示例和作业。Sage 是开源、跨平台支持的免费软件,能够在数学和计算机代数系统的学习过程中提供强大、灵活和易学的软件包。与 Mathematica, Maple 和 MATLAB 等系统不同,Sage 没有专利保护和使用费的限制。因此,Sage 可以在学校的计算机和网络上使用,学生也可以分别将其下载到他们自己的个人计算机上在家里使用。使用 Sage 的另外一个好处是学生可以掌握一个非常强大、灵活的工具来帮助计算几乎所有的数学问题,而不仅限于密码学。

在对密码算法数学基础的教学过程中,使用 Sage 能够显著增强教学效果。本书的附录 B 中提供了涵盖各种密码学概念的大量 Sage 示例。

附录 C 按照密码学概念的分类给出了习题集,使学生能够通过练习手把手地理解密码算法。

本书的教师资源中心 IRC 为教师提供了该附录。附录 C 中专门有一节介绍如何下载和使用 Sage，另一节介绍 Sage 编程基础，除此以外还包括为学生准备的以下分类习题：

- **第 2 章——古典密码**：仿射密码和 Hill 密码。
- **第 3 章——分组密码和数据加密标准 DES**：基于 SDES 的练习。
- **第 4 章——数论和有限域基本概念**：欧几里得算法和扩展欧几里得算法，多项式算法，有限域 $GF(2^n)$。
- **第 5 章——高级加密标准 AES**：基于 Sage 的练习。
- **第 6 章——伪随机数发生器和流密码**：BBS，线性同余和 ANSI X9.17 伪随机数发生器。
- **第 8 章——数论**：欧拉函数，Miller-Rabin 测试，因子分解，模幂运算，离散对数，以及中国剩余定理。
- **第 9 章——公钥密码和 RSA**：RSA 加密/解密以及签名。
- **第 10 章——其他公钥密码算法**：Diffie-Hellman 密钥交换，椭圆曲线密码。
- **第 11 章——密码学 Hash 函数**：基于数论的 Hash 函数。
- **第 13 章——数字签名**：DSA。

第五版新增内容

与本书的前几次再版相比，《密码编码学与网络安全——原理与实践》的本次新版的修改更加广泛和充实。

本书第四版出版后的三年中，该领域仍处于不断地变革之中。该新版中，我试图在继续广泛涵盖本领域内容的同时，增加这些新的变化。进行本次修订之初，本书第四版由许多讲授该领域课程的教授仔细审阅过。而且，许多研究该领域的专业人员也审阅过某些章节。这使得许多地方的叙述变得清晰、紧凑，对插图也进行了改进，而且增加了许多新的“现场测试”习题。

本书的主要修改之一是，对整体结构重新进行了组织，这使得相关问题的描述更加清晰。新增了第三部分，其中涵盖了密码算法中所有涉及数据完整性的内容，包括密码学 Hash 函数，消息认证码，以及数字签名。关于密钥管理和密钥交换的内容，在本书早期版本中散布在各章中，新版中组成了独立的一章。对于用户认证的内容也有类似调整。

除了这些为改进教学法和方便用户所做的修改以外，还有一些实质性的变化贯穿本书，最主要包括下列几个方面：

- **欧几里得算法和扩展的欧几里得算法（修订）**：这些算法对于许多密码函数和算法都非常重要。我们对于整数和多项式的欧几里得算法和扩展的欧几里得算法的内容进行了彻底地重新编写，给出了更清晰和系统的描述。
- **高级加密标准 AES（修订）**：AES 目前已经成为最通用的对称加密算法，在各种应用中被广泛使用。相应地，本版大幅扩展了学习和理解 AES 标准的资源。关于 AES 算法的章节被重新修订并扩充，为了清晰描述该算法而添加了更多的图和细节示例。同时还添加了使用 Sage 的示例和习题。本书目前包括了 AES 密码实验库，能够给学生提供手把手的实验环境，来学习 AES 密码的内容结构和工作模式。本书的网站中提供了该库使用的 AES 计算小程序，能够使用 AES 分组密码对测试数据进行加密或解密。
- **分组密码工作模式（修订）**：我们对第 6 章中关于工作模式的内容进行了扩充，并重新绘制了更清晰的图示。

- **伪随机数发生器和伪随机函数(修订)**:我们对该重要主题的处理方法的介绍进行了扩充,增加了使用对称加密算法和密码学 Hash 函数来构造伪随机函数的新内容。
- **ElGamal 加密和数字签名(新增)**:新增加了一节对于该流行的公钥算法进行介绍。
- **密码学 Hash 函数和消息认证码(修订)**:关于 Hash 函数和 MAC 的内容被重新修订和重新组织,使得描述更清晰和系统。
- **SHA-3(新增)**:尽管 SHA-3 算法目前还在征集选择过程中,对于学生们掌握该即将问世的密码标准的设计准则是非常重要的。
- **认证加密(新增)**:本书增加了重要的新算法 CCM 和 GCM,这两个算法能够同时提供机密性和数据完整性保护。
- **密钥管理和分配(修订)**:在第四版中该部分内容被穿插在三个章节中介绍,第五版中该部分内容被重新修改合并为独立的一章,使得描述统一和系统。
- **远程用户认证(修订)**:在第四版中该部分内容被分为两章介绍,第五版中该部分内容被重新修改合并为独立的一章,使得描述统一和系统。
- **联合身份识别(新增)**:新增一节介绍这种通用的身份管理方案,该方案在许多企业和无数应用中使用,服务于成百上千甚至于百万的用户。
- **HTTPS(新增)**:新增一节介绍 HTTPS 协议,该协议为 Web 浏览器和 Web 服务器之间的安全通信提供保护。
- **安全内核(新增)**:新增一节介绍 SSH,SSH 是加密技术最广泛的应用之一。
- **域密钥身份识别邮件 DKIM(新增)**:新增一节介绍 DKIM,DKIM 是应对垃圾邮件的邮件认证的标准。
- **无线网络安全(新增)**:新增一章专门讨论该网络安全中的重要领域。本章介绍无线局域网中使用的 IEEE 802.11(WiFi)安全标准;移动 Web 浏览器与 Web 服务器之间通信的安全标准无线应用协议(WAP)。
- **IPsec(修订)**:我们对介绍 IPsec 的一章几乎完全重新进行了编写。新版包括了 IPsecv3 和 IKEv2。此外,我们对表述也进行了修改使得更加清晰,并增加了内容的广度。
- **法律与道德(新增)**:新增了在线章节讨论该重要话题。
- **在线附录(新增)**:本书的网站上有 15 个附录,为感兴趣的同学们提供更深更广的各种材料。
- **Sage 示例和问题(新增)**:如上所述,本次新版使用开源、免费的 Sage 计算机代数系统,使学生能够亲手进行各种密码算法的实验。

对于每次新版的修订,在对全书保持合理的页数和增加新的内容之间进行取舍是非常困难的。在前几版中对篇幅的控制是通过将过时的内容删除以及尽量精简描述来实现的。对于本版,一些次重要的章节和附录转移到了独立的在线 PDF 文档中。这使得我们能够尽可能地扩充本书的内容而不增加本书的页数和价格。

致谢

本次修改得益于许多人的审阅,他们花费了大量的时间和精力。下列这些人员审阅了所有或大部分手稿:Marius Zimand(Towson State University),Shambhu Upadhyaya(University of Buffalo),Nan Zhang(George Washington University),Dongwan Shin(New Mexico Tech),Michael Kain(Drexel

University), William Bard(University of Texas), David Arnold(Baylor University), Edward Allen(Wake Forest University), Michael Goodrich(UC-Irvine), Xunhua Wang(James Madison University), Xianyang Li(Illinois Institute of Technology),以及 Paul Jenkins(Brigham Young University)。

我还要感谢那些详细审阅其中某一章或数章的人员:Martin Bealby, Martin Hlavac(Department of Algebra, Charles University in Prague, Czech Republic), Martin Rublik(BSP Consulting and University of Economics in Bratislava), Rafael Lara(President of Venezuela's Association for Information Security and Cryptography Research), Amitabh Saxena,以及 Michael Spratte(Hewlett-Packard Company)。我还要特别感谢 Nikhil Bhargava(IIT Delhi)对本书许多章节的细致审阅。

Joan Daemen 审阅了关于 AES 的章节。Vincent Rijmen 审阅了有关 Whirlpool 的内容。而 Edward F. Schaefer 审阅了有关简化 AES 的内容。

Nikhil Bhargava(IIT Delhi)开发了一系列的在线家庭作业和解答。Microsoft 和 University of Washington 的 Dan Shumow 开发了附录 B 和附录 C 中所有的 Sage 示例和作业。Dakota State University 的 Sreekanth Malladi 教授开发了黑客练习。Australian Defence Force Academy 的 Lawrie Brown 提供了 AES/DES 分组密码项目和安全评估练习。

Purdue University 的 Sanja Rao 和 Ruben Torres 为教师资源中心 IRC 里的实验室练习做了很多工作。下列人员为教师资源中心中的课程计划方面做了工作:Henning Schulzrinne(Columbia University), Cetin Kaya Koc(Oregon State University)和 David Balenson(Trusted Information Systems and George Washington University)。Kim McLaughlin 提供了习题库。

最后,我要感谢负责本书出版的工作人员,他们都做得很优秀。包括编辑 Tracy Dunkelberger,以及她的助理 Melinda Hagerty,产品经理 Rose Kernan。还要感谢 Warde 出版社的 Jake Warde 组织了整个审稿。

在这么多帮助面前,我几乎没有什么可以居功自傲的。但我可以自豪地说,没有这些帮助,我也会选择所有这些内容。

作者介绍

William Stallings 在计算机安全、计算机网络和计算机体系结构等技术的发展方面成就卓著。他编写出版了 17 部著作,经修订再版累计共 42 本上述相关领域的书籍。他的著作无数次出现在 ACM 和 IEEE 出版物中,包括 Proceedings of the IEEE 和 ACM Computing Reviews。

他 11 次获得美国"教材和著作家协会"(Text and Academic Authors Association)颁发的"年度最佳计算机科学教材"奖。

在过去的 30 年中,他曾在该领域的数个高科技企业中担任技术骨干、技术管理者和技术执行领导。他设计和实现了适用于从微型机到大型机的各种类型的计算机和操作系统的基于 TCP/IP 和基于 OSI 的协议。目前,他作为独立顾问为政府机构、计算机硬件制造商、软件开发商以及广大用户提供包括设计、选择和使用网络软件和产品的咨询服务。

他建设并维护计算机科学专业学生资源网 WilliamStallings.com/StudentSupport.html。该网站提供为计算机科学专业的学生(和专业人员)提供各种文档和链接。他是 *Cryptologia* 杂志的编委,该杂志是密码学的学术期刊。

William Stallings 博士先后获得了 Notre Dame 电气工程学士学位和 MIT 计算机科学博士学位。

目　录

第一部分　对 称 密 码

第二部分 公 钥 密 码

第三部分 密码学数据完整性算法