国外计算机科学教材系列

Pearson

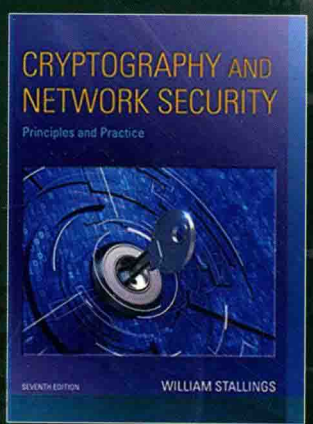
★William Stallings

密码编码学与网络安全

——原理与实践（第七版）

Cryptography and Network Security

Principles and Practice, Seventh Edition



[美] William Stallings 著

王后珍 李 莉 杜瑞颖 等译

张焕国 审校

中国工信出版集团

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(第七版)

Cryptography and Network Security

Principles and Practice, Seventh Edition

[美] William Stallings 著

王后珍 李 莉 杜瑞颖 等译

张焕国 审校

電子工業出版社

Publishing House of Electronics Industry

内 容 简 介

本书系统地介绍了密码编码学与网络安全的基本原理和应用技术。纸质教材分为六部分：背景知识部分介绍计算机与网络安全的概念、数论；对称密码部分讨论古典加密技术、分组加密和数据加密标准、有限域、高级加密标准、分组加密操作、随机位生成和流密码；非对称密码部分讨论公钥加密和 RSA、其他公钥加密体制；密码编码数据完整性算法部分讨论哈希函数、消息认证编码、数字签名；互信部分讨论密钥管理与分发、用户鉴别；网络和互联网安全部分讨论网络访问控制和云安全、传输层安全、无线网络安全、电子邮件安全和 IP 安全。在线内容分为两部分：系统安全部分讨论恶意软件、入侵者、防火墙；法律和道德问题部分讨论与计算机和网络安全相关的法律与道德问题。与第六版相比，书的章节组织基本不变，但增加了许多新内容，如数论、格式保留加密、真随机数生成器、云安全、传输层安全、移动设备安全等。

本书可作为高校计算机、网络安全、信息安全、软件工程等专业研究生和高年级本科生的教材，也可供从事网络空间安全、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：01-2016-9453

图书在版编目（CIP）数据

密码编码学与网络安全：原理与实践：第七版 /（美）威廉·斯托林斯（William Stallings）著；王后珍等译.
北京：电子工业出版社，2017.12
（国外计算机科学教材系列）
书名原文：Cryptography and Network Security: Principles and Practice, Seventh Edition
ISBN 978-7-121-32921-0

I. ①密… II. ①威… 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. ①TP309.7②TP393.08

中国版本图书馆 CIP 数据核字（2017）第 257831 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：涿州市京南印刷厂
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：864 千字
版　　次：2003 年 11 月第 1 版（原著第 3 版）
　　2017 年 12 月第 5 版（原著第 7 版）
印　　次：2017 年 12 月第 1 次印刷
定　　价：95.00 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）88254888，88258888。
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。
本书咨询联系方式：（010）88254552，tan02@phei.com.cn。

译 者 序

随着信息科学技术的高速发展和广泛应用，社会实现了信息化，人类社会进入信息时代。人们生活和工作在由物理世界、人类社会和网络空间组成的三元世界中。网络空间是信息时代人们赖以生存的信息环境，是所有信息系统的集合。

哪里有信息，哪里就存在信息安全问题，信息安全是信息的影子。信息论的基本观点告诉我们：系统是载体，信息是内涵。网络空间是人类和信息的生存环境，因此网络空间安全是人类和信息对网络空间的基本要求。网络空间是所有信息系统的集合，是复杂的巨系统。因此，网络空间存在更加突出的信息安全问题。网络空间安全的核心内涵仍是信息安全，没有信息安全就没有网络空间安全。

当前，一方面是信息技术与产业的空前繁荣，另一方面是危害信息安全的事件不断发生。敌对势力的破坏、黑客攻击、利用计算机犯罪、网上有害内容泛滥、隐私泄露等，对信息安全构成了极大威胁。信息安全的形势是十分严峻的。因此，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。

我国已经成为信息产业大国，但仍不是信息产业强国。实现信息化和确保信息安全是建设中国特色社会主义强国的两个重要方面。两者相辅相成，缺一不可。没有信息化，就没有国家现代化；没有信息安全，就没有国家安全。显然，只有同时实现信息化并确保信息安全，才能把我国建成中国特色社会主义强国。

把我国建设成信息技术和产业强国，人才是关键。人才培养，教育是关键。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 2015 年翻译出版了《密码编码学与网络安全——原理与实践（第六版）》这本优秀的教科书。这本书翻译出版后得到广大读者的厚爱，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信息安全知识传播发挥了重要作用。

2017 年原书作者又出版了该书的第七版。与第六版相比，第七版大体上保持了相同的章节，但修正了许多内容并增加了一些新的内容。最主要的变化包括以下几个方面：

① 安全设计基本原则：第 1 章新增了一个小节，讨论美国国家信息保障/网络空间防御专业认证计划（由美国国家安全局和国土安全部联合举办）所列出的一些安全设计原则。

② 攻击面和攻击树：第 1 章新增了这两个概念，有助于安全威胁的评估和归类。

③ 数论知识：将第六版中所提到的数论知识统一写成一个独立的第 2 章。

④ 有限域：对有限域章节进行了修改和扩展。

⑤ 保留格式加密：第 7 章新增了一节来讨论这种新的加密模式。

⑥ 真随机数生成器的校正和性能测试：现在第 8 章包含了这些重要的研究方向。

⑦ 用户认证模型：第 15 章给出了一般用户认证模型的新描述方法。

⑧ 云安全：第 16 章有关云安全的内容做了更新和扩展。

⑨ 传输层安全（TLS）：第 17 章的传输层安全相关内容进行了更新，并且增加了新 TLS 版本 1.3 的讨论。

⑩ 邮件安全：完全重写了第 19 章。

其中，新增了以下内容：

- 对邮件的威胁及一种全面保证邮件安全的方法。
- 保障 SMTP 机密性的新方法 STARTTLS。
- DNSSEC 在保证邮件安全中所起的作用。
- 基于 DNS 的命名实体认证（DANE）以及使用这种方法加强 SMTP 和 S/MIME 中证书的安全性。
- 发送方策略框架（SPF）。SPF 是一种用于认证电子邮件发件人的标准方法。
- 允许发件人自己定义邮件的处理办法 DMARC。

其中，修改了以下内容：

- 有关域名密钥识别邮件（DKIM）标准的讨论。
- 将 S/MIME 更新至最新的 3.2 版本。

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第七版。

本书的作者 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。本书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 13 次获得美国“教材和著作家协会”（Textbook and Academic Authors Assiciation）颁发的年度最佳计算机科学教材奖。

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。全书主要包含以下八个部分。第一部分：概览。主要介绍计算机与网络安全概念和数论知识。第二部分：对称密码。主要介绍古典密码、数据加密标准（DES）、有限域知识、高级加密标准（AES）、分组密码工作模式、伪随机数和流密码。第三部分：公钥密码。介绍了公钥密码原理、RSA 密码、ElGamal 密码和椭圆曲线密码。第四部分：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。第五部分：互信，介绍了密钥管理和用户认证。第六部分：网络与 Internet 安全。讨论了网络访问控制和云安全、传输层安全、无线网络安全、电子邮件安全和 IP 安全等内容。第七部分：系统安全。讨论了恶意软件、非法入侵、防火墙技术。第八部分：法律和道德，讨论了与计算机和网络安全相关的法律和道德问题。

为了使中文版读者能够读到原书的完整内容，我们特别翻译了原书的在线内容（第七部分：系统安全、第八部分：法律和道德、附录 C-Y）。从而给中文读者提供一本完整的中文《密码编码学与网络安全——原理与实践（第七版）》[①]。

本书内容丰富，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。

本书的第一部分和附录由李莉翻译。第二部分由唐明翻译。第三部分和前言由王后珍翻

① 有关本书在线部分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注册下载——编者注。

译。第四部分由王张宜翻译。第五部分由陈晶翻译。第六部分由杜瑞颖翻译。第七部分和第八部分由彭国军翻译。

全书由张焕国统稿和校审。

研究生刘金会、刘鳌、汪鹏程、陈施旅、罗华、郭崎、文皓冬、熊璐、胡岸琪、于慧、陈震杭参与了翻译和译稿整理工作。

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

2017 年 6 月

前　言

第七版的新内容

在本书第六版出版后的 4 年中，该领域仍处于不断地发展变革之中。在新版中，我试图在继续广泛涵盖本领域的主要内容的同时，增加这些新的变化。进行本次修订之初，许多讲授该课程的教授和研究该领域的专业人员都已经阅读过本书的第六版。这使得许多地方的叙述变得更清晰、更紧凑，对插图也进行了改进。

除了这些为改进教学法和使用户易读所做的修改以外，还有一些实质性的变化贯穿在本书中。与第六版相比，本书大体上保持了相同的章节，但修正了许多内容并增加了一些新内容。最主要的变化包括以下几个方面：

- **基本的安全设计原则**　第 1 章包含了一个新的小节讨论美国国家信息保障/网络空间防御专业认证计划（由美国国家安全局和国土安全局联合举办）所列出的一些安全设计原则。
- **攻击面和攻击树**　第 1 章包含了一个新的小节描述这两个概念，有助于安全威胁的评估和归类。
- **数论相关知识介绍**　为了便于读者参考，把第六版中所提到的数论知识点统一到了一个独立章节，即第 2 章。第 2 章的相关部分是根据本书密码算法学习需要来安排的。
- **有限域**　已经对有限域章节进行了修改和扩展，主要是增加了一些文字和新的图片以使读者便于理解。
- **保留格式加密**　这种相对较新的加密模式获得了越来越多的商业成功。第 7 章新增了一节来讨论这种加密模式。
- **真随机数生成器的校正和性能测试**　现在第 8 章包含了这些重要的研究方向。
- **用户认证模型**　第 15 章给出了一般用户认证模型的新描述，以助于统一讨论各种不同用户认证模型。
- **云安全**　第 16 章有关云安全的内容已经做了更新和扩展，力求凸显它的重要性和最新的研究进展。
- **传输层安全（TLS）**　第 17 章的传输层安全相关内容已经更新而且重新组织以求更加清晰，并且增加了新 TLS 版本 1.3 的讨论。
- **邮件安全**　第 19 章已经完全重写以求提供一个全面的、最新的邮件安全讨论。它包括：
  - 新增：讨论邮件威胁及一种全面的保证邮件安全方法。
  - 新增：增加 STARTTLS 的讨论。STARTTLS 是提供保证 SMTP 机密性的一种新方法。
  - 修改：S/MIME 已经更新至最新的 3.2 版本。
  - 新增：新增加了 DNSSEC 的讨论及其在保证邮件安全中所起的作用。

- 新增：讨论了基于 DNS 的命名实体认证（DANE）以及使用这种方法加强 SMTP 和 S/MIME 中证书的安全性。
- 新增：新增加了发送方策略框架（SPF）的讨论。SPF 是一种用于认证电子邮件发件人的标准方法。
- 修改：修订了有关域名密钥识别邮件（DKIM）标准的讨论。
- 新增：增加了 DMARC 的讨论。DMARC 是一种允许发件人自己定义邮件的处理办法，用于接收反馈报告的类型以及这些返回报告的频率。

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。本书的前一部分给出关于密码学和网络安全的指导性的概述。后一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掌握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背景知识的动机，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。

ACM/IEEE 计算机科学课程 2013 的支持

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学与网络安全方面课程的教材，学时为一学期。本版的修订是为了支持当前草案版本的 ACM/IEEE 计算机科学课程 2013（CS2013）。CS2013 在课程体系中增加了 IAS（Information Assurance and Security）内容的课程，并将其作为计算机科学知识体系中的一个知识领域。CS2013 认为把 IAS 纳入课程体系，是因为 IAS 对于计算机科学教育具有关键作用。CS2013 把将所有课程分为三类：核心课程-1（课程应包含所有的课题）；核心课程-2（应包含全部或几乎全部的课题）；选修课程（根据意愿适当地提供广度与深度）。在 IAS 领域，CS2013 推荐把网络安全的基本概念纳入核心课程-1 和核心课程-2 中，而把密码学部分作为选修。本书实际上涵盖了 CS2013 所列举的三类课程中的所有课题。

本书还可用作参考用书或作为自学教材。

本书的组织

本书由以下八个部分组成。

- 概览
- 对称密码
- 公钥密码

- 密码学中的数据完整性算法
- 互信
- 网络与 Internet 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、习题、思考题和推荐读物。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。

教学支持文档[①]

本学科十分有趣而且发展迅速，本书的主要目的是为讲授这一学科内容提供一个有效的教学工具。该目的反映在本书的结构及支持文档。对于教师，我们提供了下列补充材料：

- **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。
- **习题集**：按章的习题集和答案。
- **教学大纲样例**：本书包含多于在一学期讲授的内容，因此为教师提供了若干教学大纲样例，以指导在有限时间使用本书。这些样例基于使用本书第五版的教授的实践经验。

在教师资源中心 IRC（Instructor Resource Center）中提供了所有的这些支持文档，可以通过出版商的网站：www.personhighered.com/stallings 或点击本书网站 WilliamStallings.com/Cryptography 上的教师资源链接来获取。

在本书网站 WilliamStallings.com/Cryptography 上（单击教师资源链接）还包括以下资源：

- 链接到使用本书的其他课程的网站。
- 使用本书的教师的邮箱列表，他们通过邮件互相讨论问题或对作者提出建议。

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，以加深对课本中所学知识的理解。本书在很大程度上对该课程提供全面的支持，包含了课程中一整套的项目组件。教师资源中心（IRC）不仅包含如何布置和构建项目，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。

① 教辅申请方式请联系 Te_service@phei.com.cn 获取（只向教师提供）——编者注。

- **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** 一系列针对本书里的概念进行编程和做实验的项目。
- **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。
- **防火墙项目** 一个简易的网络防火墙可视化模拟器课题，用以支持讲授防火墙基本原理的练习。
- **案例研究** 一系列的实际案例研究，包括学习目标，案例描述，系列的案例讨论问题。
- **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。

这些各种各样的项目和学生练习使得教师能够方便地使用本书，把它当作丰富多样的教学经验中的一个组件。从而可以方便地安排课程计划，以适应教师和学生的各种特殊需求。具体细节请参见附录 A。

Sage 计算机代数系统

本书的一个最重要的特色就是使用 Sage 实现密码算法示例和作业。Sage 是一个开源的、跨平台的免费软件包，它实现了一个强大的、灵活的、易学的数学和计算机代数系统。与 Mathematica，Maple 和 MATLAB 等系统不同，Sage 没有使用许可和使用费的限制。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电脑上在家里使用。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解决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，它能够使学生得到关于密码算法的第一手经验。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——数论和有限域** 欧几里得算法和扩展欧几里得算法、多项式算术、有限域 GF（2^4）、欧拉函数、Miller-Rabin 测试、因式分解、模幂运算、离散数学以及中国剩余定理。
- **第 3 章——传统加密技术** 仿射密码和 Hill 密码。
- **第 4 章——分组密码和数据加密标准** 基于 SDES 的练习。
- **第 6 章——高级加密标准 AES** 基于 SAES 的练习。
- **第 8 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 9 章——公钥密码与 RSA** RSA 加密/解密以及签名。
- **第 10 章——密钥管理和其他公钥密码体制** 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。

提供给学生的在线文档[①]

在新版书中，两个 Web 站点为学生提供了大量在线原始支持材料。WilliamStallings.com/Cryptography 上的伙伴网站（点击学生资源链接）包含一系列按章组织的章节和本书的勘误表。

购买新一版的书可以获得 6 个月在线材料访问权限，包括以下内容：

- **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 20 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，我们单独提供了家庭习题和答案集。
- **关键论文** 我们从专业文献中选择了一定数量的论文，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。

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：Hossein Beyzavi（Marymount University），Donald F. Costello（University of Nebraska-Lincoln），James Haralambides（Barry University），Anand seetharam（California State University at Monterey Bay），Marius C. Silaghi（Florida Institute of Technology），Shambhu Upadhyaya（University at Buffalo），Zhengping Wu（California State University at san Bernardino），Liangliang Xiao（Frostburg State University），Seong-Moo（Sam）Yoo（The University of Alabama in Huntsville），and Hong Zhang（Armstrong State University）。

我还要感谢那些详细审阅其中某一章或数章的人员：Dino M. Amaral, Chris Andrew, Prof.（Dr）. C. Annamalai, Andrew Bain, Ricccardo Bernardini, Olivier Blazy, Zervopoulou Christina, Maria Christofi, Dhananjoy Dey, Mario Emmanuel, Mike Fikuart, Alexander Fries, Pierpaolo

① 部分文件也可登录华信教育资源网（www.hxedu.com）注册下载——编者注。

Giacomin, Pedro R. M. Inácio, Daniela Tamy Iwassa, Krzysztof Janowski, Sergey Katsev, Adnan kilic, Rob Knox, Mina Pourdashty, Yuri Poeluev, Pritesh Prajapati, Venkatesh Ramamoorthy, Andrea Razzini, Rami Rosen, Javier Scodelaro, Jamshid Shokrollahi, Oscar So, and David Tillemans。

此外，我也有幸审阅了一些领域大师的研究成果，这些大师包括英特尔公司的 Jesse Walker（英特尔的数字随机数发生器）、Vigil Security 公司的 Russ Housley（密钥封装）、Joan Daemen（AES），Santa Clara 大学的 Edward F. Schaefer（简化的 AES）、前 RSA 实验室的 Tim Mathews（S/MIME）、Waterloo 大学的 Alfred Menezes（椭圆曲线密码学）、*The Cryotogram* 一书的编辑与发行人 William Sutton（古典密码）、Johns Hopkins 大学的 Avi Rubin（数论）、信息安全公司的 Michael Markowitz（SHA 和 DSS）、IBM 因特网安全系统部的 Don Davis（Kerberos）、BBN 科技公司的 Steve Kent（X.509）和 Phil Zimmerman（PGP）。

Nikhil Bhargava（IIT Delhi）开发了一系列的在线家庭作业和解答。Microsoft 和华盛顿大学的 Dan Shumow 开发了附录 B 和附录 C 中所有的 Sage 示例和作业。Dakata 州立大学的 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 大学的 Sanjay Rao 和 Ruben Torres 为教师资源中心（IRC）的实验室练习做了很多工作。下列人员为教师资源中心的项目计划做了许多工作：Henning Schulzrinne（Columbia 大学），Cetin Kaya Koc（Oregon 州立大学）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 Pearson 出版社的工作人员，特别是责任编辑 Tracy Johnson，项目经理 Carole Snyder，以及产品部经理 Bob Engelhardt。还要感谢 Pearson 出版社的市场和销售工作人员，没有他们的努力，这本书就不可能摆在你的面前。

关于作者

William Stallings 编写出版了 18 部著作，经修订再版累计共出版了 40 多本关于计算机安全、计算机网络和计算机体系结构等领域的书籍。他的著作无数次出现在出版物中，包括 *Proceedings of the IEEE*、*ACM Computing Reviews and Cryptologia*。

他 13 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站 WilliamStallings.com/StudentSupport.html。该网站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。

符 号 表

符号	表达式	含义
D,K	D(K,Y)	用密钥 K 和对称密码算法解密密文 Y
D,PR_a	D(PR_a,Y)	用 A 的私钥 PR_a 和非对称密码算法解密密文 Y
D,PU_a	D(PU_a,Y)	用 A 的公钥 PU_a 和非对称密码算法解密密文 Y
E,K	E(K,X)	用密钥 K 和对称密码算法加密明文 X
E,PR_a	E(PR_a,X)	用 A 的公钥 PU_a 和非对称密码算法加密明文 X
E,PU_a	E(PU_a,X)	用 A 的公钥 PU_a 和非对称密码算法加密明文 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, $\equiv$	$a \equiv b \pmod m$	$a \bmod m = b \bmod m$
mod, $\neq$	$a \neq b \pmod m$	$a \bmod m \neq b \bmod m$
dlog	$\mathrm{dlog}_{a,p}(b)$	以 a 为底 b 的对数，模 p 运算
φ	$\varphi(n)$	欧拉函数，小于 n 且和 n 互素的正整数个数
$\sum$	$\sum_{i=1}^{n} a_i$	$a_1+a_2+\cdots+a_n$
$\prod$	$\prod_{i=1}^{n} a_i$	$a_1 \times a_2 \times \cdots \times a_n$
$\mid$	$i \mid j$	i 整除得尽 j，即 i 除 j 的余数为零
$\lvert,\rvert$	$\lvert a \rvert$	a 的绝对值
$\parallel$	$x \parallel y$	级联 x 和 y
$\approx$	$x \approx y$	x 约等于 y
$\oplus$	$x \oplus y$	单比特变量时是异或运算，多比特变量时是按位异或
$\lfloor,\rfloor$	$\lfloor x \rfloor$	小于等于 x 的最大整数
$\in$	$x \in S$	元素 x 包含于集合 S
$\longleftrightarrow$	$A \longleftrightarrow (a_1,a_2,\cdots,a_k)$	整数 A 和整数序列$(a_1,a_2,\cdots,a_k)$对应

目　录

在 线 部 分