

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（第二版）

Cryptography and Network Security
Principles and Practice
Second Edition

[美] William Stallings 著

杨明 胥光辉 齐望东 等译

谢希仁 审校



电子工业出版社

Publishing House of Electronics Industry
URL: <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(第二版)

Cryptography and Network Security Principles and Practice
Second Edition

[美] William Stallings 著

杨明 胥光辉 齐望东 等译

谢希仁 审校

电子工业出版社

Publishing House of Electronics Industry

北京·BEIJING

内 容 简 介

密码编码学与网络安全是当今通信与计算机界的热门课题。本书内容新颖丰富,讲述了基本的数据加密原理和数论的概念、各种加密算法和常用的协议以及它们在网络中的应用。书中各章都提供了许多习题和参考读物,并列出了推荐网站。

本书适用于通信或计算机专业的本科生或研究生,也可作为通信或计算机领域的研究人员和专业技术人员的参考书。

Authorized translation from the English language edition published by Prentice-Hall, Inc. Copyright© 1999.

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording or by any information storage retrieval system, without permission from the Publisher.

Simplified Chinese language edition published by Publishing House of Electronics Industry. Copyright© 2001.

本书中文简体专有翻译出版版权由 Pearson 教育集团所属的 Prentice-Hall, Inc. 授予电子工业出版社。其原文版权及中文翻译出版版权受法律保护。未经许可,不得以任何形式或手段复制或抄袭本书内容。

图书在版编目(CIP)数据

密码编码学与网络安全:原理与实践(第二版)/(美)斯大林(Stallings, W.)著;杨明等译.

—北京:电子工业出版社,2001.4

国外计算机科学教材系列

书名原文: Cryptography and Network Security: Principles and Practice Second Edition

ISBN 7-5053-6604-1

I. 密... II. ①斯...②杨... III. ①保密编码-理论②计算机网络-安全技术 IV. TP309.7

中国版本图书馆 CIP 数据核字(2001)第 18948 号

丛 书 名: 国外计算机科学教材系列

书 名: 密码编码学与网络安全:原理与实践(第二版)

原 书 名: Cryptography and Network Security: Principles and Practice Second Edition

著 者: [美]William Stallings

译 者: 杨 明 胥光辉 齐望东 等

审 校 者: 谢希仁

责任编辑: 吴 源

排版制作: 电子工业出版社计算机排版室监制

印 刷 者: 北京天竺颖华印刷厂

出版发行: 电子工业出版社 URL: <http://www.phei.com.cn>

北京市海淀区万寿路 173 信箱 邮编 100036

经 销: 各地新华书店

开 本: 787×1092 1/16 印张: 28.5 字数: 729 千字

版 次: 2001 年 4 月第 1 版 2001 年 4 月第 1 次印刷

书 号: ISBN 7-5053-6604-1
TP·3665

定 价: 48.00 元

版权贸易合同登记号 图字: 01-2000-3488

凡购买电子工业出版社的图书,如有缺页、倒页、脱页、所附磁盘或光盘有问题者,请向购买书店调换。若书店售缺,请与本社发行部联系调换。电话 68279077

出版说明

随着 21 世纪的到来, 计算机技术的发展更加迅猛, 在各行各业的应用更加广泛, 越来越多的高等院校增设了有关计算机科学的课程内容, 或对现有计算机课程设置进行了适当调整, 以紧跟前沿技术。在这个教学体系和学科结构变革的大环境下, 对适合不同院系、不同专业、不同层次的教材的需求量与日俱增。此时, 如果能够借鉴、学习国外一流大学的先进教学体系, 引进具有先进性、实用性和权威性的国外一流大学计算机教材, 汲取其精华, 必能更好地促进中国高等院校教学的全面改革。

美国 Prentice Hall 出版公司是享誉世界的高校教材出版商, 自 1913 年成立以来, 一直致力于教材的出版, 所出版的计算机教材为美国众多大学采用, 其中有不少是专业领域中的经典名著, 已翻译成多种文字在世界各地的大学中使用, 成为全人类的共同财富。许多蜚声世界的教授、学者都是该公司的资深作者, 如道格拉斯·科默 (Douglas E. Comer)、威廉·斯大林 (William Stallings) 等。早在 1997 年, 电子工业出版社就从 Prentice Hall 引进了一套计算机英文版专业教材, 并将其翻译出版, 同时定名为《国外计算机科学教材系列》(下称: 第一轮教材)。截至 2000 年 12 月, 该系列教材已出版 23 种, 深受读者欢迎, 被许多大学选为高年级学生和研究生教材或参考书。

4 年过去了, 已出版的教材中多数已经有了后续版本。因此, 我们开始设计新一轮教材 (第二轮教材) 的出版, 成立了由我国计算机界著名专家和教授组成的“教材出版委员会”, 并结合第一轮教材的使用情况和师生反馈意见, 组织了第二轮《国外计算机科学教材系列》出版工作。

第二轮教材的出版原则为:

1. 引进 Prentice Hall 出版公司 2000 年和 2001 年推出的新版教材, 作为替换版本。
2. 在著名高校教授的建议下, 除了从 Prentice Hall 新选了一些教材之外, 还从 McGraw-Hill 和 Addison Wesley Longman 等著名专业教材出版社、麻省理工学院出版社和剑桥大学出版社等著名大学出版社引进了一些经典教材, 作为增补版本。
3. 对于第一轮中无新版本的优秀教材, 我们将其作为延用版本, 直接进入第二轮使用。
4. 对于第一轮中翻译质量较好且无新版本的教材, 我们将其进行了修订, 也作为延用版本, 进入第二轮使用。

这次推出的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 and 自由组合使用。

按照计划, 本轮教材规划出版 37 种, 其中替换版本 8 种, 新增版本 14 种, 延用版本 15 种。教材内容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。本轮教材计划于 2001 年 7 月前全部出版。教材的使用年限平均为 3 年。我们还将陆续推出一些教材的参考课件, 希望能为授课老师提供帮助。

为了保证本轮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轮教材的选题、翻译和审校工作。他们中既有讲授同类教材的骨干教师和博士,也有积累了几十年教学经验的教授和博士生导师。

在本轮教材的选题、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:

1. 对于新选题和新版本进行了全面论证。
2. 对于沿用版本,认真审查了前一版本教材,修改了其中的印刷错误。
3. 对于译者和编辑的选择,达到了专业对口。
4. 对于从英文原书中发现的错误,我们通过与作者联络、从网上下载勘误表等方式,一一做了修改。
5. 对于翻译、审校、编辑、排版、印刷质量进行了严格的审查把关。

通过这些工作,保证了本轮教材的质量较前一轮有明显的提高。相信读者一定能够从字里行间体会到我们的这些努力。

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。

由于我们对国际计算机科学、我国高校计算机教育的发展存在认识上的不足,在选题、翻译、出版等方面的工作中还有许多有待提高之处,恳请广大师生和读者提出批评和建议。

电子工业出版社
2001年春

教材出版委员会

- | | | |
|----|-----|---|
| 主任 | 杨芙清 | 北京大学教授
中国科学院院士
北京大学信息与工程学部主任
北京大学软件工程研究所所长 |
| 委员 | 王 珊 | 中国人民大学信息学院院长、教授 |
| | 胡道元 | 清华大学计算机科学与技术系教授
国际信息处理联合会通信系统中国代表 |
| | 钟玉琢 | 清华大学计算机科学与技术系教授
中国计算机学会多媒体专业委员会主任 |
| | 谢希仁 | 中国人民解放军理工大学教授
全军网络技术研究中心主任、博士生导师 |
| | 尤晋元 | 上海交通大学计算机科学与工程系教授
上海分布计算技术中心主任 |
| | 施伯乐 | 中国计算机学会常务理事、上海市计算机学会理事长
上海国际数据库研究中心主任、复旦大学教授 |
| | 邹 鹏 | 国防科学技术大学计算机学院教授、博士生导师
教育部计算机基础教学课程指导委员会副主任委员 |
| | 张昆藏 | 青岛大学信息工程学院教授 |

译 者 序

我们愿意向广大读者推荐 William Stallings 教授的《密码编码学与网络安全:原理与实践(第二版)》的中译本。

Stallings 早年在麻省理工学院获博士学位,是国际上颇有影响的计算机网络专业的教授。他先后出版了十几种不同的教材,内容涉及数据通信、计算机通信、高速网络、计算机操作系统、计算机组织与体系结构、网络安全等领域。本书的第一版曾在 1999 年获美国 TEXTY 的最佳计算机科学与工程教科书奖。

本书的特点是内容丰富新颖,既有基本的数据加密原理和最基本的数论的概念,也有各种加密算法和常用的协议以及它们在网络中的应用。本书各章都有相当数量的习题。一些较深入的内容还放在有些章的附录中,可供读者进一步学习。在每章的后面还附上了作者推荐的一些有价值的参考读物和网站,以便读者上网查找更多的信息。由于网络安全是一个发展非常迅速的领域,对这一领域有兴趣的读者可以在本书的基础上进一步从因特网上找到更多信息。

本书的原书序和第 1 章至第 2 章由陈鸣教授(博士)翻译,第 3 章至第 6 章由齐望东副教授(博士)翻译,第 7 章至第 11 章由杨明讲师(博士)翻译,第 12 章至第 16 章和附录由胥光辉讲师(博士)翻译,全书由谢希仁教授审校。

原书的一些错误已在翻译过程中予以更正。对于作者在因特网上发布的勘误表中没有列出的错误,我们都曾用电子邮件与作者进行过联系。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。

原 书 序

在这个世界范围的电子连通时代中,既有病毒和黑客,又有电子窃听和电子欺骗,网络安全每时每刻都是举足轻重的。下面两个趋势的一起到来使得本书中的主题至关重要:首先,计算机系统及其网络互联的爆炸性增长,使得机构和个人都更增加了对使用这些系统存储信息和交流信息的依赖性,因此导致了保护数据和资源免遭泄密、确保数据和消息处于机密并保护系统免受基于网络攻击意识的提高。其次,密码编码学和网络安全的学科已经成熟,从而导致加强具有安全性的实用的应用程序的研制。

目的

本书的目的是给出密码编码学和网络安全在原则和实践两方面的概述。在本书的前两部分,与网络安全能力有关的基本问题通过提供指南和密码编码学和网络安全技术的纵览来探讨,本书后面的部分涉及网络安全的实践:能提供网络安全性且已经被实现或正在使用的实际应用。

因此本书的主题是从许多学科提取出来的。特别是如果对一些基本理论和某些来自概率论的结果不了解,要理解在本书中所讨论的技术的重要性是不可能的。总之,作者试图使本书能够包含尽可能足够多的内容。本书不仅给出了所需要的基本数学结果,而且为读者提供了对这些结果的直觉理解,还根据需要提供了有关的背景材料。这种方法有助于激发对这些材料的学习热情,并且作者认为这比在书的开始就一下全部给出所有数学材料的做法要好。

读者

本书是为从事学术和专业的读者而写的。作为一本教科书,它能够作为计算机科学、计算机工程和电气工程专业的本科生所开设的密码编码学和网络安全课程的教材,也可作为基本的参考资料并适合于自学。

本书的结构

本书由四部分组成:

第一部分——**常规加密**:详细介绍了常规加密算法和设计原则,包括用于机密性事务的常规加密的讨论。

第二部分——**公钥加密和散列函数**:详细介绍了公钥算法和加密原则。此部分还讲解了报文鉴别编码和散列函数的使用以及数字签名和公钥证书。

第三部分——**网络安全实践**:涵盖重要的网络安全工具和应用,包括 Kerberos、X.509v3 证书、PGP、S/MIME、IP安全性、SSL/TLS 和 SET。

第四部分——**系统安全性**:考虑了系统级的安全性问题,包括入侵者和病毒的威胁和反措施以及防火墙和可信系统的使用。

在第 1 章结尾将有一个更为详细的提要;此外,本书还包括了一个范围广泛的词汇表,一个经常使用的首字母缩写词表和一个参考文献表;在每章的结束有习题和进一步阅读的建议。

针对教师和学生的 Internet 服务

本书有一个相应的网页,该网页对学生和教师提供支持。网页包括与相关站点的链接,以 PDF(Adobe Acrobat)格式提供书中的原版插图以及有关本书的 Internet 邮件列表的签约信息。该 Web 页位于 <http://www.shore.net/~ws/Security2e.html>。此外,还建立了一个 Internet 邮件列表,因此使用本书的教师能够彼此之间以及与作者之间交换信息、建议和问题。一旦发现印刷或其他错误,可在 <http://www.shore.net/~ws> 处找到本书的勘误表。

用于教授密码编码学和网络安全的项目

对许多教师而言,密码编码学或安全性课程的一个重要组成部分是一个项目或一系列项目,学生能通过项目获得专业经验,以加深对书本概念的理解。本书在课程中包含一个项目部分,给学生提供了强有力的支持。教师手册不仅包括如何指派和构造项目的指南,也包括一系列建议项目,这些项目涵盖了范围广泛的主题:

- 研究项目:一系列研究任务指示学生研究 Internet 上的特定主题并书写报告。
- 编程项目:一系列编程项目涵盖范围广泛的主题,能够在任何平台上以任何适合的语言加以实现。
- 阅读/报告任务:文献中的一些论文(每章一篇),而且要求学生读后写出简短报告。详情请参见附录。

第二版新在何处

自从本书的第一版出版以来过去 4 年了,该领域一直在经历着不断的革新和改进。在这个新版中,作者在使内容广泛和全面覆盖整个领域的同时,试图反映这些变化。在开始校订的过程中,本书的第一版由许多教授该课程的教授们进行了全面的检查和评论。其结果是,许多地方的叙述变得明确而紧凑,而且插图也得以改进。另外,增加了许多新的“现场测试”问题。

一个明显的变化是本书的标题;本书现在称为《密码编码学与网络安全:原理与实践(第二版)》,以反映在网络安全中的密码编码算法的中心作用。本书也已经彻底重组,以提供一个逻辑性更好的顺序供课堂教学和自学使用。

除了改进教学法和用户友好性外,本书通篇有重大的和实质性的变化。最显著的部分包括:

- 新增加的——分组密码设计的讨论:增加了三节内容来讨论分组密码的结构、分组密码设计原则和近期先进密码的特性,大大加强了常规加密的全面讨论。
- 新增加的——增加了常规加密算法:本书现在包括近来在商用产品和 Internet 标准中使用的算法,包括 Blowfish、RC5 和 CAST-128。
- 新增加的——椭圆曲线密码的处理:这已经成为 RSA 和 Diffie-Hellman 公钥密码的一个重要替代算法。
- 扩展的——数论的篇幅:其范围已经被扩展为整章,包括许多设计出来的例子以阐明这个抽象的主题。
- 新增加的——散列编码和 MAC 设计的讨论:增加了有关散列函数的设计原则和安全性以及报文鉴别编码的讨论。
- 扩展的——X.509 和 X.509v3 新处理的篇幅:X.509 公钥证书(尤其是版本 3)现在已经

在许多产品和 Internet 标准中得到应用。

- 新增加的——S/MIME 的篇幅：S/MIME 已经成为商用安全电子邮件的标准。
- 新增加的——IP 安全性章节：IPsec 是一个构造虚拟专用网和对跨越 Internet 端到端安全性的重要的新标准集合，已经增加了完整的一章来研究这个重要题目。
- 新增加的——Web 安全性章节：Web 安全性已经成为网络安全最为重要的领域之一，并产生了许多新挑战，已经增加了完整的一章来研究这个重要题目。该章包括了两个主要的 Web 安全性标准：
 - 安全套接层(SSL)和运输层安全性(TLS)：SSL 是对 Web 安全性事实上的标准，事实上能够在所有浏览器和服务器的提供中找到它；TLS 是一个正在出现的试图替代 SSL 的标准。
 - 安全电子交易(SET)：SET 是一个经过 Web 进行安全电子商务的新兴标准。
- 新增加的——防火墙的章节。防火墙已作为保护与 Internet 相连的企业站点的产品。
- 新增加的——扩展了对教师的支持：和以前一样，教师手册包括对本书中所有习题的答案。此外，如前所述，手册提供了对学生项目的支持。
- 其他变化：这些变化包括如下：
 - 有关 bent 功能的新的一节，这些功能对用于常规加密算法的 S 盒子的设计是重要的。
 - 在许多章的“推荐读物”中给出了相关 Web 站点。
 - 新增了几十道课后作业题。

致谢

本书得益于在该领域中许多专家的评审，他们为此慷慨奉献出他们的时间和专业知识。下列专家评审了第一版的所有的或大部分内容：Shivakumar Sastry (Rocawell Automation)、Alan Sherman (MD Baltimore Country 大学)、Tom Dunigan (田纳西大学)、Dan Boneh (斯坦福大学)、Sushil Jajodia (George Mason 大学)。

此外，我对由“主题领域领袖”(subject-area gurus)对各个主题进行评审感到极为幸运，他们是 MIT 的 Ron Rivest (RC5 和 MD5)、RSA 数据安全的 Tim Mathews (S/MIME)、床罩系统的 Bruce Schneier (Blowfish)、信托技术的 Carlisle Adams (CAST 和 bent 函数)、滑铁卢大学的 Alfred Menezes (椭圆曲线密码编码学)、Ritter 软件工程的 Terry Ritter (bent 函数)、《密码》(杂志)的编辑和出版商 William G. Sutton (经典加密)、AT&T 实验室的 Aviel Rubin (数论)、Katholieke Universiteit Leuven 的 Bart Preneel (RIPEMD-160)、信息安全公司的 Michael Markowitz (SHA 和 DSS)、R3 安全工程 AG 的 Xuejia Lai (IDEA)、Openvision 技术的 Don Davis (Kerberos)、Steve Kent (X.509)、巨石软件工程的 Phil Zimmermann (PGP) 以及 Santa Clara 大学的 Ed Scheafer (简化的 DES)。

下列人员对教师手册中的项目任务做出了贡献：Henning Schulzrinne (哥伦比亚大学)、Cetin Kaya Koc (俄勒冈州大学)、David Balenson (委托信息系统和乔治华盛顿大学)。我也要感谢那些对习题做出贡献的人：Luke O'Connor、MITER 的 Joseph Kusmiss、Stratus 的 Carl Ellison、Shunmugavel Rajarathinam 和 Jozef Vyskoc (他对那些令人惊奇的福尔摩斯问题做出了贡献)。

目 录

第 1 章 引言	1
1.1 攻击、服务和机制	2
1.1.1 服务	3
1.1.2 机制	4
1.1.3 攻击	4
1.2 对安全的攻击	5
1.2.1 被动攻击	6
1.2.2 主动攻击	6
1.3 安全服务	7
1.3.1 机密性	7
1.3.2 鉴别	7
1.3.3 完整性	7
1.3.4 不可抵赖	8
1.3.5 访问控制	8
1.3.6 可用性	8
1.4 网络安全模型	8
1.5 本书概要	10
1.6 推荐读物	12
附录 1A Internet 和 Web 资源	12
本书的 Web 站点	12
其他 Web 站点	12
USENET 新闻组	13
第一部分 常规加密	14
第 2 章 常规加密的经典技术	16
2.1 常规加密模型	16
2.1.1 密码编码学	17
2.1.2 密码分析	18
2.2 隐写术	20
2.3 经典加密技术	21
2.3.1 替代技术	22
2.3.2 置换技术	32
2.3.3 转子机(Rotor Machine)	33
2.4 推荐读物	34
2.5 习题	35

第3章 常规加密的现代技术	38
3.1 简化的 DES	38
3.1.1 概述	38
3.1.2 S-DES 密钥的产生	39
3.1.3 S-DES 的加密操作	41
3.1.4 对简化版 DES 的分析	43
3.1.5 与 DES 的关系	43
3.2 分组密码的原理	44
3.2.1 流密码和分组密码	44
3.2.2 Feistel 密码结构的设计动机	44
3.2.3 Feistel 密码	46
3.3 数据加密标准	51
3.3.1 DES 加密	52
3.3.2 DES 的解密	57
3.3.3 雪崩效应	57
3.4 DES 的强度	58
3.4.1 56 bit 密钥的使用	58
3.4.2 DES 算法的性质	59
3.5 差分与线性密码分析	60
3.5.1 差分密码分析	60
3.5.2 线性密码分析	61
3.6 分组密码设计原理	62
3.6.1 DES 的设计准则	62
3.6.2 循环次数	63
3.6.3 函数 F 的设计	64
3.6.4 密钥调度算法	65
3.7 分组密码的操作方式	65
3.7.1 电子密码本方式	66
3.7.2 密码分组链接方式	66
3.7.3 密码反馈方式	68
3.7.4 输出反馈方式	70
3.8 推荐读物	71
3.9 习题	71
附录 3A 曲折函数(bent function)	73
第4章 常规加密的算法	75
4.1 三重 DES	75
4.1.1 双重 DES	75
4.1.2 两个密钥的三重 DES	77

4.1.3	使用三个密钥的三重 DES	79
4.2	国际数据加密算法	79
4.2.1	设计原理	79
4.2.2	IDEA 加密	82
4.2.3	IDEA 的解密	85
4.3	Blowfish	87
4.3.1	子密钥和 S 盒子的产生	87
4.3.2	加密和解密	89
4.3.3	讨论	90
4.4	RC5	91
4.4.1	RC5 的参数	92
4.4.2	密钥扩展	92
4.4.3	加密	94
4.4.4	解密	95
4.4.5	RC5 的操作方式	95
4.5	CAST-128	96
4.5.1	CAST-128 的加密	96
4.5.2	替代盒子	97
4.5.3	子密钥产生	98
4.5.4	讨论	98
4.6	RC2	99
4.6.1	密钥扩展	100
4.6.2	加密	100
4.7	先进对称分组密码的特点	101
4.8	习题	102
第 5 章	使用常规加密进行保密通信	105
5.1	加密功能的位置	105
5.1.1	窃密攻击的可能位置	105
5.1.2	链路加密与端到端加密	107
5.2	通信量的机密性	111
5.2.1	链路加密方式	112
5.2.2	端到端加密方式	112
5.3	密钥分配	112
5.3.1	一个密钥分配方案	114
5.3.2	层次式密钥控制	115
5.3.3	会话密钥的使用寿命	116
5.3.4	一种透明的密钥控制方案	116
5.3.5	分散式密钥控制	117

5.3.6	控制密钥的使用方式	118
5.4	随机数的产生	119
5.4.1	随机数的用途	119
5.4.2	随机数的来源	120
5.4.3	伪随机数产生器	121
5.4.4	密码编码方式产生的随机数	122
5.4.5	Blum Blum Shub 产生器	124
5.5	推荐读物	125
5.6	习题	126
第二部分 公开密钥加密和散列函数		129
第 6 章 公开密钥密码编码学		130
6.1	公开密钥密码系统的原理	131
6.1.1	公开密钥密码系统	131
6.1.2	公开密钥密码系统的应用	135
6.1.3	对公开密钥密码编码学的要求	136
6.1.4	公开密钥密码分析	137
6.2	RSA 算法	137
6.2.1	对算法的描述	138
6.2.2	计算方面	139
6.2.3	RSA 的安全性	142
6.3	密钥管理	145
6.3.1	公开密钥的分配	145
6.3.2	秘密密钥的公开密钥加密分配	149
6.4	Diffie-Hellman 密钥交换	151
6.5	椭圆曲线密码编码学	154
6.5.1	椭圆曲线	154
6.5.2	有限域上的椭圆曲线	156
6.5.3	使用椭圆曲线的密码编码学	157
6.5.4	椭圆曲线密码编码学的安全性	159
6.6	推荐读物	159
6.7	习题	160
附录 6A	算法的复杂性	164
第 7 章 数论导引		167
7.1	素数和互为素数	167
7.1.1	因子	167
7.1.2	素数	168
7.1.3	互为素数	169

7.2	模运算	170
7.2.1	模运算操作	171
7.2.2	模运算的性质	172
7.3	费马定理和欧拉定理	174
7.3.1	费马定理	174
7.3.2	欧拉函数	175
7.3.3	欧拉定理	176
7.4	检测素数	177
7.5	欧几里德算法	178
7.5.1	寻找最大公因子	179
7.5.2	寻找乘法逆元	180
7.6	中国余数定理	181
7.7	离散对数	183
7.7.1	整数幂, 模 n	183
7.7.2	指数	184
7.7.3	离散对数的计算	186
7.8	推荐读物	186
7.9	习题	187
第 8 章	报文鉴别与散列函数	190
8.1	鉴别的需求	190
8.2	鉴别函数	190
8.2.1	报文加密	191
8.2.2	报文鉴别码	195
8.2.3	散列函数	197
8.3	报文鉴别码	200
8.3.1	MAC 的需求	200
8.3.2	基于 DES 的报文鉴别码	201
8.4	散列函数	202
8.4.1	散列函数的需求	203
8.4.2	简单的散列函数	203
8.4.3	生日攻击	205
8.4.4	分组链接技术	207
8.5	散列函数和 MAC 的安全性	207
8.5.1	强行攻击	208
8.5.2	密码分析	209
8.6	推荐读物	210
8.7	习题	211
附录 8A	生日攻击的数学基础	211

8A.1	相关问题	212
8A.2	生日悖论	212
8A.3	有用的不等式	213
8A.4	重复问题的一般性例子	213
8A.5	两个相交的集合	215
第9章	散列算法	216
9.1	MD5 报文摘要算法	216
9.1.1	MD5 逻辑	216
9.1.2	MD5 压缩函数	219
9.1.3	MD4	222
9.1.4	MD5 的强度	223
9.2	安全的散列算法	223
9.2.1	SHA-1 逻辑	223
9.2.2	SHA-1 压缩函数	225
9.2.3	SHA-1 与 MD5 的比较	227
9.3	RIPEMD-160	228
9.3.1	RIPEMD-160 逻辑	228
9.3.2	RIPEMD-160 压缩函数	230
9.3.3	RIPEMD-160 设计思想	232
9.3.4	与 MD5 和 SHA-1 的比较	233
9.4	HMAC	234
9.4.1	HMAC 设计目标	234
9.4.2	HMAC 算法	235
9.4.3	HMAC 的安全性	236
9.5	习题	237
第10章	数字签名和鉴别协议	239
10.1	数字签名	239
10.1.1	需求	239
10.1.2	直接数字签名	240
10.1.3	需仲裁的数字签名	240
10.2	鉴别协议	242
10.2.1	相互鉴别	242
10.2.2	单向鉴别	246
10.3	数字签名标准	248
10.3.1	DSS 方法	248
10.3.2	数字签名算法	249
10.4	推荐读物	250

10.5 习题	251
附录 10A 数字签名算法的证明	253
第三部分 网络安全实践	255
第 11 章 鉴别应用	256
11.1 Kerberos	256
11.1.1 动机	256
11.1.2 Kerberos 第 4 版	257
11.1.3 Kerberos 第 5 版	266
11.2 X.509 鉴别服务	270
11.2.1 证书	270
11.2.2 鉴别过程	274
11.2.3 X.509 第 3 版	275
11.3 推荐读物	277
11.4 习题	277
附录 11A Kerberos 加密技术	278
11A.1 口令到密钥的转换	278
11A.2 传播密码分组链接模式	279
第 12 章 电子邮件的安全性	281
12.1 PGP 加密软件	281
12.1.1 符号	281
12.1.2 操作描述	282
12.1.3 加密密钥和密钥环	286
12.1.4 公开密钥管理	292
12.2 S/MIME	296
12.2.1 RFC 822	296
12.2.2 通用 Internet 邮件扩充 MIME	296
12.2.3 S/MIME 的功能	302
12.2.4 S/MIME 报文	304
12.2.5 S/MIME 证书的处理	307
12.2.6 增强的安全服务	309
12.3 推荐读物	310
12.4 习题	310
附录 12A 使用 ZIP 的数据压缩	310
12A.1 压缩算法	311
12A.2 解压算法	312
附录 12B Radix-64 转换	312
附录 12C PGP 随机数的产生	314