Mc Graw Hill Education

清华计算机图书·译丛

Cryptography and Network Security

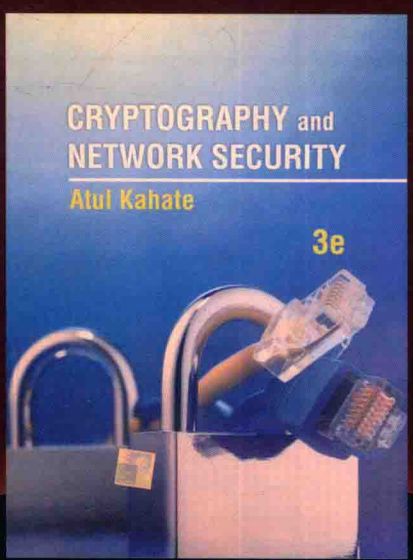
Third Edition

密码学与网络安全

（第3版）

Atul Kahate 著

金名 等译



清华大学出版社

清华计算机图书·译丛

Cryptography and Network Security

Third Edition

密码学与网络安全

（第3版）

Atul Kahate 著

金名 等译

清华大学出版社

北京

Atul Kahate
Cryptography and Network Security, 3e
EISBN: 978-1-25-902988-2

图书在版编目（CIP）数据

密码学与网络安全(第 3 版)/(印)阿图尔·卡哈特(Atul Kahate)著；金名等译. —北京：清华大学出版社，2018
(清华计算机图书译丛)
书名原文：Cryptography and Network Security, Third Edition
ISBN 978-7-302-47935-2

Ⅰ. 密…　Ⅱ. ①阿…　②金…　Ⅲ. ①密码学　②计算机网络－网络安全　Ⅳ. ①TN918.1　②TP393.08

中国版本图书馆 CIP 数据核字(2017)第 196354 号

责任编辑：龙启铭
封面设计：傅瑞学
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
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　　邮　　编：100084
社 总 机：010-62770175　　邮　　购：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课件下载：http://www.tup.com.cn,010-62795954
印 装 者：清华大学印刷厂
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张**：26.5　　**字　　数**：639 千字
版　　次：2018 年 1 月第 1 版　　**印　　次**：2018 年 1 月第1 次印刷
印　　数：1～2000
定　　价：79.00 元

产品编号：072880-01

译者序

随着计算机技术，尤其是网络技术的飞速发展，各行各业都离不开计算机，离不开网络。网络技术的出现和发展，在极大地方便了我们的工作和学习的同时，也带来了很多安全方面的难题。因安全漏洞和黑客入侵而造成巨大损失的案例日益增多。网络安全问题日益重要和迫切。要实现网络安全，就离不开加密技术。

加密技术，已经与我们的日常生活息息相关了。我们每天通过网络传输的邮件、银行账户、密码等信息，都是经过加密后发送出去的，只不过我们通常没有意识到这些加密工作，都是由相应的应用程序为我们完成而已。如果不经过加密，那么后果难以想象。

人们通常认为加密是一种很高深很神秘的技术。其实不尽然。这里举一个简单的例子。

> 小明班上总共有 n 名同学（n 大于等于 3），一次数学考试后，老师把判分后的试卷发回给每个同学，由于老师忘了统计这次数学考试的班平均成绩，因此请小明来替老师完成这项工作，且要求确保每个同学自己的得分不让其他同学知道。那么，小明该怎样做呢？

这里，小明只需可以使用一个小的加密，就可以完成老师交给的这项工作。通过本书的学习，读者就可以帮小明找到解决办法。

本书以清晰的脉络、简洁的语言，介绍各种加密技术、网络安全协议与实现技术等内容，并给出具体的案例实现分析，是一本关于密码学与网络安全的理论结合实践的优秀教材。

本书由金名主译，黄刚、陈宗斌、陈河南、傅强、宋如杰、蔡江林、陈征、戴锋、蔡永久、邱海艳、张军鹏、吕晓晴、杨芳、郭宏刚、黄文艳、刘晨光、苗文曼、崔艳荣、王祖荣、王珏辉、陈中举、邱林、陈勇、杨舒、秦航、潘劲松、黄艳娟、姜盼、邱爽、张丹、胡英、刘春梅、姜延丰、钟宜峰、李立、李彤、付瑶、张欣欣、张宇超、朱敏、王晓亮、杨帆、万书振、解德祥等人也参与了部分翻译工作。欢迎广大读者指正。

作者介绍

Atul Kahate 在印度和世界 IT 业已经有 17 年的工作经验。目前，他是 Pune 大学和 Symbiosis 国际大学的兼职教授。他在 IIT、Symbiosis、Pune 以及其他很多大学多次讲授了实训编程研修班课程。

Atul Kahate 是一位多产的作者，他已经编写了 38 本书，涉及计算机科学、科学与技术、医学、经济学、板球、管理学以及历史等领域。他编写的 *Web Technologies*、*Cryptography and Network Security*、*Operating Systems Data Communications and Networks*、*An Introduction to Database Management Systems* 等书被印度和其他很多国家的大学用作教材，其中一些已翻译为中文。

Atul Kahate 获得过多次奖项。他出现在不少电视频道的节目中。他还是多个国际板球比赛中的官方统计员和计分员。此外，他还收集了大量关于 IT、板球、科学与技术、历史、医学、管理方面的文章 4000 多篇。

第3版前言

本书的前两个版本已被好几千的学生、教师和IT专业人员所使用。本版针对的读者对象仍然不变。本书可用作计算机安全或密码学课程的本科、研究生教材。本书主要阐述密码学的知识，任何对计算机科学和网络技术有基本了解的人都可以学习本书，不需要其他预备知识。

计算机与网络安全是今天最重要的领域。现在，对所有类型的计算机系统和网络发生了太多的攻击，因此，对那些将来要成为IT专业人员的学生来说，学习这些知识尤为重要。所以，在本版中增加了云安全、Web服务安全等内容。本书以非常清晰的方式，并给出大量图表，阐述每个主题的内容。

本书特点

(1) 以自底向上的方式介绍：密码学→网络安全→案例研究。

(2) 涵盖了最新内容：IEEE 802.11安全、ElGamal加密、云安全以及Web服务安全。

(3) 对加密法、数字签名、SHA-3算法的介绍进行了改进。

(4) 通过案例研究，帮助读者掌握相关内容的实际应用。

(5) 更新内容包括：

- 150道编程题；
- 160道练习题；
- 170道多选题；
- 530幅插图；
- 10个案例研究。

本书的组织结构如下。

第1章介绍安全的基本概念，讨论安全需求、安全原则，以及针对计算机系统与网络的各种攻击。介绍所有这些内容背后的概念理论，以及实际问题，并一一举例说明，以便加深对安全性的了解。如果不了解为什么需要安全性，有什么威胁，就无从了解如何保护计算机系统与网络。新增有关无线网络攻击的内容。删除一些有关Cookie与ActiveX控件的过时内容。

第2章介绍密码学的概念，这是计算机安全的核心内容。加密是用各种

算法来实现的。所有这些算法或者将明文替换成密文，或者用某种变换方法，或者是二者的组合。然后该章将介绍加密与解密的重要术语。该章详细介绍 Playfair 加密和希尔加密，展开介绍 Diffie-Hellman 密钥交换，详细介绍各种攻击的类型。

第 3 章介绍基于计算机的对称密钥加密法的各种问题。介绍流和块加密以及各种链接模式，并介绍主要的对称密钥加密算法，如 DES、IDEA、RC5 与 Blowfish。详细介绍 Feistel 加密，对 AES 的安全性问题也进行介绍。

第 4 章介绍非对称密钥加密的概念、问题与趋势，介绍非对称密钥加密的历史，然后介绍主要的非对称密钥加密，如 RSA、MD5、SHA 与 HMAC。该章介绍消息摘要、数字签名等关键术语，还介绍如何把对称密钥加密与非对称密钥加密结合起来。介绍 ElGamal 加密和 ElGamal 数字签名，介绍 SHA-3 算法，以及 RSA 数字签名的有关问题。

第 5 章介绍当前流行的公钥基础设施（PKI），介绍什么是数字证书，如何生成、发布、维护与使用数字证书，介绍证书机构（CA）与注册机构（RA）的作用，并介绍公钥加密标准（PKCS）。删除一些过时内容，如漫游数字证书、属性证书等。

第 6 章介绍 Internet 中的重要安全协议，包括 SSL、SHTTP、TSP、SET 与 3D 安全。该章详细介绍电子邮件安全性，介绍 PGP、PEM 与 S/MIME 等主要电子邮件安全协议，并介绍无线安全性。减少对较旧内容 SET 协议的介绍，扩展介绍 3D 安全，删除电子货币介绍，介绍域密钥身份识别邮件（Domain Keys Identified Mail，DKIM），详细介绍 IEEE 802.11（Wi-Fi）的安全。

第 7 章介绍如何认证用户，可以使用多种方法认证用户。该章详细介绍每种方法及其利弊，介绍基于口令认证、基于口令派生信息的认证、认证令牌、基于证书认证和生物认证，并介绍著名的 Kerberos 协议。扩展介绍生物技术，介绍对各种认证方案的攻击。

第 8 章介绍加密的实际问题。目前，实现加密的 3 种主要方法是：使用 Sun 公司提供的加密机制（在 Java 语言中）、Microsoft 加密机制和第三方工具箱的加密机制，我们将介绍每种方法。删除对操作系统安全和数据库安全的介绍，增加对 Web 服务安全和云安全的介绍。

第 9 章介绍网络层安全，介绍防火墙及其类型与配置，然后介绍 IP 安全性，最后介绍虚拟专用网（VPN）。

每章前面都有一个概述，解释该章的内容，每章后面还有一个小结。每章有多选题和各种问题，用于了解学生的掌握情况。在恰当的地方给出一些案例研究，为相关内容给出一个真实实践。每个不易理解的概念都用图形加以阐述。本书尽可能避免使用不必要的数学知识。

在线学习中心

本书在线学习中心（Online Learning Center，OLC）为 https://www.mhhe.com/kahate/cns3。

对学生，内容包括：

- 不同难度级别的编程题。
- DES 与 AES 的加密演示小程序。
- Web 资源（最新更新的链接）。

- 真实的案例研究。

对教师，内容包括：

- 练习题答案。
- 本书附加材料列表。
- Web 参考(一些有趣的链接)。

致谢

感谢我所有家人、同事和朋友对我的帮助。本书的前面版本对几百位学生和老师表示了感谢，这使得我能非常愉快地开始新版本的编写工作。这里要特别感谢我之前的学生 Swapnil Panditrao 和 Pranav Sorte 对第 3 版的帮助。Nikhil Bhalla 先生指出了本书之前版本中的不少错误。

衷心感谢 TMH 出版社的所有成员：Shalini Jha、Smruti Snigdha、Sourabh Maheshwari、Satinder Singh、Sohini Mukherjee 和 P L Pandita，他们在本书出版过程中的各个环节给予了帮助。

还要感谢本书的所有评阅者，他们抽出时间来评阅本书，并给出了非常有用的建议。这些评阅者如下：

Vrutika Shah　Institute of Technology and Engineering, Ahmedabad, Gujarat

Metul Patel　Shree Swami Atmanandan College of Engineering, Ahmedabad, Gujarat

Amitab Nag　Academy of Technology, Kolkata

Subhajit Chatterjee　Calcutta Institute of Engineering and Management, Kolkata

Garimella Rama　Murthy International Institute of Information Technology (IIIT), Hyderabad

反馈

欢迎读者在我的网址 www. atulkahate. com 上给我留下反馈或评价，也可以发电子邮件到 akahate@gmail. com。

Atul Kahate

目录

第 1 章　计算机攻击与计算机安全 …… 1

1.1　概述 …… 1
1.2　安全需求 …… 1
1.2.1　基本概念 …… 1
1.2.2　攻击的现代性 …… 2
1.3　安全方法 …… 4
1.3.1　可信系统 …… 4
1.3.2　安全模型 …… 4
1.3.3　安全管理实务 …… 5
1.4　安全性原则 …… 5
1.4.1　保密性 …… 6
1.4.2　认证 …… 6
1.4.3　完整性 …… 6
1.4.4　不可抵赖性 …… 7
1.4.5　访问控制 …… 7
1.4.6　可用性 …… 8
1.5　攻击类型 …… 8
1.5.1　一般意义上的攻击 …… 8
1.5.2　技术角度的攻击概念 …… 10
1.5.3　实际的攻击 …… 12
1.5.4　攻击程序 …… 12
1.5.5　对付病毒 …… 14
1.5.6　特定攻击 …… 16
1.6　本章小结 …… 20
1.7　实践练习 …… 20
1.7.1　多项选择题 …… 20
1.7.2　练习题 …… 21
1.7.3　设计与编程 …… 22

第2章 密码技术 …… 23

2.1 概述 …… 23
2.2 明文与密文 …… 24
2.3 替换加密技术 …… 26
2.3.1 凯撒加密法 …… 26
2.3.2 凯撒加密法的改进版本 …… 27
2.3.3 单码加密法 …… 29
2.3.4 同音替换加密法 …… 29
2.3.5 块替换加密法 …… 29
2.3.6 多码替换加密法 …… 30
2.3.7 Playfair 加密法 …… 30
2.3.8 希尔加密法 …… 35
2.4 变换加密技术 …… 37
2.4.1 栅栏加密技术 …… 37
2.4.2 简单分栏式变换加密技术 …… 37
2.4.3 Vernam 加密法 …… 39
2.4.4 书加密法/运动密钥加密法 …… 40
2.5 加密与解密 …… 40
2.6 对称与非对称密钥加密 …… 42
2.6.1 对称密钥加密与密钥发布问题 …… 42
2.6.2 Diffie-Hellman 密钥交换协议/算法 …… 44
2.6.3 非对称密钥操作 …… 49
2.7 夹带加密法 …… 51
2.8 密钥范围与密钥长度 …… 51
2.9 攻击类型 …… 54
2.10 案例研究：拒绝服务攻击 …… 57
2.11 本章小结 …… 59
2.12 实践练习 …… 60
2.12.1 多项选择题 …… 60
2.12.2 练习题 …… 61
2.12.3 设计与编程 …… 61

第3章 对称密钥算法与 AES …… 63

3.1 概述 …… 63
3.2 算法类型与模式 …… 63
3.2.1 算法类型 …… 63
3.2.2 算法模式 …… 66
3.3 对称密钥加密法概述 …… 72

3.4 数据加密标准 …… 73
3.4.1 背景与历史 …… 73
3.4.2 DES 的工作原理 …… 73
3.4.3 DES 的变体 …… 81
3.5 国际数据加密算法 …… 84
3.5.1 背景与历史 …… 84
3.5.2 IDEA 的工作原理 …… 85
3.6 RC4 …… 89
3.6.1 背景与历史 …… 89
3.6.2 算法描述 …… 90
3.7 RC5 …… 92
3.7.1 背景与历史 …… 92
3.7.2 RC5 工作原理基本原理 …… 92
3.7.3 RC5 的模式 …… 97
3.8 Blowfish …… 98
3.8.1 简介 …… 98
3.8.2 操作 …… 98
3.9 高级加密标准 …… 101
3.9.1 简介 …… 101
3.9.2 操作 …… 102
3.9.3 一次性初始化处理 …… 103
3.9.4 每轮的处理 …… 107
3.10 案例研究：安全的多方计算 …… 110
3.11 本章小结 …… 111
3.12 实践练习 …… 112
3.12.1 多项选择题 …… 112
3.12.2 练习题 …… 113
3.12.3 设计与编程 …… 114

第 4 章 基于计算机的非对称密钥算法 …… 115

4.1 概述 …… 115
4.2 非对称密钥加密简史 …… 115
4.3 非对称密钥加密概述 …… 116
4.4 RSA 算法 …… 118
4.4.1 简介 …… 118
4.4.2 RSA 示例 …… 118
4.4.3 了解 RSA 的关键 …… 120
4.4.4 RSA 的安全性 …… 120
4.5 ElGamal 加密 …… 122

4.5.1 ElGamal密钥生成 …… 122
4.5.2 ElGamal密钥加密 …… 122
4.5.3 ElGamal密钥解密 …… 122
4.6 对称与非对称密钥加密 …… 123
4.6.1 对称与非对称密钥加密比较 …… 123
4.6.2 两全其美 …… 123
4.7 数字签名 …… 126
4.7.1 简介 …… 126
4.7.2 消息摘要 …… 128
4.7.3 MD5 …… 131
4.7.4 安全散列算法 …… 138
4.7.5 SHA-512 …… 141
4.7.6 SHA-3 …… 143
4.7.7 消息认证码 …… 143
4.7.8 HMAC …… 144
4.7.9 数字签名技术 …… 148
4.8 背包算法 …… 151
4.9 ElGamal数字签名 …… 151
4.9.1 签名过程 …… 152
4.9.2 验证过程 …… 152
4.10 对数字签名的攻击 …… 152
4.11 公钥交换的问题 …… 153
案例研究1：虚拟选举 …… 154
案例研究2：合同签署 …… 155
4.12 本章小结 …… 156
4.13 实践练习 …… 157
4.13.1 多项选择题 …… 157
4.13.2 练习题 …… 158
4.13.3 设计与编程 …… 158

第5章 公钥基础设施 …… 160

5.1 概述 …… 160
5.2 数字证书 …… 160
5.2.1 简介 …… 160
5.2.2 数字证书的概念 …… 161
5.2.3 证书机构 …… 162
5.2.4 数字证书技术细节 …… 162
5.2.5 生成数字证书 …… 164
5.2.6 为何信任数字证书 …… 169

5.2.7 证书层次与自签名数字证书 …… 172
5.2.8 交叉证书 …… 175
5.2.9 证书吊销 …… 175
5.2.10 证书类型 …… 182
5.3 私钥管理 …… 183
5.3.1 保护私钥 …… 183
5.3.2 多个密钥对 …… 183
5.3.3 密钥更新 …… 184
5.3.4 密钥存档 …… 184
5.4 PKIX 模型 …… 184
5.4.1 PKIX 服务 …… 184
5.4.2 PKIX 体系结构模型 …… 185
5.5 公钥加密标准 …… 186
5.5.1 简介 …… 186
5.5.2 PKCS#5：基于口令加密标准 …… 187
5.5.3 PKCS#8：私钥信息语法标准 …… 188
5.5.4 PKCS#10：证书请求语法标准 …… 189
5.5.5 PKCS#11：加密令牌接口标准 …… 189
5.5.6 PKCS#12：个人信息交换语法 …… 189
5.5.7 PKCS#14：伪随机数生成标准 …… 189
5.5.8 PKCS#15：加密令牌信息语法标准 …… 191
5.6 XML、PKI 与安全 …… 191
5.6.1 XML 加密 …… 191
5.6.2 XML 数字签名 …… 193
5.6.3 XML 密钥管理规范 …… 194
5.7 用 Java 创建数字签名 …… 195
案例研究：交叉网站脚本攻击 …… 200
5.8 本章小结 …… 202
5.9 实践练习 …… 203
5.9.1 多项选择题 …… 203
5.9.2 练习题 …… 204
5.9.3 设计与编程 …… 204

第 6 章 Internet 安全协议 …… 206

6.1 概述 …… 206
6.2 基本概念 …… 206
6.2.1 静态 Web 页面 …… 206
6.2.2 动态 Web 页面 …… 208
6.2.3 活动 Web 页面 …… 208

6.2.4 协议与 TCP/IP …… 209
6.2.5 分层组织 …… 211
6.3 安全套接层 …… 212
6.3.1 简介 …… 212
6.3.2 SSL 在 TCP/IP 协议中的位置 …… 212
6.3.3 SSL 工作原理 …… 212
6.3.4 关闭与恢复 SSL 连接 …… 219
6.3.5 SSL 的缓冲区溢出攻击 …… 220
6.4 传输层安全 …… 220
6.5 安全超文本传输协议 …… 221
6.6 安全电子事务规范 …… 221
6.6.1 简介 …… 221
6.6.2 SET 参与者 …… 222
6.6.3 SET 过程 …… 222
6.6.4 SET 如何达到目的 …… 224
6.6.5 SET 技术内幕 …… 224
6.6.6 SET 结论 …… 229
6.6.7 SET 模型 …… 230
6.7 SSL 与 SET …… 231
6.8 3D 安全协议 …… 231
6.8.1 概述 …… 232
6.8.2 幕后情形 …… 233
6.9 电子邮件安全性 …… 234
6.9.1 简介 …… 234
6.9.2 隐私增强型邮件协议 …… 236
6.9.3 PGP …… 239
6.9.4 安全多用途 Internet 邮件扩展 …… 246
6.9.5 域密钥身份识别邮件 …… 250
6.10 无线应用程序协议安全性 …… 251
6.10.1 简介 …… 251
6.10.2 WAP 堆栈 …… 251
6.10.3 安全层：无线传输层安全 …… 252
6.11 GSM 安全性 …… 253
6.12 3G 安全性 …… 255
6.13 IEEE 802.11 安全性 …… 257
6.13.1 有线等效保密协议 …… 257
6.13.2 IEEE 802.11 认证 …… 257
6.13.3 Wi-Fi 受保护接入 …… 259
6.14 链路安全与网络安全 …… 260

案例研究 1：内部分支支付交易的安全防护 …… 261
案例研究 2：Cookie 与隐私保护 …… 264
6.15 本章小结 …… 265
6.16 实践练习 …… 267
6.16.1 多项选择题 …… 267
6.16.2 练习题 …… 268
6.16.3 设计与编程 …… 268

第 7 章 用户认证机制 …… 270

7.1 概述 …… 270
7.2 认证基础 …… 270
7.3 口令 …… 271
7.3.1 简介 …… 271
7.3.2 明文口令 …… 271
7.3.3 口令推导形式 …… 273
7.3.4 安全问题 …… 279
7.4 认证令牌 …… 280
7.4.1 简介 …… 280
7.4.2 认证令牌类型 …… 282
7.5 基于证书认证 …… 287
7.5.1 简介 …… 287
7.5.2 基于证书认证工作原理 …… 287
7.5.3 使用智能卡 …… 289
7.6 生物认证 …… 291
7.6.1 简介 …… 291
7.6.2 生物认证的工作原理 …… 291
7.7 Kerberos …… 292
7.7.1 简介 …… 292
7.7.2 Kerberos 工作原理 …… 292
7.7.3 Kerberos 版本 5 …… 295
7.8 密钥分发中心 …… 296
7.9 安全握手的陷阱 …… 297
7.9.1 单向认证 …… 297
7.9.2 双向认证 …… 301
7.10 单次登录方法 …… 304
7.10.1 脚本 …… 304
7.10.2 代理 …… 305
7.11 对认证机制的攻击 …… 305
7.12 案例研究：单次登录 …… 306

7.13 本章小结 …… 308
7.14 实践练习 …… 309
7.14.1 多项选择题 …… 309
7.14.2 练习题 …… 310
7.14.3 设计与编程 …… 311

第8章 加密与安全实现 …… 312

8.1 概述 …… 312
8.2 Java加密方案 …… 312
8.2.1 简介 …… 312
8.2.2 Java加密体系结构 …… 313
8.2.3 Java加密扩展 …… 316
8.2.4 结论 …… 317
8.3 使用Microsoft .NET的加密方案 …… 319
8.3.1 类模型 …… 319
8.3.2 程序员的角度 …… 320
8.4 加密工具库 …… 321
8.5 Web服务安全 …… 321
8.6 云安全 …… 323
8.7 本章小结 …… 324
8.8 实践练习 …… 325
8.8.1 多项选择题 …… 325
8.8.2 练习题 …… 326
8.8.3 设计与编程 …… 326

第9章 网络安全、防火墙与VPN …… 328

9.1 概述 …… 328
9.2 TCP/IP简介 …… 328
9.2.1 基本概念 …… 328
9.2.2 TCP数据段格式 …… 329
9.2.3 IP数据报文格式 …… 331
9.3 防火墙 …… 332
9.3.1 简介 …… 332
9.3.2 防火墙的类型 …… 334
9.3.3 防火墙配置 …… 342
9.3.4 非军事区网络 …… 344
9.3.5 防火墙的局限性 …… 344
9.4 IP安全性 …… 345
9.4.1 简介 …… 345

9.4.2 IPSec 概述 …… 346
9.4.3 认证头 …… 351
9.4.4 封装安全荷载 …… 353
9.4.5 IPSec 密钥管理 …… 356
9.5 虚拟专用网 …… 358
9.5.1 简介 …… 358
9.5.2 虚拟专用网的体系结构 …… 359
9.6 入侵 …… 360
9.6.1 入侵者 …… 360
9.6.2 审计记录 …… 361
9.6.3 入侵检测 …… 362
9.6.4 分布式入侵检测 …… 363
9.6.5 Honeypot 技术 …… 363
案例研究 1：IP 欺骗攻击 …… 363
案例研究 2：创建 VPN …… 364
9.7 本章小结 …… 365
9.8 实践练习 …… 367
9.8.1 多项选择题 …… 367
9.8.2 练习题 …… 368
9.8.3 设计与编程 …… 368

附录 A 数学背景知识 …… 370

A.1 概述 …… 370
A.2 素数 …… 370
A.2.1 因子分解 …… 370
A.2.2 欧几里得算法 …… 371
A.2.3 求模运算与离散对数 …… 372
A.2.4 测试素数 …… 372
A.2.5 素数的平方根模 …… 372
A.2.6 平方余数 …… 372
A.3 费尔马定理与欧拉定理 …… 373
A.3.1 费尔马定理 …… 373
A.3.2 欧拉定理 …… 374
A.4 中国剩余定理 …… 374
A.5 拉格朗日符号 …… 375
A.6 雅可比符号 …… 375
A.7 哈塞定理 …… 375
A.8 平方互换定理 …… 376
A.9 Massey-Omura 协议 …… 376