

● 权威作者 ● 经典教材

网络安全

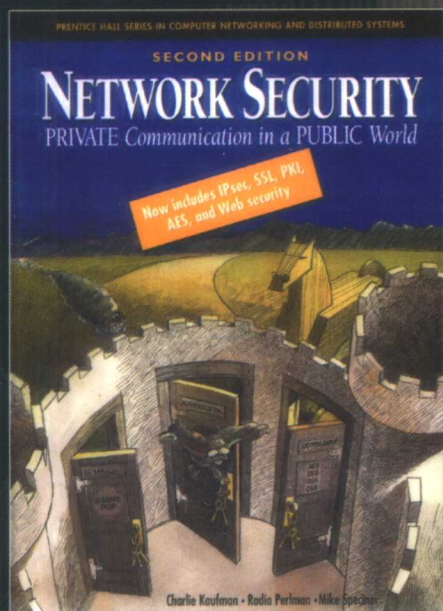
—— 公众世界中的秘密通信

(第二版)

Network Security

Private Communication in a Public World

Second Edition



Charlie Kaufman

[美] Radia Perlman 著

Mike Speciner

许剑卓 左英男 等译

戴英侠 审校



电子工业出版社

Publishing House of Electronics Industry
<http://www.phei.com.cn>

国外计算机科学教材系列

网 络 安 全

——公众世界中的秘密通信

(第二版)

Network Security: Private Communication in a Public World

Second Edition

Charlie Kaufman

[美] Radia Perlman 著

Mike Speciner

许剑卓 左英男 等译

戴英侠 审校

电子工业出版社

Publishing House of Electronics Industry

北京 · BEIJING

内 容 简 介

本书全面阐述了信息安全理论,全书共分五个部分,即密码学、认证、标准、电子邮件以及其他安全机制。其中,第一部分阐述了密码算法的基本原理以及各种经典的和现代的加密算法。第二部分介绍了如何在网络中证明身份、人在向设备证明自己的身份时可能碰到的问题、认证握手协议的细节以及协议可能存在的多种缺陷。第三部分讲述了一系列安全协议(如 Kerberos, IPSec 和 SSL 等)以及 PKI 的一些标准。第四部分讲述了电子邮件安全中的若干问题,列出了与电子邮件相关的几个安全特性,并描述了这些安全特性的具体实现方式。第五部分介绍了防火墙、各种操作系统的安全性问题、浏览网站时所涉及的协议以及对安全实践经验的总结。本书提供了章后习题,书后还给出了大量参考文献。

本书从日常应用入手,以简单易懂的方式阐述了深奥的理论,加之原作者文笔生动幽默,堪称风格独特。本书可作为相关专业高年级本科生和研究生的教学用书以及相关领域专业人员的参考用书。

Authorized translation from the English language edition, entitled *Network Security: Private Communication in Public World*, Second Edition, ISBN: 0130460192 by Charlie Kaufman, Radia Perlman, Mike Speciner, published by Pearson Education, Inc., publishing as Prentice Hall PTR, Copyright © 2002.

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 Pearson Education, Inc.

Simplified Chinese language edition published by Publishing House of Electronics Industry, Copyright © 2004.

This edition is authorized for sale only in the People's Republic of China excluding Hong Kong, Macau and Taiwan.

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 PTR 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。

此版本仅限在中华人民共和国境内(不包括香港、澳门特别行政区以及台湾地区)发行与销售。

版权贸易合同登记号 图字: 01-2003-0593

图书在版编目(CIP)数据

网络安全: 公众世界中的秘密通信(第二版)/(美)考夫曼(Kaufman, C.)等著;许剑卓等译.

-北京:电子工业出版社,2004.9

(国外计算机科学教材系列)

书名原文: *Network Security: Private Communication in a Public World*, Second Edition

ISBN 7-5053-9945-4

I. 网… II. ①考… ②许… III. 计算机网络-安全技术-教材 IV. TP393.08

中国版本图书馆CIP数据核字(2004)第089447号

责任编辑:刘 静

印 刷:北京兴华印刷厂

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

经 销:各地新华书店

开 本:787×1092 1/16 印张:30 字数:845千字

印 次:2004年9月第1次印刷

定 价:45.00元

凡购买电子工业出版社的图书,如有缺损问题,请向购买书店调换;若书店售缺,请与本社发行部联系。

联系电话:(010)68279077。质量投诉请发邮件至 zltz@phei.com.cn, 盗版侵权举报请发邮件至 dbqq@phei.com.cn。

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关键时期,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 and 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

- | | | |
|----|-----|---|
| 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 | 上海国际数据库研究中心主任、复旦大学教授
中国计算机学会常务理事、上海市计算机学会理事长 |
| | 邹 鹏 | 国防科学技术大学计算机学院教授、博士生导师
教育部计算机基础课程教学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

对信息安全的认识是从所需的安全属性开始的,安全属性包括信息的保密性、完整性、可用性以及不可否认性。人们最早意识到的信息安全属性是保密性,即信息仅为授权者所享有,不被泄露给非授权的用户、实体或过程。电报、电话的发明和应用,特别是如今网络通信的普及,使人们获得了远距离交流消息的各种手段。因此,远程通信安全的重要性显得特别突出。密码技术成为安全保密的重要支撑技术,因为报文加密使得第三方难以窃听到所传输消息的真正意义。当然,除了信息的保密性问题以外,还存在完整性(即信息未经授权不能进行更改的特性)问题。此外,当对信息进行存储、处理和传输时,要求整个系统能正常运行。但是,由于种种原因(如发生了拒绝服务攻击、非法滥用资源、计算机病毒侵害、由不熟练导致的误操作、自然灾害等情况),通信系统可能会失去或部分地失去工作能力。这就是可用性(即信息及信息系统可被授权实体访问并按需求使用的安全特性)的安全需求。例如,在授权用户或实体需要信息服务时,信息服务应该可以使用,或者在信息系统部分受损或需要降级使用时,仍能为授权用户或实体提供有效服务。最后,我们还必须提到不可否认性(又称抗抵赖性,即人们不能否认自己的信息行为)的问题。不可否认性分为源发不可否认和接收不可否认,前者用于防止发送者否认自己已发送的数据和数据内容,后者用于防止接收者否认已接收到的数据和数据内容。实现不可否认性的手段与技术有很多,最常用的是数字证书和数字签名。

本书围绕上述各种问题,全面地阐述了安全性。全书共分为五个部分:密码学(第2章至第8章)、认证(第9章至第12章)、标准(第13章至第19章)、电子邮件(第20章至第22章)以及其他安全机制(第23章至第26章)。第一部分深入浅出地阐述了密码算法的基本原理以及经典的和现代的各种加密算法。其中,第2章是必读的,因为这一章的内容对于理解本书的其他内容至关重要。第7章和第8章讲述了密码学背后更深层次的数学原理,这两章对于理解本书的其他内容并无影响,所以读者可以放在最后阅读。第二部分介绍了如何在网络中证明身份、人在向设备证明自己身份时可能碰到的问题、认证握手协议的细节以及协议可能存在的多种缺陷。第三部分讲述了一系列安全协议(如Kerberos, IPSec和SSL等),以及PKI的一些标准。第四部分主要讲述了电子邮件安全中的若干问题,列出了与电子邮件相关的几个安全特性,并描述了这几个安全特性的具体实现方式。最后一部分介绍了防火墙、各种操作系统的安全性问题、浏览网站时所涉及的协议以及对安全实践经验的总结。

本书原作者对密码算法和安全协议等有深入的研究,在很多方面都有独到见解,文笔生动、幽默。他用形象的语言讲述了自己的学术观点,引人入胜。同时,作者对安全的误区和一些错误的观点也给出了一针见血的评述。

本书适合作为高年级本科生或研究生的教材,也可以作为相关领域专业人员的参考书。

本书的第1章到第14章由许剑卓翻译,第15章到第26章由左英男翻译,全书的整理由戴英侠负责。此外,黄英达、左晓栋、代亮、魏军、杨东晓、鲍旭华、李闻和冯萍慧等也参与了翻译工作。

由于译者水平有限,书中难免存在疏漏和不当之处,恳请广大读者和专家批评指正。

致 谢

虽然围绕网络安全问题有着大量的争论,但我们仍感觉到网络安全领域的人士很乐于分享智慧和时间。在向提供帮助的人表示感谢时,我们总是担心可能会漏掉其中的某些人,但是不对任何人表示感谢显然也是不妥的。

Eric Rescorla和Hilarie Orman对本书进行了仔细的审阅并回答了我们提出的很多问题。其他对本书进行审阅并提供帮助的人有:Tom Wu, Kevin Fu, Marshall Ross, Joe Tardo, Joe Pato, Seth Proctor, Timothy Spiller, Tom Rice, Kristen McIntyre, Gary Winiger, Dan Harkins, Peter Memishian, Jeff Schiller, Burt Kaliski, Tony Lauck, Phil Karn, Ron Rivest, Steve Crocker, Steve Kent, John Linn, Steve Hanna, Jim Bidzos, Dave Jablon, Ted Ts'o, Matthew Barnes, Keith McCloughrie, Jeffrey Case, Kathrin Winkler, Philippe Auphelle, Sig Handelman, Phillip Hallam-Baker, Uri Blumenthal, Serge Vaudenay, Boyd Roberts。

如果没有下述几家公司的帮助,我们就无法完成第24章,因为该章涉及的多数是非公开的内容。在此要感谢Iris (Lotus Notes)的Al Eldridge、IBM (KryptoKnight)的Amir Herzberg和Mark Davis、OSF的Walt Tuvell以及微软(LAN Manager和Windows NT安全)的Cliff Van Dyke,他们向我们讲解了各自的系统并及时审阅了我们撰写的内容。虽然我们之中有67%的人所服务的公司生产这一领域的产品,但是本书提供的观点是我们自己的观点,而不是公司的观点。

Prentice Hall的总编Mary Franz在本书的成书过程中一直非常热心地为我们提供帮助。她知道我们在什么时候需要帮忙,也知道什么时候不需要理会我们。她知道有时需要不断地唠叨催促我们,也知道有时只需要深情地望着我们,就足以使我们知道没有及时交稿是多么内疚的事。

虽然这本书让我们的人生中很大一部分时间都变得非常繁忙,但是Ray Perlner让我们对这一创作过程充满了热情。他对本书的创作怀着真切的关心,在我们之间有争论时他提出了非常有用的建议,他帮助我们查找参考文献并审校了本书的部分章节,他还特别喜欢纠正我们用错的代词,其实有时我们故意用错一些代词只是希望能够听到他咯咯的傻笑。Dawn Perlner在本书的编写过程中也提供了大量的帮助,并试图说服很多人(甚至是陌生人)购买本书。

当然还要感谢你,我们的读者。我们欢迎你提出宝贵的建议和批评,当然也非常欢迎你的赞美。我们希望能够定期更新本书的内容,如果你希望我们在本书的新版本中讨论什么题目或者改正哪些错误,都请你告诉我们。通过网站<http://www.phptr.com/networksecurity>可以与Errata取得联系。

我们现在使用的电子邮件地址是ckaufman@us.ibm.com, radia@alum.mit.edu和ms@alum.mit.edu,但我们发现电子邮件不总是可靠的,并且地址也总是改变。如果无法与我们之中的任何一个人取得联系,你可以和出版商Prentice Hall联系,特别是可以和我们的编辑Mary Franz (mfranz@prenhall.com)联系以获得我们最新的电子邮件地址。

目 录

第1章 简介	1
1.1 本书内容	2
1.2 本书所属类型	2
1.3 术语	3
1.4 符号	4
1.5 网络基础知识	4
1.6 积极攻击和被动攻击	9
1.7 分层和密码学	9
1.8 授权	10
1.9 风暴	10
1.10 为执法部门实施密钥托管	11
1.11 为粗心的用户实施密钥托管	12
1.12 病毒、蠕虫和特洛伊木马	12
1.13 安全的多层模型	17
1.14 法律问题	22

第一部分 密码学

第2章 密码学简介	26
2.1 什么是密码学	26
2.2 破解密码算法	28
2.3 密码算法函数	29
2.4 秘密密钥算法	29
2.5 公开密钥算法	31
2.6 哈希算法	34
2.7 习题	36
第3章 秘密密钥算法	37
3.1 简介	37
3.2 分组密码算法	37
3.3 数据加密标准	39
3.4 IDEA 算法	48
3.5 AES 算法	52

3.6	RC4 算法	59
3.7	习题	59
第 4 章	运算模式	61
4.1	简介	61
4.2	加密长消息	61
4.3	生成 MAC	67
4.4	使用 DES 算法实施多次加密	70
4.5	习题	74
第 5 章	哈希和消息摘要	75
5.1	简介	75
5.2	哈希算法的一些有趣的应用	78
5.3	MD2	82
5.4	MD4	85
5.5	MD5	88
5.6	SHA-1	90
5.7	HMAC	91
5.8	习题	92
第 6 章	公钥算法	95
6.1	简介	95
6.2	模运算	95
6.3	RSA	98
6.4	Diffie-Hellman	107
6.5	数字签名标准	111
6.6	RSA 和 Diffie-Hellman 的安全性	114
6.7	椭圆曲线算法	114
6.8	零知识证明系统	115
6.9	习题	118
第 7 章	数论	119
7.1	简介	119
7.2	模运算	119
7.3	素数	119
7.4	欧几里得算法	120
7.5	中国余数定理	122
7.6	$\mathbb{Z}_n^*$	123
7.7	欧拉的 totient 函数	124
7.8	欧拉定理	125
7.9	习题	125

第 8 章	AES 和椭圆曲线的数学基础	127
8.1	简介	127
8.2	符号	127
8.3	群	128
8.4	域	129
8.5	Rijndael 算法的数学基础	133
8.6	椭圆曲线算法	134
8.7	习题	135

第二部分 认证

第 9 章	认证系统概述	138
9.1	基于口令的认证	138
9.2	基于地址的认证	140
9.3	密码认证协议	143
9.4	正在接受认证的人是谁	143
9.5	使用口令作为密钥	143
9.6	窃听及数据库读取	144
9.7	可信的第三方	145
9.8	会话密钥协商	149
9.9	代理	150
9.10	习题	151
第 10 章	认证人的身份	152
10.1	口令	152
10.2	在线口令猜解	153
10.3	离线口令猜解	154
10.4	应该使用多大数量的秘密	156
10.5	侦听	156
10.6	口令及粗心的用户	157
10.7	分发初始口令	159
10.8	认证令牌	160
10.9	物理接触	161
10.10	生物特征	161
10.11	习题	162
第 11 章	安全握手协议的缺陷	163
11.1	只进行登录	163
11.2	双向认证	167
11.3	加密数据和保护数据完整性	170

11.4	受干预的认证	173
11.5	Nonce 类型	178
11.6	选择随机数	179
11.7	性能	180
11.8	认证协议核对表	181
11.9	习题	182
第 12 章	强口令协议	185
12.1	简介	185
12.2	Lamport 哈希	185
12.3	强口令协议	187
12.4	强口令证明书下载协议	191
12.5	习题	192

第三部分 标准

第 13 章	Kerberos V4	196
13.1	简介	196
13.2	门票和门票分发门票	196
13.3	配置	197
13.4	登录网络	198
13.5	备份 KDC	200
13.6	域	201
13.7	域间认证	202
13.8	密钥版本号	203
13.9	加密以保证保密性和完整性	203
13.10	通过加密只保护完整性	204
13.11	门票中的网络层地址	205
13.12	消息格式	206
13.13	习题	215
第 14 章	Kerberos V5	216
14.1	ASN.1	216
14.2	名称	217
14.3	权限代理	217
14.4	门票生存时间	219
14.5	密钥版本	220
14.6	在不同的域中使用不同的主密钥	221
14.7	优化	221
14.8	密码算法	221

14.9	域的层次结构	224
14.10	避免离线口令猜解	226
14.11	认证值中的密钥	226
14.12	双 TGT 认证	227
14.13	PKINIT: 用户的公开密钥	227
14.14	KDC 数据库	228
14.15	Kerberos V5 消息	228
14.16	习题	236
第 15 章	公钥基础设施	238
15.1	引言	238
15.2	一些技术	238
15.3	PKI 信任模型	238
15.4	证书撤销	245
15.5	目录服务与 PKI	247
15.6	PKIX 和 X.509	249
15.7	X.509 和 PKIX 证书	251
15.8	授权的前景	254
15.9	习题	257
第 16 章	实时通信安全	258
16.1	协议应当实现在哪一层	258
16.2	会话密钥的建立	260
16.3	完美的前向保密性	260
16.4	PFS 挫败	262
16.5	拒绝服务 / 防阻塞	262
16.6	端点识别符隐藏	264
16.7	通信双方的实时确认	265
16.8	并行计算	266
16.9	会话重用	266
16.10	似是而非的否认	267
16.11	数据流保护	268
16.12	协商密码参数	268
16.13	简单问题	269
16.14	习题	269
第 17 章	IPSec: AH 和 ESP	272
17.1	IPSec 概述	272
17.2	IP 和 IPv6	275
17.3	AH	278

17.4	ESP	280
17.5	我们是否需要 AH	281
17.6	编码方式的比较	282
17.7	问答题	282
17.8	习题	283
第 18 章	IPSec: IKE	284
18.1	Photuris	284
18.2	SKIP	285
18.3	IKE 的历史	286
18.4	IKE 的阶段	286
18.5	IKE 的阶段 1	287
18.6	IKE 的阶段 2	299
18.7	ISAKMP/IKE 编码	300
18.8	习题	308
第 19 章	SSL/TLS	309
19.1	引言	309
19.2	使用 TCP	309
19.3	SSL 协议的历史	309
19.4	SSL/TLS 基本协议	309
19.5	会话重用	311
19.6	密钥的计算	312
19.7	客户认证	312
19.8	SSL 中使用的 PKI	312
19.9	版本号	313
19.10	协商密码套件	314
19.11	协商压缩方法	315
19.12	SSLv3 弥补的安全漏洞	315
19.13	可出口性	315
19.14	编码	318
19.15	推荐读物	323
19.16	问答题	323
19.17	习题	323

第四部分 电子邮件

第 20 章	电子邮件安全	326
20.1	分发列表	326
20.2	存储和转发	328

20.3	电子邮件的安全服务	328
20.4	建立密钥	329
20.5	私有性	330
20.6	源认证	332
20.7	消息完整性	333
20.8	非否认	334
20.9	邮件提交证据	336
20.10	邮件投递证据	336
20.11	消息流的机密性	336
20.12	匿名性	337
20.13	防泄漏	338
20.14	令人烦恼的文本格式问题	338
20.15	名称和地址	340
20.16	校验消息的真正发送时间	341
20.17	习题	342
第 21 章	PEM 和 S/MIME	344
21.1	引言	344
21.2	PEM 消息的结构	344
21.3	建立密钥	347
21.4	PEM 的历史	348
21.5	PEM 证书分层结构	349
21.6	CRL	350
21.7	为穿越邮件网关而重新格式化数据	351
21.8	PEM 消息的大致结构	351
21.9	加密	352
21.10	源认证和完整性保护	353
21.11	多接收者	353
21.12	明确 PEM 消息的边界	354
21.13	转发和附件	356
21.14	未受保护的信息	357
21.15	消息格式	358
21.16	用 DES-CBC 作为 MIC 是不安全的	364
21.17	S/MIME 与 PEM 的差别	366
21.18	S/MIME 证书的分层结构	368
21.19	习题	369
第 22 章	PGP	371
22.1	引言	371
22.2	概述	372

22.3	密钥分发	372
22.4	有效的编码方式	373
22.5	证书和密钥撤销	374
22.6	签名类型	375
22.7	用户私钥	375
22.8	密钥环	375
22.9	异常情况	376

第五部分 其他安全机制

第 23 章	防火墙	384
23.1	包过滤	386
23.2	应用级网关	387
23.3	加密隧道	388
23.4	比较	389
23.5	为什么防火墙不起作用	389
23.6	拒绝服务攻击	390
23.7	是否应当抛弃防火墙	390
第 24 章	更多的安全系统	391
24.1	NetWare V3	391
24.2	NetWare V4	392
24.3	KryptoKnight	396
24.4	DASS/SPX	398
24.5	Lotus Notes 安全	401
24.6	DCE 安全机制	406
24.7	Microsoft Windows 安全	409
24.8	网络拒绝服务	412
24.9	Clipper	414
24.10	习题	417
第 25 章	Web 安全问题	418
25.1	引言	418
25.2	URL/URI	418
25.3	HTTP	419
25.4	HTTP 摘要认证	420
25.5	cookie	422
25.6	其他 Web 安全问题	425
25.7	习题	428

第 26 章 实践经验	429
26.1 完美的前向保密性	429
26.2 定期改变密钥	429
26.3 多个数据流复用单个 SA	430
26.4 在连接的两个方向上使用不同的密钥	431
26.5 加密和完整性保护分别使用不同的秘密密钥	431
26.6 为不同的目的使用不同的密钥	432
26.7 签名和加密使用不同的密钥	432
26.8 让通信双方对主密钥都有所贡献	433
26.9 不要让一方决定密钥	433
26.10 在对口令做哈希运算时包含一个常量	433
26.11 使用 HMAC 算法而不是简单的 MD 算法	434
26.12 密钥扩展	434
26.13 随机选择 IV	435
26.14 在协议中使用 Nonce	435
26.15 加密数据不应以常量开头	435
26.16 加密数据不应以可预测的值开头	436
26.17 在加密数据之前进行压缩	436
26.18 不应只使用加密保护	436
26.19 避免使用弱密钥	437
26.20 最小设计和冗余设计	437
26.21 高估密钥长度	437
26.22 硬件随机数生成器	437
26.23 时间攻击	438
26.24 把校验和放在数据结尾	438
26.25 前向兼容性	439
26.26 协商参数	441
26.27 习题	441
术语表	443
参考文献	454

第1章 简介

在一个月黑风高的夜晚，远处传来野狗的嚎叫。Alice突然看到一个闪亮的物体，一个钻石链扣！家里只有一个人能够买得起钻石链扣，肯定是管家偷了主人的钻石链扣！Alice必须马上告知Bob，但是她怎么才能通知Bob而不被管家发现呢？如果打电话给Bob，管家可能会在另一个分机上偷听，如果用信鸽并将消息系到它的脚上，Bob又怎么知道是Alice发送的消息呢？他说不定会以为是Trudy故意陷害管家，因为管家拒绝了她的求爱。

这就是本书要讲解的内容。本书恐怕不会过多地描述Alice和Bob的个性，也不会讲述关于管家的事情。但是，我们将讲解如何通过不安全的信道进行安全的通信。

安全的通信是什么意思呢？Alice必须能够发送只有Bob可以看懂的消息给Bob，即使别人能够看到她发送的消息也无所谓。当Bob接收到消息的时候，他必须能够识别出该消息确实是Alice发送的，而且没有人在Alice发送消息与Bob接收到消息之间篡改消息。

不安全的信道是什么意思呢？在一些词典或其他解释中，Internet被描述为“不安全的信道”。整个世界的每台计算机正在逐步走向互联，人们正在谈论如何连接家里的各种家用电器，这将形成一个美妙的全球网络。多么美好啊！你可以通过电子邮件将信息发送给全世界的任何人。你在斐济度假的时候，可以通过网络发送一个简单的命令控制你的核能源工厂。网络世界是可怕的，侦听者可以窃听网络上的很多连接。信息必须经过包交换机转发，重新配置这些交换机就有可能侦听或修改经过的数据包。

这种状况看起来很让人失望，但是可以利用神奇的数学原理来解决这些问题，特别是利用密码学。利用密码学原理，可以将一串数值转换为密文。密文是一组乱码，只有知道秘密的人才能对其做反向转换。密码学让我们能够伪装数据，使得侦听者虽然能够窃听传输的消息，但却无法获取任何有用的信息。密码学还使得我们能够创建一个无法伪造的消息，并且可以监测出该消息在传输过程中是否被篡改。一种实现这一目的的技术叫数字签名，数字签名是与消息相关联的一个数值，其他人可以检验这一数值，以识别消息发送者的身份。只有发送者能够生成该数字签名。这看起来让人惊讶，怎么才能做到让你只能检验某个数值而无法生成该数值呢？一个人的手写签名只能是这个人生成的，但可以被其他人所识别。但是，看起来似乎不难生成某个数值，即使这个数值还必须是能够被检验的。理论上讲，可以尝试大量的数值并检验是否为某个人的签名。这样不就可以生成别人的数字签名了吗？但是，由于使用的数值非常大，用这种方法生成签名可能需要花费大量的时间（比如整个宇宙时间的几倍）。所以，数字签名和手写签名有着相同的特性，也就是只能是某个人生成的。但是数字签名比手写签名具有更多有用的特性，因为数字签名取决于消息的内容，如果有人修改了消息的内容，那么签名也就不再是正确的了，这样就可以发现篡改行为。在学习过第2章之后，读者就会很清楚这一点了。

密码学是本书的主要内容，这不是因为密码学本身非常有趣（当然它确实很有趣），而是因为人们希望计算机网络能够具备的安全特性可以通过密码学来实现。