TURING 图灵计算机科学丛书

PEARSON Prentice Hall

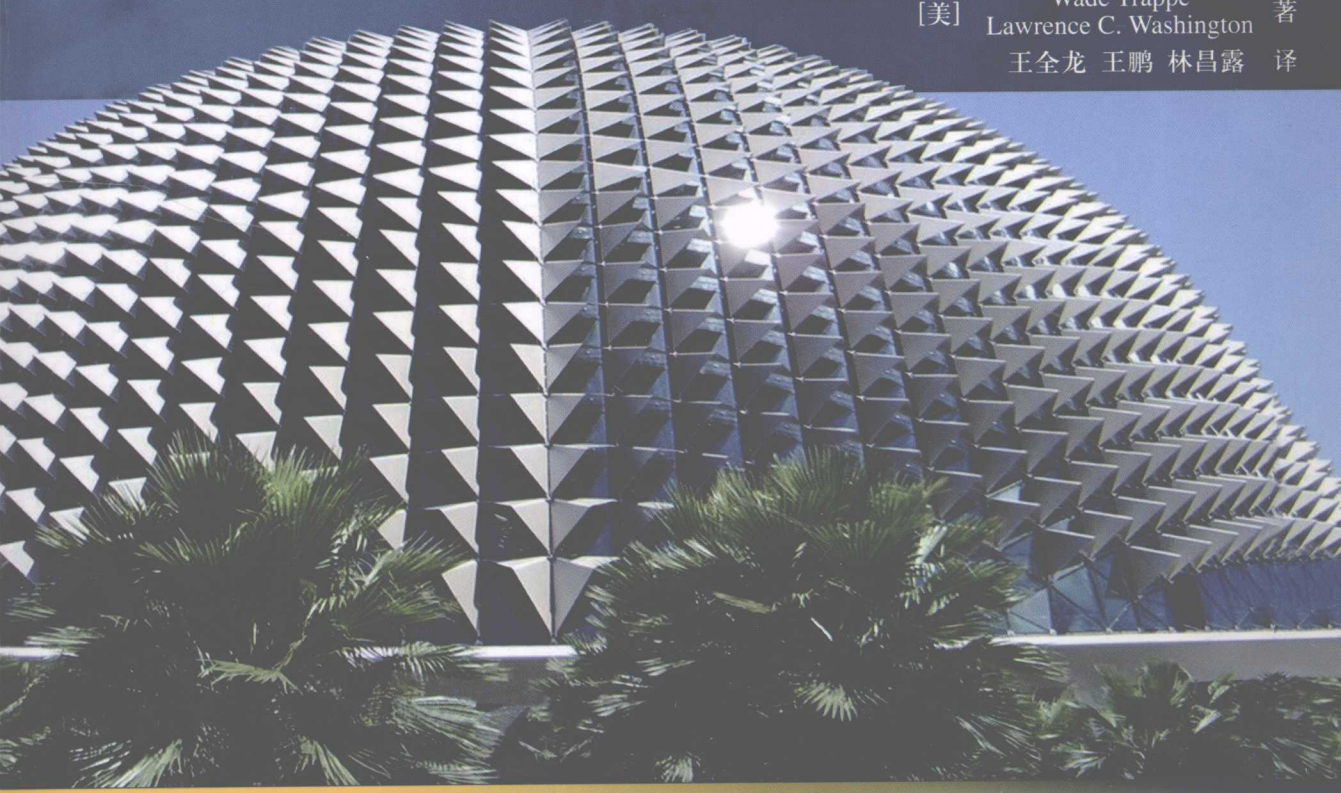
密码学与编码理论

（第2版）

Introduction to Cryptography with Coding Theory

Second Edition

[美] Wade Trappe
Lawrence C. Washington 著
王全龙 王鹏 林昌露 译



人民邮电出版社
POSTS & TELECOM PRESS

TURING 图灵计算机科学丛书

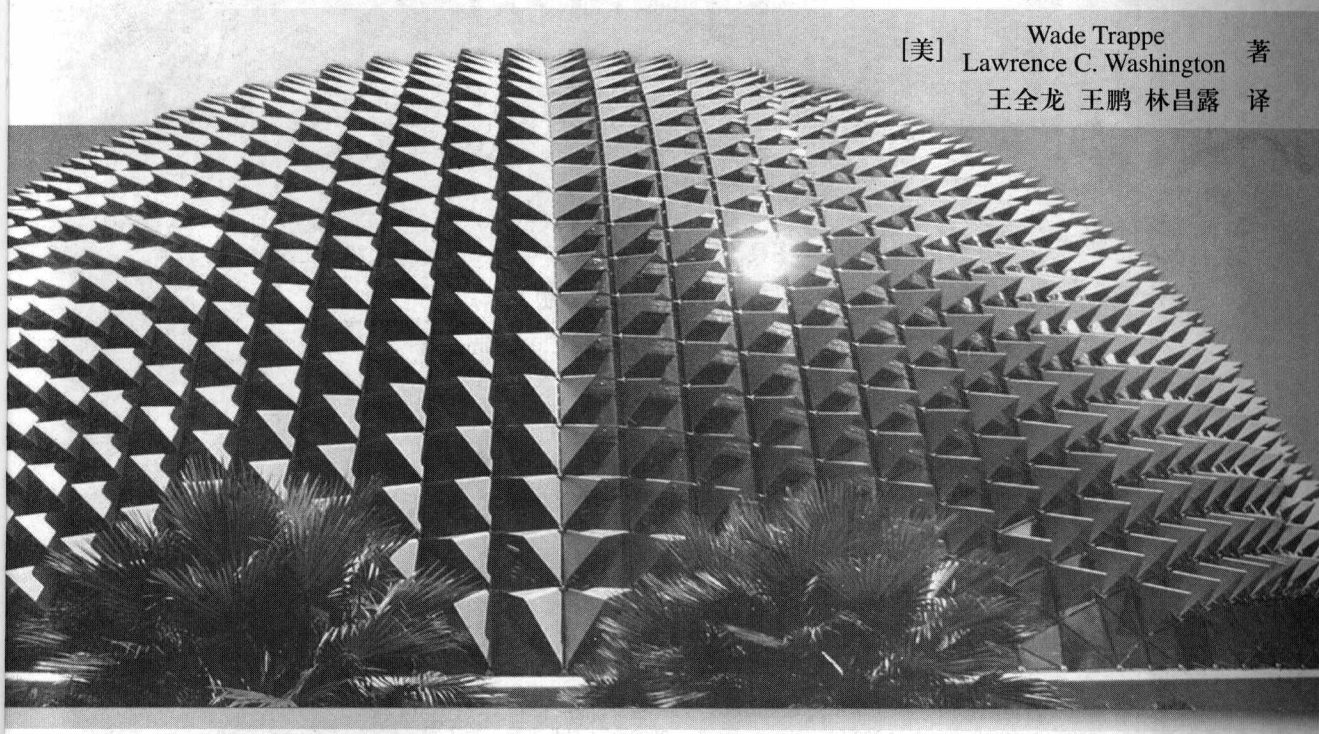
密码学与编码理论

（第2版）

Introduction to Cryptography with Coding Theory

Second Edition

[美] Wade Trappe
Lawrence C. Washington 著
王全龙 王鹏 林昌露 译



人民邮电出版社
北 京

图书在版编目（CIP）数据

密码学与编码理论：第2版 /（美）特拉普（Trappe, W.），（美）华盛顿（Washington, L. C.）著；王全龙，王鹏，林昌露译. —北京：人民邮电出版社，2008.4
（图灵计算机科学丛书）
ISBN 978-7-115-17435-2

Ⅰ. 密… Ⅱ. ①特…②华…③王…④王…⑤林… Ⅲ. ①密码—理论—高等学校—教材 ②编码理论—高等学校—教材 Ⅳ. TN918.1 O157.4

中国版本图书馆CIP数据核字（2007）第204955号

内 容 提 要

本书是密码学方面的经典著作，是作者对其多年教学经验的总结。书中主要内容包括数论、数据加密标准（DES）、高级加密标准Rijndael、RSA算法、离散对数、散列函数、信息论、格方法、纠错码以及量子密码等，其中许多内容都反映了业内的新进展。本书配有大量实例、习题以及用Mathematica®、Maple®、MATLAB®编写的上机练习。

本书可作为高等院校相关专业密码学、通信安全和网络安全等课程的教材或参考书，也可供计算机工程技术人员参考。

图灵计算机科学丛书

密码学与编码理论（第2版）

◆ 著 [美] Wade Trappe Lawrence C. Washington
译 王全龙 王 鹏 林昌露
责任编辑 杨海玲 左艾鑫

◆ 人民邮电出版社出版发行 北京市崇文区夕照寺街14号
邮编 100061 电子函件 315@ptpress.com.cn
网址 http://www.ptpress.com.cn
北京鸿佳印刷厂印刷
新华书店总店北京发行所经销

◆ 开本：787×1092 1/16
印张：20
字数：538千字 2008年4月第1版
印数：1–4 000册 2008年4月北京第1次印刷

著作权合同登记号 图字：01-2006-3664号

ISBN 978-7-115-17435-2/TP

定价：49.00元

读者服务热线：(010)88593802 印装质量热线：(010)67129223
反盗版热线：(010)67171154

版权声明

译 者 序

当今有关密码学的书籍非常多，但如何选择一本适合自己的书似乎又很困难。Wade Trappe和Lawrence C. Washington的这本书却让人在“众里寻他千百度”中为之眼前一亮！这是一本不可多得的好书。本书的作者在其相关研究领域均有很深的造诣，其中Wade Trappe是信息通信领域的专家，Lawrence C. Washington是数学领域的专家，他们在科研和教学上都有着非常丰富的经验，同时还是多部畅销著作的作者（详情可查阅他们的网页）。本书融合了他们各自的专长，可谓是珠联璧合之作。本书具有以下特点。

(1) 深入浅出。对基本概念和原理的阐述细致清晰，既有通俗的表述和背景知识的介绍，又不失数学的严谨，数学证明过程详细易懂。

(2) 内容全面。对从古典的密码系统到现代的密码学算法和协议，以及与此相关的数学内容（如初等数论、椭圆曲线、格方法等）都有充分的介绍。另外，本书还介绍了信息论、纠错码以及较新的量子密码。

(3) 例证丰富。用大量简单的例子详细说明了密码算法和协议的执行过程，这些例子都是可以动手操作的，这对初次学习这些内容的读者非常有帮助。

(4) 习题新颖。习题有两类，一类是理论的练习题，包含对基本概念和原理的练习题目和对正文内容补充的问题；另一类是上机练习，需要利用一些程序设计语言做一些计算。这两类习题可以帮助读者熟悉和进一步理解密码学的内容。

(5) 程序实现。在本书的附录中，提供了Mathematica、Maple以及MATLAB三种流行的数学程序设计语言的简介及其密码学程序源码，读者可以根据需要选择其一进行练习，从实践中体会密码学的原理。

本书可以作为本科高年级或者研究生低年级的密码学教材。由于本书的特点，初学者可以利用本书熟悉密码学的全貌，程序员可以利用本书中简单的例子迅速掌握有关算法和协议，同时专业的研究者也可以通过本书的背景知识和习题对密码学有更深刻的理解。

全书由王全龙、王鹏和林昌露合作翻译，具体分工是：王全龙翻译第1、3、7、13、14、15和19章以及前言和附录D，王鹏翻译第2、4、5、6、8、9、10、11和12章以及附录A、B和C，林昌露翻译第16、17和18章。全书由王全龙统稿。

由于译者水平有限，译文中难免会有一些错误，欢迎读者批评指正。

前　言

本书是基于密码学课程多年教学经验而著，这门课程从1997年开始在马里兰大学向高年级本科生和一年级研究生讲授，并于2003年开始在罗格斯（Rutgers）大学讲授。在设计这门课时，我们考虑了以下要求：

- 课程内容应该是该领域的最新成果，并且从数学观点上要涵盖大部分主题。
- 讲授的内容应使不熟悉数论和计算机编程，但具有数学背景知识的学生也易于接受。
- 一些例子中应包含足够大的数，用来说明各种算法如何在实际中应用。

尽量避免只关注RSA和离散对数，因为这样会让这门课变成一门关于数论的课。也不能把注意力集中在各种协议和如何防范入侵上，那样会让这门课的数学性不够强。

本书包含很多可在密码学基础课程中讨论的主题。我们尽量把其中大部分主题包括在内。书中各章的内容基本涵盖了我们在教授该课程的几个学期中所讲的主题，当然本书的材料要多于一学期中所讲的内容。前9章是核心部分，其余章节的选取取决于学生的水平和教师的目标。

各个章节都有编号，这表明了它们的阅读顺序。但是，除第3章介绍了遍及全书的关于数论的知识外，其余各章彼此独立，因此可以按任何顺序合理安排。虽然我们并不主张这样做，但读者完全可以按相反的顺序阅读第4章到第19章，只要做几次前后对照就可以。由于学生具有不同程度的数论背景知识，因此我们把基本的数论知识集中放在第3章作为参考，但我们还是建议按照课程的进度逐步向学生介绍所需的数论概念。

关于信息论、椭圆曲线、量子密码学、格方法和纠错码的几个章节比其他章节更偏重于数学性。纠错码这一章按几位审稿人的建议放入本书，因为同时介绍密码学和编码理论的课程相当普遍。

上机实例

假设你想给出一个RSA的例子。可以选2个1位素数来模仿50位素数的运算，或者可以用自己喜欢的软件包来做一个有大素数的实际示例。也许你正在使用移位密码，试图通过尝试密文的所有26种移位而对一个消息进行解密，这个工作应该由计算机来完成。本书配有分别用Mathematica®、Maple®和MATLAB®编写的上机实例[①]，这些实例会告诉你如何进行计算，之所以选择这些语言，是因为它们界面友好且不需要有编程经验。虽然这门课在不使用计算机的情况下仍能成功地教授给学生，但这些练习仍然是本书中不可分割的部分，因此应尽量去学习。其中不仅包含了关于怎样做某些计算的数值方面的练习，还说明了涉及的重要思想和论题。这些计算机实例之所以放在最后，是出于逻辑和美观的考虑，因为各章后面已经包含了很多用3种语言编写的上机练习。

用3种语言中的任何一种编写的这些练习的程序可以在www.prenhall.com/washington网站下载，教室里所需要的就是一台计算机（安装了其中的一种软件）和一台在讲课时展示实例

① 其中Mathematica®实例见附录A，Maple®和MATLAB®上机实例的PDF文件可在图灵网站（www.turingbook.com）本书配套网页注册下载。——编者注

的投影仪。基于上述软件的家庭作业（即各章后的上机问题）可以让学生独自操作这些练习。当然，有更多编程背景的学生可以自己编写程序。

第2版的新添内容

密码学是一门发展迅速的学科。自本书第1版问世以来，密码学在诸如散列函数和基于标识的加密等方面又有了重大进展，这使得书中的内容需要更新。也有许多人对本书的表述方式提出了建议，以及要求增加更多的练习。第2版增加的主要内容包括：

(1) 许多新的练习，特别是第2章、第3章、第5章、第6章和第16章中的练习；
(2) 收录在新章节（第8章）中关于散列函数的新内容和扩充材料；
(3) 关于安全协议的新章节（第10章）；
(4) 关于格方法的新章节（第17章）；
(5) 第16章中关于基于标识的加密的一节；
(6) 第3章中关于勒让德和雅可比符号以及连分数的几节；
(7) 第4章中更多的操作模式；
(8) 第6章中对RSA的更多的攻击。

我们当然欢迎任何建议和修正。本书的勘误表可在网站www.prenhall.com/washington中找到。习题解答（供教师专用）可以从Prentice Hall 的发行代表那里获得。

致谢

本书在准备过程中得到了许多人的帮助与鼓励。首先要感谢我们的学生，他们的热情、洞察力和建议都对本书贡献极大。特别感谢许多提供修改意见和其他信息的人，尤其是我们的同事Bill Gasarch和Jeff Adams。Jonathan Rosenberg和Tim Strobell提供了可贵的技术支持。还要感谢Wenyuan Xu、Qing Li和Pandurang Kamat，他们为本书作了几幅图并且为第2版中的新增材料提供了反馈意见。本书的审稿人值得特别感谢，第1版的审稿人David Grant（科罗拉多大学Boulder分校）、David M. Pozar（马萨诸塞大学Amherst分校）、Jugal K. Kalita（科罗拉多大学 Colorado Springs分校）、Anthony Ephremides（马里兰大学College Park分校）、J.Felipe Voloch（得克萨斯大学奥斯汀分校）、Agnes Chan（东北大学）、Daniel F. Warren（海军研究生院），以及一位未提供姓名的审校人。第2版的审稿人包括Eric Bach（威斯康星大学）、James W.Brewer（佛罗里达大西洋大学）、Siman Wong（马萨诸塞大学Amherst分校）、Thomas P. Cahill（布鲁克林理工大学）和Edmund Lamagna（罗得岛大学）。他们对内容的组织和展开提出的建议极大地完善了本书。我们很高兴与Prentice Hall的员工一起工作，特别是数学编辑George Lobell以及制作编辑Jeanne Audino（第1版）和Raegan Keida（第2版）。

本书的第一作者要感谢Nisha Gilra给予的鼓励和建议，感谢Sheilagh O'Hare引领他进入密码学领域；感谢K. J. Ray给予的支持。

本书的第二作者要感谢Susan Zengerle和Patrick Washington在他编写本书时所给予的耐心帮助和鼓励。

Wade Trappe
trappe@winlab.rutgers.edu
Lawrence C. Washington
lcw@math.umd.edu

人民邮电出版社
POSTS & TELECOM PRESS

精选大师名作
打造专业品牌

TURING 图灵教育

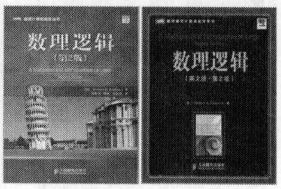
人民邮电出版社图灵公司专注于引进国外经典教材与优秀科技图书，出版国内高校教师编写的专业教材，专业方向包括：计算机、数学、统计学和电子电气等。合作伙伴包括Prentice-Hall、Addison-Wesley、Wiley、McGraw-Hill、剑桥大学出版社、Elsevier、IEEE Press、Wrox、SIAM等多家世界知名出版公司，具有丰富的选题资源和雄厚的出版力量。

图灵计算机科学丛书　　图灵原版计算机科学系列　　高等院校计算机教材系列

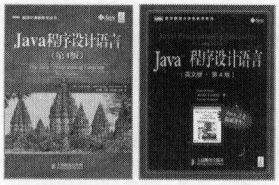
书　名：数据结构与问题求解——Java语言描述（第3版）（中英文版）
原书名：Data Structures and Problem Solving Using Java
作　者：Mark Allen Weiss
译　者：翁惠玉 严骏
中文版书号：7-115-14988-7
英文版书号：7-115-16245-8
中文版定价：49.00元
英文版定价：65.00元

书　名：UML 面向对象建模与设计(第2版)(中英文版)
原书名：Object-Oriented Modeling and Design with UML, Second Edition
作　者：Michael Blaha，James Rumbaugh
译　者：车皓阳 杨眉
中文版书号：7-115-14223-8
英文版书号：7-115-14076-6
中文版定价：45.00元
英文版定价：55.00元

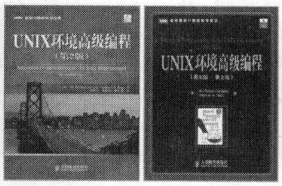
书　名：数据结构与算法分析——C++描述(第3版)(中英文版)
原书名：Data Structures and Algorithm Analysis in C++
作　者：Mark Allen Weiss
译　者：张怀勇
中文版书号：7-115-13923-7
英文版书号：7-115-15233-0
中文版定价：49.00元
英文版定价：59.00元



书　名：数理逻辑（第2版）(中英文版)
原书名：A Mathematical Introduction to Logic,2E
作　者：Herbert B.Enderton
译　者：沈复兴 陈磊 孙运传
中文版书号：7-115-14311-0
英文版书号：7-115-14145-2
中文版定价：29.00元
英文版定价：39.00元



书　名：Java程序设计语言(第4版)(中英文版)
原书名：The Java Programming Language
作　者：Ken Arnold, James Gosling, David Holmes
译　者：陈昊鹏 章程 张思博 李楠
中文版书号：7-115-15297-7
英文版书号：7-115-14762-0
中文版定价：69.00 元
英文版定价：99.00 元



书　名：UNIX环境高级编程(第2版)(中英文版)
原书名：Advanced Programming in the UNIX Environment, 2nd Edition
作　者：W.Richard Stevens, Stephen A.Rago
译　者：尤晋元 张亚英 戚正伟
中文版书号：7-115-14731-0
英文版书号：7-115-14484-2
中文版定价：99.00元
英文版定价：99.00元

书　名：数据挖掘导论（中英文版）
原书名：Introduction to Data Mining
作　者：Pang-Ning Tan, Michael Steinbach, Vipin Kumar
译　者：范明 范宏建
中文版书号：7-115-14698-5
英文版书号：7-115-14144-4
中文版定价：49.00元
英文版定价：59.00元

书　名：现代编译原理—C 语言描述(中英文版)
原书名：Modern Compiler Implementation in C
作　者：Andrew W.Appel
译　者：赵克佳 黄春 沈志宇
中文版书号：7-115-14552-0
英文版书号：7-115-13771-4
中文版定价：45.00元
英文版定价：59.00元

书　名：计算机图形学
原书名：Fundamentals of Computer Graphics
作　者：Peter Shirley
译　者：高春晓
书　号：7-115-15867-3
定　价：49.00 元

书　名：Java教程(第4版)
原书名：The Java Tutorial: A Short Course on the Basics
作　者：Sharon Zakhour
译　者：马春晖
书　号：7-115-16336-3
定　价：49.00元

书　名：计算机科学概论（第9版）
原书名：Computer Science: An Overview
作　者：J.Glenn Brookshear
译　者：刘艺 冯坤 徐建桥
书　号：7-115-16280-9
定　价：49.00 元

书　名：TCP/IP基础教程:基于实验的方法
原书名：TCP/IP Essentials: A Lab-Based Approach
作　者：Shivendra S.Panwar, 陈涓 等
译　者：
书　号：7-115-15386-8
定　价：29.00元

书　名：软件工程(第3版)
原书名：Software Engineering: Theory and Practice
作　者：Shari Lawrence Pfleeger, Joanne M.Atlee
译　者：杨卫东
书　号：978-7-115-15829-1
定　价：59.00元

书　名：Beginning Java Objects 中文版：从概念到代码
原书名：Beginning Java Objects: From Concepts to Code
作　者：Jacquie Barker
译　者：万波
书　号：7-115-15440-6
定　价：78.00元

书　名：TSP：领导开发团队
原书名：TSP: Leading a Development Team, 1E
作　者：Watts S.Humphrey
译　者：张家才 江 贺 车皓阳
书　号：7-115-13919
定　价：35.00元

书　名：TSP：培训开发团队
原书名：TSP: Coaching Development Team
作　者：Watts S.Humphrey
译　者：车皓阳　杨眉
书　号：7-115-16993-8
定　价：59.00元

书　名：数据库系统：面向应用的方法
原书名：Database Systems: An Applic-ation-Oriented Approach, Introductory Version
作　者：Michael Kifer, Arthur Bernstein, Philip M.Lewis
译　者：陈立军 赵加奎 邱海艳 帅宏
书　号：7-115-15269-1
定　价：49.00元

书　名：数据库系统基础：初级篇（第5版）
原书名：Fundamentals of Database Systems
作　者：Ramez Elmasri Shamkant B. Navathe
译　者：邵佩英 徐俊刚 王文杰
书　号：7-115-16408-7
定　价：49.00元

书　名：数据库系统基础：高级篇（第5版）
原书名：Fundamentals of Database Systems
作　者：Ramez Elmasri Shamkant B. Navathe
译　者：邵佩英 徐俊刚 王文杰
书　号：7-115-17160-3
定　价：49.00元

书　名：UML用户指南(第2版)
原书名：The Unified Modeling Language User Guide
作　者：Grady Booch, James Raumbaugh, Ivar Jacobson
译　者：邵维忠 麻志毅 马浩海 刘辉
书　号：7-115-14833-3
定　价：49.00 元

相关教辅资料和习题答案可从图灵网站（www.turingbook.com）下载

人民邮电出版社
POSTS & TELECOM PRESS

精选大师名作
打造专业品牌

TURING 图灵教育

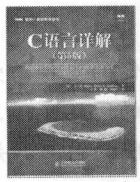
图灵计算机科学丛书　　图灵原版计算机科学系列　　高等院校计算机教材系列

书　名：计算机网络实验教程
原书名：Computer Networking: Internet Protocols in Action
作　者：Jeanna Matthews
译　者：李毅超 曹跃 王钰
书　号：7-115-14250-5
定　价：29.00元

书　名：算法分析与设计
原书名：Algorithm Design: Foundations, Analysis, and Internet Examples
作　者：Michael T.Goodrich, Roberto Tamassia
译　者：霍红卫
书　号：7-115-15054-0
定　价：55.00元

书　名：Java程序设计与问题解决：基础篇（第4版）
原书名：Java: An Introduction to Problem Solving and Programming
作　者：Walter Savitch
译　者：陈涓 赵振平
书　号：7-115-16566-4
定　价：49.00元

书　名：Java程序设计与问题解决：高级篇（第4版）
原书名：Java: An Introduction to Problem Solving and Programming
作　者：Walter Savitch
译　者：陈涓 赵振平
书　号：7-115-16922-8
定　价：49.00元



书　名：C语言详解（第5版）
原书名：Problem Solving and Program Design in C
作　者：Jeri Hanly, Elliot Koffman
译　者：万波 潘蓉 郑海红
书　号：7-115-16427-8
定　价：69.00元

书　名：C语言程序设计：现代方法
原书名：C Programming: A Modern Approach
作　者：K.N.King
译　者：吕秀锋
书　号：7-115-16707-1
定　价：55.00元

书　名：计算机组成：结构化方法（第5版）
原书名：Structured Computer Organization
作　者：Andrew S.Tanenbaum
译　者：刘卫东 宋佳兴 徐恪
书　号：7-115-14891-0
定　价：65.00元

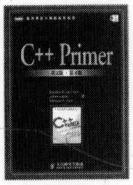
书　名：UNIX实用教程
原书名：Just Enough UNIX
作　者：Paul K. Andersen
译　者：宋虹 曾庆冬 段佳华 杨路明
书　号：7-115-16912-9
定　价：49.00元

书　名：C++教程
原书名：C++ By Dissection
作　者：Ira Pohl
译　者：陈朔鹰 马锐 薛静锋 吕坤
书　号：7-115-16708-8
定　价：49.00元

书　名：软件测试与连续质量改进（第2版）
原书名：Software Testing and Continuous Quality Improvement
作　者：William E.Lewis
译　者：陈绍英 张河涛 刘建华 金成姬
审　校：冯国云 尹众
书　号：7-115-17161-0
定　价：55.00元

书　名：嵌入式系统：硬件与软件架构
原书名：Embedded Systems Architecture: A Comprehensive Guide for Engineers and Programmers
作　者：Tammy Noergaard
译　者：马洪兵 谷源涛
书　号：7-115-16805-4
定　价：69.00元

书　名：密码学与编码理论
原书名：Introduction to Cryptography with Coding Theory
作　者：Wade Trappe, Lawrence Washington
书　号：7-115-17435-2
译　者：王金龙 王鹏 林昌露
定　价：49.00元



书　名：C++ Primer（英文版·第4版）
作　者：Stanley Lippman
书　号：7-115-15169-5
定　价：99.00元

书　名：Java程序设计与问题解决：基础篇(英文版·第4版)
原书名：Java: An Introduction to Problem Solving and Programming
作　者：Walter Savitch
书　号：7-115-15288-8
定　价：59.00元

书　名：Java程序设计与问题解决:高级篇(英文版·第4版)
原书名：Java: An Introduction to Problem Solving and Programming
作　者：Walter Savitch
书　号：7-115-15289-6
定　价：59.00元

书　名：C语言程序设计(英文版·第3版)
原书名：Programming in C
作　者：Stephen G.Kochan
书　号：7-115-14763-9
定　价：55.00元

书　名：系统分析与设计(英文版·第3版)
原书名：Essentials of System Analysis and DesignThird Edition
作　者：Joseph S. Valacich; Jeffrey A. Hoffer
书　号：7-115-15154-7
定　价：55.00元

书　名：数据结构与算法分析—C语言描述(英文版·第2版)
原书名：Data Structures and Algorithm Analysis in C
作　者：Mark Allen Weiss
改　编：陈越
书　号：7-115-13984-9
定　价：49.00元

书　名：C语言程序设计
作　者：楼永坚
书　号：7-115-15096-6
定　价：28.00元

书　名：实用数据结构教程：Java语言描述
作　者：周大庆
书　号：7-115-15907-6
定　价：28.00 元

书　名：计算机日语
作　者：张凯
书　号：7-115-16281-6
定　价：45.00 元

书　名：计算机算法：设计与分析导论
作　者：朱清新 杨凡 钟黔川 等
书　号：7-115-16833-7
定　价：35.00元

书　名：数据库原理与应用
作　者：徐保民 孙丽君 李爱萍
书　号：[新编]
书　号：7-115-17072-9
定　价：32.00元

好书不断，期待关注

图灵计算机科学丛书　　图灵原版计算机科学系列　　高等院校计算机教材系列

书　名：数据库系统基础：初级篇（英文版•第4版）
作　者：Ramez Elmasri,Shamkant Navathe
定　价：49.00元（估）
预计出版时间：2007年12月

书　名：TCP/IP 指南（卷1）：底层核心协议
作　者：Charles M.Kozierok
译　者：陈鸣
定　价：79.00元（估）
预计出版时间：2007年12月

书　名：软件测试基础教程（英文版•第2版）
作　者：Andreas Spillner,Tilo Linz,Hans Schaefer
定　价：55.00元（估）
预计出版时间：2008年2月

书　名：现代系统分析与设计（第4版）
作　者：Jeffrey Hoffer，Joey George
译　者：刘鹏 郝晓玲 张娥 雷蕾
定　价：55.00元（估）
预计出版时间：2008年2月

书　名：TCP/IP 指南(卷2)：应用层协议
作　者：Charles M.Kozierok
译　者：陈鸣
定　价：79.00元（估）
预计出版时间：2008年2月

书　名：Java面向对象方法（第3版）
作　者：David Barnes, Michael Kölling
定　价：59.00元（估）
注释版预计出版时间：2008年2月

书　名：电子商务（英文版•第3版）
作　者：Elias M.Awad
定　价：65.00元（估）
预计出版时间：2008年2月

书　名：编程珠玑II
作　者：Jon Bentley
译　者：刘田
定　价：29.00元（估）
预计出版时间：2008年1月

相关教辅资料和习题答案可从图灵网站（www.turingbook.com）下载

读者意见交流卡

亲爱的读者：

感谢您对我们的支持与爱护。为了今后为您提供更优秀的图书，请您抽出宝贵时间填写本表（或通过我们的网站www.turingbook.com填写本表），将您的意见及时告知我们。您将有机会免费获赠我们出版的图书，并能获得最新的出版信息和更多服务，谢谢！

系列书名：图灵计算机科学丛书
本 书 名：密码学与编码理论（第 2 版）

读者资料：

姓　　名：_____　性　　别：☐男　☐女　年　　龄：_____
职　　业：_____　文化程度：_____　通信地址：_____
电　　话：_____　传　　真：_____　电子信箱（E-mail）：_____

1. 您是如何得知本书的：

☐别人推荐　☐书店　☐出版社图书目录
☐杂志、报纸、网络等的介绍（请指明）
☐其他（请指明）_____

2. 您从何处购得本书：

☐新华书店　☐电脑专业书店　☐网上书店　☐其他 _____

3. 影响您购买本书的因素：

☐内容和质量　☐装帧设计　☐价格
☐内容提要、前言或目录　☐书评广告
☐出版社名气　☐作者名气　☐其他 _____

4. 您对本书封面和封底设计的满意度：

☐很满意　☐比较满意　☐一般　☐较不满意　☐不满意
☐建议 _____

5. 您认为本书：

价格：　☐高　☐合适　☐低
翻译质量：　☐高　☐一般　☐差
图书印刷质量：　☐高　☐一般　☐差

6. 您希望本书哪些方面进行改进？

_____
_____

7. 您感兴趣或希望出版的图书有：

_____
_____

请寄：北京市西四环北路140号京鼎原商务楼405房间　人民邮电出版社图灵公司　市场部收
邮编：100097　电话：010-88593802　传真：010-88593803
电子信箱（E-mail）：contact@turingbook.com　网址：www.turingbook.com

目　录

第1章 密码学及其应用概述

人们总想对他人保守自己信息的秘密，历史上有不少这方面的例子。国王和将军们利用基本的密码方法与他们的军队进行通信，以防止敌人获得敏感的军事信息。据说凯撒大帝（Julius Caesar）就用过一种后来以他名字命名的简单密码。

随着社会的发展，人们对更先进的数据保护方法的需求在不断增加。在如今的信息时代，这种需求比以往更为显著。随着世界的联系变得更加紧密，对信息和电子服务的需求也在不断增长，这种需求的增长造成了对电子系统的更加依赖。诸如信用卡号之类的敏感信息交换在因特网上已经成了一件普通事。保护数据与电子系统对我们的生活方式至关重要。

用来保护数据的技术属于密码学领域。实际上，它有cryptography、cryptology和cryptanalysis 3个名字，这些名字经常交替使用。但是从技术上说，cryptology是一个全面的术语，它指的是对不安全信道上的通信及相关问题的研究，而设计能够进行这种通信的密码系统的过程则称为cryptography。cryptanalysis所处理的问题是破译这种密码系统。当然，不管是进行cryptography还是cryptanalysis，如果对这两方面中的方法没有良好理解，那基本上是不可能做到的。

编码理论（coding theory）这个术语经常会被用来描述密码学，但这样会导致混淆。编码理论所做的是把输入的信息符号用称为码符号的输出符号表示出来。编码理论包括3个基本应用——压缩、保密和纠错。在过去的几十年中，编码理论这个术语变成主要是和纠错码相关了。编码理论因此成为研究噪声信道上的通信以及如何确保收到正确消息的理论，与密码学相反，它是要保护不安全信道上的通信。

虽然纠错码是本书的一个次要论题，但我们还是要强调，在任何一个现实世界的系统中，纠错码都是和加密一起使用的，因为任何一位的改变都足以破坏一个设计良好的密码系统的消息完整性。

现代密码学是一个高度依赖于数学、计算机科学和聪明才智的领域。本书介绍了建立安全的数据传输和电子系统所需的数学和协议知识，以及包括电子签名和秘密共享在内的技术。

1.1 安全通信

在如图1-1所描绘的基本通信模式中，有Alice 和 Bob两方互相通信。第三方Eve，则是一个隐藏的窃听者。

当Alice向Bob发送消息（称之为**明文**）时，她与Bob使用预先约定的方法对消息进行加密。通常，假定加密方法为Eve所知；能使消息保密的是**密钥**。当Bob收到加密的消息（称之为**密文**）时，他便用解密密钥把密文还原成明文。

Eve可能有如下意图：

(1) 阅读该消息；

(2) 找到密钥以便阅读所有用该密钥加密的消息；

(3) 窜改Alice的消息，使Bob以为Alice发的是改写后的那条消息；

(4) 冒充Alice与Bob通信，并使Bob相信自己是在和Alice通信。

我们面临的是以上哪种情形要视Eve有多邪恶而定。情形(3)和(4)分别与完整性和鉴别相关，我们将很快讨论到这些。像情形(3)和(4)中那样比较主动和恶意的敌方，在文献中通常称他Mallory；而更为被动的观察者（如情形(1)和(2)中那样）则有时称为Oscar。我们一般仅用Eve这个名字，并且假定她在条件所允许的情况下会做到最坏。

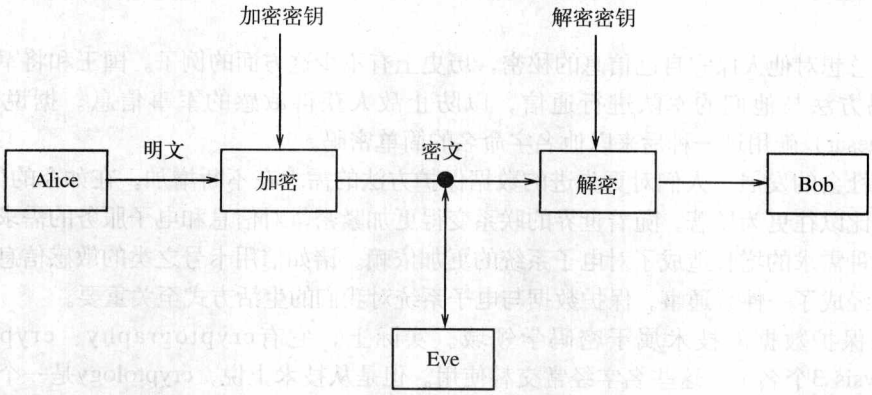


图1-1　密码学基本通信模式

1.1.1　可能的攻击

Eve有4种主要的攻击方式。这些攻击方式的区别在于Eve在试图获取密钥时所拥有的信息量。这4种攻击方式如下所述。

(1) **唯密文**：Eve只有一份密文的副本。

(2) **已知明文**：Eve有一份密文的副本以及相应的明文。例如，假设Eve截获了一份加密的通信稿，并在第二天看到了解密后的通信稿。如果Alice没有改变密钥而Eve又能推断出解密密钥来，那么她就能读出将来的所有信息。或者，如果Alice总是以“Dear Bob”作为其消息的开头，那么Eve就有了一小份密文和相对应的明文。对许多弱密码系统来说，这足以找到密钥了。即使是对于像二战中使用的德国的Enigma密码机这样比较强的密码系统，上述的这种信息也起了很大的作用。

2
~
3

(3) **选择明文**：Eve有短暂的机会接触加密机。她不能打开机器来找密钥，但可以加密大量经过适当选择的明文，然后试着利用所得的密文来推断密钥。

(4) **选择密文**：Eve有短暂的机会接触解密机，她用它来对若干字符串符号解密，然后试着用所得结果推断密钥。

有一种选择明文攻击可能按如下方式发生。你想识别一架飞机是敌机还是友机。向这架飞机发送一个随机消息，飞机对消息自动加密后将其返回。假定只有友机有正确的密钥。将从飞机上返回的消息与正确加密的消息相比较，如果吻合那么飞机是友机，否则就是敌机。但是，敌方可以发送大批经过选择的消息给你方的某架飞机，然后查看收到的密文。如果他们可以因此推断出密钥，那敌方就可以把他们的飞机伪装成友机。

一个已知明文攻击的实例据说发生在二战时期的撒哈拉沙漠。一个孤立的德军前哨每天都会发送一个同样的消息，报告没有什么新情况，这条消息当然是用当天的密钥加密的，所以盟

军每天可以获得一个明文－密文对，这对于确定密钥来说是非常有用的。而事实上在撒哈拉战役期间，蒙哥马利将军一直在非常小心地控制着这个前哨，以使得这种消息传递不会被中断。

现代密码学中一个最要的假设就是**Kerckhoffs原则**：在评估一个密码系统的安全性时，必须假定敌方知道所用的加密方法。这个原则是由Auguste Kerckhoffs于1883年在他的经典论文*La Cryptographie Militaire*中阐明的。敌方可以有很多方式获得这个信息，如加密/解密机可以被俘获和分析，或者人员叛变或被捕。系统的安全性因而应该基于密钥而不是所用算法的隐蔽性。所以，我们总是假定Eve知道用来加密的算法。

1.1.2 对称和公钥算法

加密/解密方法可分成两个范畴：**对称密钥**和**公钥**。在对称密钥算法中，加密密钥和解密密钥为Alice和Bob所共知。例如加密密钥共享后，解密密钥很容易由其算出。在很多情况下，加密密钥和解密密钥是相同的。所有的传统（1970年以前）密码系统都是对称密码，正如后来的数据加密标准（DES）和高级加密标准（AES）。

4

20世纪70年代提出的公钥算法是密码学的一次革命。假设Alice想和Bob安全地通信，但他们相隔数百公里而且没有商量好要用的密钥。如果没有事先碰头商量好密钥或由一个信得过的信使把密钥从一方送到另一方，那么要想做到安全通信看起来几乎是不可能的。Alice当然不能通过公开信道发送消息来告诉Bob密钥，然后发送用这个密钥加密的密文。令人惊奇的是这个问题居然有解，即所谓的公钥密码学：加密密钥是公开的，但是如果没有仅为Bob所知的信息，要找到解密密钥在计算上是不可行的。应用最为普遍的公钥算法是RSA（见第6章），它是基于大整数因子分解的困难性。其他公钥算法（见第7章、第17章和第18章）还有ElGamal 系统（基于离散对数问题），NTRU（基于格）和McEliece系统（基于纠错码）。

有一个非数学的方式可以用来解释公钥密码通信。Bob发送给Alice一个盒子和一把开着的挂锁。Alice把消息放入盒子并用Bob的锁锁上，然后送还给Bob。当然，只有Bob能够打开盒子阅读信息。前面提到的公钥方法正是这个想法的数学实现。显然这里有鉴别的问题必须解决。例如Eve可能会截住第一次传送的盒子并换上她自己的锁。如果她接着截住Alice发还给Bob的上锁的盒子，那么就可以打开她的锁，然后阅读Alice的消息。这是任何此种系统必须解决的普遍性问题。

公钥密码学所代表的可能是这段令人感兴趣的历史进步中的最后一步。在密码学的初期，安全性依赖于加密方法的保密。后来就假定加密方法是已知的，而安全性则依赖于将（对称）密钥保密或不让敌方知晓。在公钥密码学中，加密方法和加密密钥是公开的，而且每个人都知道如何去找解密密钥。其安全性依赖于这样一个事实（或愿望）：找解密密钥在计算上是不可行的。经过若干年的发展，密码算法的功能日益增强，但与此对应的是敌方所掌握的关于这些算法的信息量也在不断增加，这相当矛盾。

公钥方法功能强大，看起来对称密码似乎要被废弃了。然而，这种新添的灵活性不是免费的，它是以计算为代价的。公钥算法所需的计算量通常比DES或Rijndale这样的算法的计算量高几个数量级。经验告诉我们，不要用公钥方法来加密大批量的数据。因此，公钥方法只用于少量数据的处理上（如数字签名和发送对称密钥算法中使用的密钥）。

5

对称密码学中有两种类型的密码：流密码和分组密码。在流密码中，数据是一小片一小片（若干位或字符）地输入算法，输出也是一小片一小片地产生。但在分组密码里，一组位一次性全部输入到算法中，输出的也是一组位。在2.11节中将讨论一个基于线性反馈移位寄存器的

流密码的例子，但我们更多地还是关注分组密码。同时给出两个重要的例子，第一个是DES，第二个是Rijndael，后者被（美国）国家标准技术研究所（NIST）于2000年选来代替DES。像RSA这样的公钥方法也可以看作是分组密码。

最后，我们给出历史上两个不同类型的加密，即**码**（code）和**密码**（cipher）。在码里，单词或某个字母组合由码字（可能是符号串）代替。例如，一战期间英国海军用03680C、36276C和50302C分别代表*shipped at*、*shipped by*和*shipped from*。码的缺点在于不能使用未曾预料的单词。相反，密码不需要用到消息的语言结构，而只要用某个算法对每一串字符加密，不管它是否有意义，因此密码比码用途更广。在密码学的早期，普遍使用码，有时也结合密码一块使用，而且在今天仍被使用——隐蔽的军事行动经常以码命名。然而，任何秘密要保证安全都要使用密码加密。本书我们只讨论密码。

1.1.3　密钥长度

密码学算法的安全性是一个很难度量的性质。大多数算法会使用密钥，并且算法的安全性与敌方确定密钥的困难程度相关。最显著的方法是尝试每一个可能的密钥，看哪些能得到有意义的解密，这种攻击被称为**蛮力攻击**（brute force attack）。在蛮力攻击中，密钥的长度直接和搜索整个密钥空间所需的时间相关。例如一个密钥的长度是16位，那么就有$2^{16}=65536$个可能的密钥。DES算法的密钥长度为56位，从而有$2^{56}\approx 7.2\times 10^{16}$个可能的密钥。

本书中有很多这样的情况，即系统看起来似乎可以通过简单地尝试所有可能的密钥而被破解，可是说起来容易做起来难。假定需要尝试10^{30}种可能性，而你的计算机每秒可做10^{9}次这种运算。一年大约有3×10^{7}秒，所以需要3×10^{13}年还多一些的时间才能完成这个任务，这比所预测的宇宙的寿命还长。

较长的密钥更有优势，但是这并不保证会增加敌方破译任务的困难性，算法本身也起了关键的作用。有些算法可能被蛮力之外的其他方法所攻击，还有些算法并不能很有效地使用密钥位。有一点非常重要，需要牢记：不是所有的128位的算法天生就是平等的！

例如，一个最容易破解的密码系统就是替换密码（我们将在2.4节讨论），虽然这个密码的可能密钥数为$26!\approx 4\times 10^{26}$个。相比较而言，复杂的DES（见第4章）有$2^{56}\approx 7.2\times 10^{16}$个可能的密钥，在一个特别设计的计算机上找一个DES密钥通常也要一天的时间。两者的区别在于，对替换密码的攻击用的是语言的基本结构，而对DES的攻击用的是蛮力攻击，这要尝试所有可能的密钥。

蛮力攻击应该是最后使用的手段，一个密码分析员总是希望能找到比这更快的攻击方法。我们将会碰到的例子有频率分析（用于替换密码和维吉内尔密码）和生日攻击（用于离散对数）。

我们也要告诫读者，一个算法现在看起来似乎安全，但并不意味着它以后也是如此。人类的智慧已经对密码协议产生了创造性的攻击方法。现代密码学中有很多算法或协议被成功攻破的例子，这或者是由于不当操作引起的漏洞造成的，或者是由于技术的进步造成的。DES算法经受住了20年的考验，最终被一台精心设计的并行计算机攻破。当你阅读本书时，量子计算的研究正在进行，它将极大地改变将来密码学算法的面貌。

例如，将要研究的几个系统的安全性都依赖于因子分解像200位这么大整数的困难性。假定想分解这般大小的一个数n，小学用的方法是用n除以所有不超过n的平方根的素数。小于10^{100}的素数大约有4×10^{97}个，用每一个去试是不可能的。宇宙中电子的数目据估计小于10^{90}，早在你完成计算之前，就会接到电力公司的电话让你停止计算。显然，必须使用更精致的因子分解算法，而不是这种蛮力攻击。当RSA被发明时已经有一些好的因子分解算法可用，但是据