大学计算机教育国外著名教材、教参系列（影印版）

Cryptography and Network Security: *Principles and Practice*

Second Edition

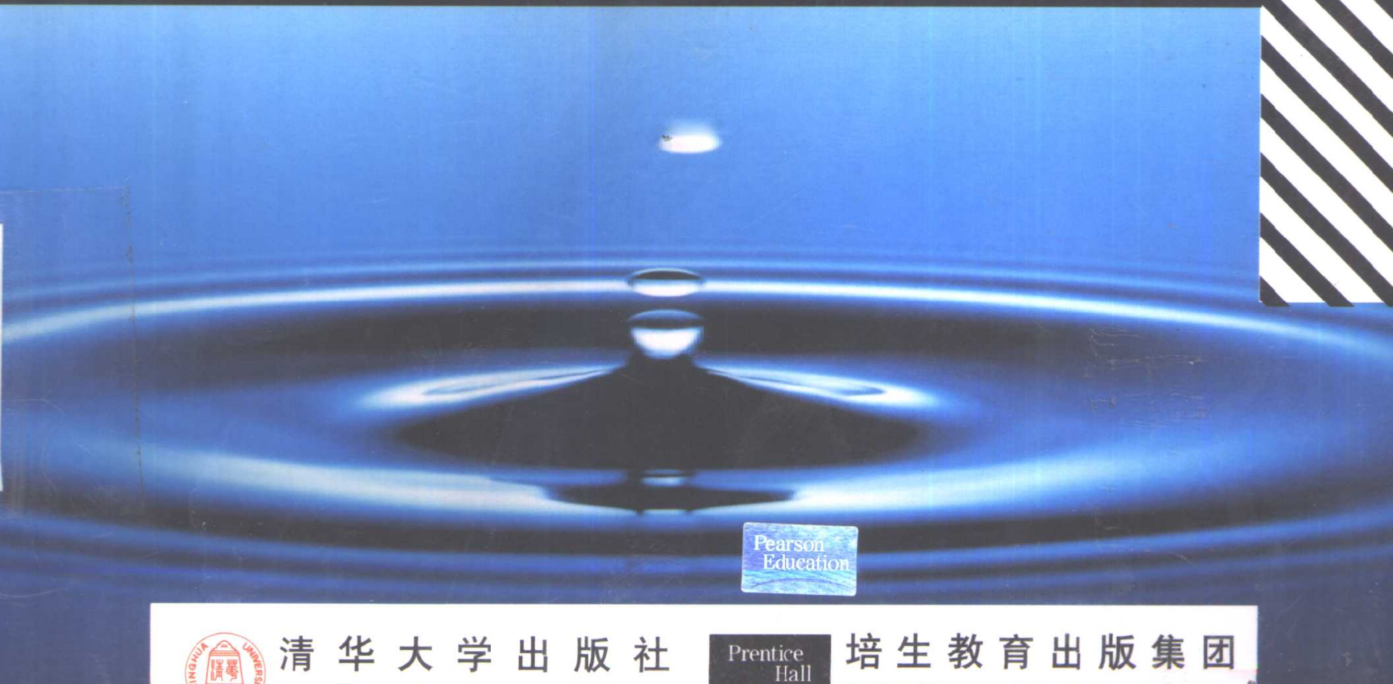
William Stallings

Winner of the 1999 TEXTY award for the best computer science and engineering textbook

密码学与网络安全：原理与实践

3

（第 2 版）



清华大学出版社
http://www.tup.tsinghua.edu.cn

Prentice Hall
培生教育出版集团
http://www.pearsoned.com

Cryptography and Network Security :

Principles and Practice

Second Edition

密码学与网络安全：

原理与实践

（第 2 版）

William Stallings

清华大学出版社　　培生教育出版集团

（京）新登字 158 号

Cryptography and network security: principles and practice 2nd ed.
William Stallings

北京市版权局著作权合同登记号：图字：01-2002-1660

图书在版编目(CIP)数据

密码学与网络安全：原理与实践：第 2 版 / (美) 斯托林斯著. 影印本. —北京：清华大学出版社，2002.6

（大学计算机教育国外著名教材、教参系列）

ISBN 7-302-05537-8

Ⅰ. 密… Ⅱ. 斯… Ⅲ. ① 密码－理论－高等学校－教材－英文 ② 计算机网络－安全技术－高等学校－教材－英文 Ⅳ. ① TN918.1 ② TP393.08

中国版本图书馆 CIP 数据核字（2002）第 037389 号

出版者：清华大学出版社（北京清华大学学研大厦，邮编 100084）
　　　　http:// www.tup.tsinghua.edu.cn
印刷者：北京牛山世兴印刷厂
发行者：新华书店总店北京发行所
开　本：787×960 1/16　印张：37
版　次：2002 年 6 月第 1 版　2002 年 6 月第 1 次印刷
书　号：ISBN 7-302-05537-8/TP・3260
印　数：0001～4000
定　价：53.00 元

出 版 说 明

进入 21 世纪，世界各国的经济、科技以及综合国力的竞争将更加激烈。竞争的中心无疑是对人才的争夺。谁拥有大量高素质的人才，谁就能在竞争中取得优势。高等教育，作为培养高素质人才的事业，必然受到高度重视。目前我国高等教育的教材更新较慢，为了加快教材的更新频率，教育部正在大力促进我国高校采用国外原版教材。

清华大学出版社从 1996 年开始，与国外著名出版公司合作，影印出版了“大学计算机教育丛书（影印版）”等一系列引进图书，受到了国内读者的欢迎和支持。跨入 21 世纪，我们本着为我国高等教育教材建设服务的初衷，在已有的基础上，进一步扩大选题内容，改变图书开本尺寸，一如既往地请有关专家挑选适用于我国高校本科及研究生计算机教育的国外经典教材或著名教材以及教学参考书，组成本套“大学计算机教育国外著名教材、教参系列（影印版）”，以飨读者。深切期盼读者及时将使用本系列教材、教参的效果和意见反馈给我们。更希望国内专家、教授积极向我们推荐国外计算机教育的优秀教材，以利我们把“大学计算机教育国外著名教材、教参系列（影印版）”做得更好，更适合高校师生的需要。

计算机引进版图书编辑室

2002.3

To Antigone
never dull
never boring
always a Sage

PREFACE

"The tie, if I might suggest it, sir, a shade more tightly knotted. One aims at the perfect butterfly effect. If you will permit me —"
"What does it matter, Jeeves, at a time like this? Do you realize that Mr. Little's domestic happiness is hanging in the scale?"
"There is no time, sir, at which ties do not matter."

—*Very Good, Jeeves!* P. G. Wodehouse

In this age of universal electronic connectivity, of viruses and hackers, of electronic eavesdropping and electronic fraud, there is indeed no time at which security does not matter. Two trends have come together to make the topic of this book of vital interest. First, the explosive growth in computer systems and their interconnections via networks has increased the dependence of both organizations and individuals on the information stored and communicated using these systems. This, in turn, has led to a heightened awareness of the need to protect data and resources from disclosure, to guarantee the authenticity of data and messages, and to protect systems from network-based attacks. Second, the disciplines of cryptography and network security have matured, leading to the development of practical, readily available applications to enforce network security.

OBJECTIVES

It is the purpose of this book to provide a practical survey of both the principles and practice of cryptography and network security. In the first two parts of the book, the basic issues to be addressed by a network security capability are explored by providing a tutorial and survey of cryptography and network security technology. The latter part of the book deals with the practice of network security: practical applications that have been implemented and are in use to provide network security.

The subject, and therefore this book, draws on a variety of disciplines. In particular, it is impossible to appreciate the significance of some of the techniques discussed in this book without a basic understanding of number theory and some results from probability theory. Nevertheless, an attempt has been made to make the book self-contained. The book presents not only the basic mathematical results that are needed but provides the reader with an intuitive understanding of those results. Such background material is introduced as needed. This approach helps to motivate the material that is introduced, and the author considers this preferable to simply presenting all of the mathematical material in a lump at the beginning of the book.

INTENDED AUDIENCE

The book is intended for both an academic and a professional audience. As a textbook, it is intended as a one-semester undergraduate course in cryptography and network security for computer science, computer engineering, and electrical engineering majors. The book also serves as a basic reference volume and is suitable for self-study.

Plan of the Book

The book is organized in four parts:

I. **Conventional Encryption:** A detailed examination of conventional encryption algorithms and design principles, including a discussion of the use of conventional encryption for confidentiality.

II. **Public-Key Encryption and Hash Functions:** A detailed examination of public-key encryption algorithms and design principles. This part also examines the use of message authentication codes and hash functions, as well as digital signatures and public-key certificates.

III. **Network Security Practice:** Covers important network security tools and applications, including Kerberos, X.509v3 certificates, PGP, S/MIME, IP Security, SSL/TLS, and SET.

IV. **System Security:** Looks at system-level security issues, including the threat of and countermeasures for intruders and viruses, and the use of firewalls and trusted systems.

A more detailed, chapter-by-chapter summary appears at the end of Chapter 1. In addition, the book includes an extensive glossary, a list of frequently used acronyms, and a bibliography. There are also end-of-chapter problems and suggestions for further reading.

INTERNET SERVICES FOR INSTRUCTORS AND STUDENTS

There is a Web page for this book that provides support for students and instructors. The page includes links to relevant sites, transparency masters of figures in the book in PDF (Adobe Acrobat) format, and sign-up information for the book's

Internet mailing list. The Web page is at http://www.shore.net/~ws/Security2e.html. An Internet mailing list has been set up so that instructors using this book can exchange information, suggestions, and questions with each other and with the author. As soon as typos or other errors are discovered, an errata list for this book will be available at http://www.shore.net/~ws.

PROJECTS FOR TEACHING CRYPTOGRAPHY AND NETWORK SECURITY

For many instructors, an important component of a cryptography or security course is a project or set of projects by which the student gets hands-on experience to reinforce concepts from the text. This book provides an unparalleled degree of support for including a projects component in the course. The instructor's manual not only includes guidance on how to assign and structure the projects, but also includes a set of suggested projects that covers a broad range of topics from the text:

- **Research Projects:** A series of research assignments that instruct the student to research a particular topic on the Internet and write a report.
- **Programming Projects:** A series of programming projects that cover a broad range of topics and that can be implemented in any suitable language on any platform.
- **Reading/Report Assignments:** A list of papers in the literature, one for each chapter, that can be assigned for the student to read and then write a short report.

See Appendix A for details.

WHAT'S NEW IN THE SECOND EDITION

In the four years since the first edition of this book was published, the field has seen continued innovations and improvements. In this new edition, I try to capture these changes while maintaining a broad and comprehensive coverage of the entire field. To begin this process of revision, the first edition of this book was extensively reviewed by a number of professors who teach the subject. The result is that, in many places, the narrative has been clarified and tightened, and illustrations have been improved. Also, a number of new "field-tested" problems have been added.

An obvious change is in the title; the book is now called *Cryptography and Network Security*, to reflect the central role of cryptographic algorithms in network security. The book has also been drastically reorganized to provide a more logical sequence both for classroom instruction and self-study.

Beyond these refinements to improve pedagogy and user friendliness, there have been major substantive changes throughout the book. Highlights include the following:

- **New—Discussion of Block Cipher Design:** Three sections that discuss the structure of block ciphers, block cipher design principles, and features of recent advanced ciphers have been added, greatly strengthening the overall discussion of conventional encryption.

- **New—Coverage of Additional Conventional Encryption Algorithms:** The book now includes coverage of recent algorithms that are being found in commercial products and Internet standards, including Blowfish, RC5, and CAST-128.
- **New—Treatment of Elliptic Curve Cryptography:** This is becoming an important alternative to RSA and Diffie-Hellman for public-key cryptography.
- **Expanded—Coverage of Number Theory:** The coverage has been expanded to an entire chapter and includes numerous worked-out examples to clarify this abstract subject.
- **New—Discussion of Hash Code and MAC Design:** Discussion has been added on design principles and security of hash functions and message authentication codes.
- **New—Coverage of Additional Hash and MAC Algorithms:** The book now includes coverage of recent algorithms that are being found in commercial products and Internet standards, including RIPEMD-160 and HMAC.
- **Expanded—Coverage of X.509 and New Treatment of X.509v3:** X.509 public-key certificates, especially version 3, are now found in numerous products and Internet standards.
- **New—Coverage of S/MIME:** S/MIME has become the standard for commercial secure electronic mail.
- **New—Chapter on IP Security:** IPSec is an important new set of standards for constructing virtual private networks and for end-to-end security over the Internet. An entire chapter has been added to treat this important topic.
- **New—Chapter on Web Security:** Web security has become one of the most important areas of network security and raises many new challenges. An entire chapter has been added to treat this topic. The chapter covers two major Web security standards:
    - **Secure Socket Layer (SSL) and Transport Layer Security (TLS):** SSL is the defacto standard for Web security found in virtually all browser and server offerings; TLS is an emerging Internet standard intended to replace SSL.
    - **Secure Electronic Transactions (SET):** SET is the emerging standard for secure electronic commerce over the Web.
- **New—Chapter on Firewalls:** Firewalls have emerged as the product of choice for protecting corporate sites that are connected to the Internet.
- **New—Expanded Instructor Support:** The instructor's manual, as before, includes solutions to all of the problems in the book. In addition, the manual provides support for student projects, as described previously.
- **Other changes:** These include the following:
    - A new section on bent functions, which are important in the design of S-boxes for conventional encryption algorithms.
    - Pointers to relevant Web sites are found in the Recommended Reading section of many chapters.
    - Dozens of new homework problems have been added.

ACKNOWLEDGMENTS

This book has benefited from review by numerous experts in the field, who gave generously of their time and expertise. The following people reviewed all or a large part of the first edition: Shivakumar Sastry (Rockwell Automation), Alan Sherman (University of MD Baltimore County), Tom Dunigan (University of Tennessee), Dan Boneh (Stanford University), and Sushil Jajodia (George Mason University).

In addition, I was extremely fortunate to have reviews of individual topics by "subject-area gurus," including Ron Rivest at MIT (RC5 and MD5); Tim Mathews of RSA Data Security (S/MIME); Bruce Schneier of Counterpane Systems (Blowfish); Carlisle Adams of Entrust Technologies (CAST and bent functions); Alfred Menezes of University of Waterloo (Elliptic Curve Cryptography); Terry Ritter of Ritter Software Engineering (bent functions); William G. Sutton, Editor/Publisher of the Cryptogram (Classical Encryption); Aviel Rubin of AT&T Labs (Number Theory); Bart Preneel of Katholieke Universiteit Leuven (RIPEMD-160); Michael Markowitz of Information Security Corporation (SHA and DSS); Xuejia Lai of R3 Security Engineering AG (IDEA); Don Davis of Openvision Technologies (Kerberos); Steve Kent (X.509); Phil Zimmermann of Boulder Software Engineering (PGP); and Ed Scheafer of Santa Clara University (Simplified DES).

The following people contributed project assignments that appear in the instructor's manual: Henning Schulzrinne (Columbia University); Cetin Kaya Koc (Oregon State University); and David Balenson (Trusted Information Systems and George Washington University).

Also, I would like to acknowledge those who contributed homework problems: Luke O'Connor; Joseph Kusmiss of MITRE; Carl Ellison of Stratus; Shunmugavel Rajarathinam; and Jozef Vyskoc, who contributed those marvelous Sherlock Holmes problems.

With all this assistance, little remains for which I can take full credit. However, I am proud to say that, with no help whatsoever, I selected all of the quotations.

CRYPTOGRAPHY AND NETWORK SECURITY:
Principles and Practice

SECOND EDITION

ACRONYMS

AH	Authentication Header
ANSI	American National Standards Institute
CBC	Cipher Block Chaining
CESG	Communications-Electronics Security Group
CFB	Cipher Feedback
DES	Data Encryption Standard
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
ECB	Electronic Codebook
ESP	Encapsulating Security Payload
FIPS	Federal Information Processing Standard
IAB	Internet Architecture Board
IDEA	International Data Encryption Algorithm
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPSec	IP Security
ISO	International Organization for Standardization
ITU	International Telecommunication Union
ITU-T	ITU Telecommunication Standardization Sector
IV	Initialization Vector
KDC	Key Distribution Center
LAN	Local Area Network
MAC	Message Authentication Code
MIC	Message Integrity Code
MIME	Multi-Purpose Internet Mail Extension
MD5	Message Digest, Version 5
MTU	Maximum Transmission Unit
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OFB	Output Feedback
PGP	Pretty Good Privacy
PRNG	Pseudorandom Number Generator
RFC	Request for Comments
RNG	Random Number Generator
RSA	Rivest-Shamir-Adelman
SET	Secure Electronic Transaction
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
S/MIME	Secure MIME
SNMP	Simple Network Management Protocol
SNMPv3	Simple Network Management Protocol version 3
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
WAN	Wide Area Network

大学计算机教育国外著名教材、教参系列
（影印版）图书目录

1. UNIX Network Programming Vol. 2: Interprocess Communications 2nd *ed.* 1999/*W. Richard Stevens*（UNIX 网络编程卷 2：进程间通信 第 2 版 580 页）
2. The 80x86 IBM PC and Compatible Computers（Volumes Ⅰ&Ⅱ）Assembly Language, Design, and Interfacing 3rd *ed.* 2000/*Muhammed Ali Mazidi, Janice Gillispie Mazidi*（80x86 IBM PC 及兼容计算机卷Ⅰ和卷Ⅱ：汇编语言，设计与接口技术 第 3 版 1020 页）
3. Principles of Distributed Database Systems 2nd *ed.* 1999/*M. Tamer Özsu, Patrick Valduriez*（分布式数据库系统原理 第 2 版 688 页）
4. Network Security Essentials: Applications and Standards 2000/ *William Stallings*（网络安全基础教程 382 页）
5. Cryptography and Network Security: Principles and Practice 2nd *ed.* 1999/*William Stallings*（密码学与网络安全：原理与实践 第 2 版 590 页）
6. Data Structures and Algorithm Analysis in C++ 2nd *ed.* 1999/*Mark Allen Weiss*（数据结构与算法分析 C++描述 第 2 版 606 页）
7. PCI-X System Architecture 2001/*Tom Shanley*（PCI-X 系统的体系结构 734 页）
8. Introduction to Automata Theory, Languages, and Computation 2nd *ed.* 2001/*John E. Hopcroft, Rajeev Motwani, Jeffrey D. Ullman*（自动机理论、语言和计算导论 第 2 版 535 页）
9. Operating Systems: A Systematic View 5th *ed.* 2001/*William S. Davis, T. M. Rajkumar*（操作系统实践与应用 第 5 版 636 页）
10. Introduction to Logic Design 2002/*Alan B. Marcovitz*（逻辑设计基础 584 页）

CONTENTS