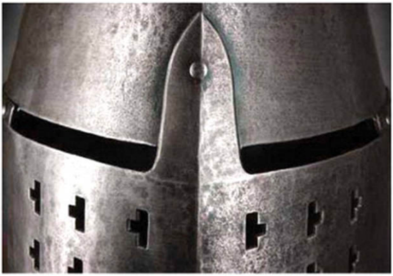

# Cryptography and Network Security

## Principles and Practice

Sixth Edition

William Stallings

## ONLINE ACCESS *for Cryptography and Network Security: Princip* *and Practice,* Sixth Edition

Thank you for purchasing a new copy of ***Cryptography and Network Security:*** ***Principles and Practice,* Sixth Edition**. Your textbook includes six months of p access to the book's Premium Web site. This prepaid subscription provides you access to the following student support areas:

- VideoNotes are step-by-step video tutorials specifically designed to en programming concepts presented in this textbook
- Online Chapters
- Online Appendices
- Supplemental homework problems with solutions
- Supplemental papers for reading

Note that this prepaid subscription does not include access to MyProgrammingLal available at http://www.myprogramminglab.com for purchase.

Use a coin to scratch off the coating and reveal your student access co
Do not use a knife or other sharp object as it may damage the code

To access the ***Cryptography and Network Security: Principles and Practice,* Sixth** Premium Web site for the first time, you will need to register online using a compu an Internet connection and a web browser. The process takes just a couple of minu only needs to be completed once.

1. Go to **http://www.pearsonhighered.com/stallings/**
2. Click on **Premium Web site**.
3. Click on the **Register** button.
4. On the registration page, enter your student access code* found beneath scratch-off panel. Do not type the dashes. You can use lower- or upperca
5. Follow the on-screen instructions. If you need help at any time during th

*This page intentionally left blank*

# CRYPTOGRAPHY AND NETWORK SECURITY

## *PRINCIPLES AND PRACTICE*

## SIXTH EDITION

**William Stallings**

*For Tricia never dull never boring*
*the smartest and bravest*
*person I know*

**Editorial Director, ECS:** Marcia Horton
**Executive Editor:** Tracy Johnson
**Associate Editor:** Carole Snyder
**Director of Marketing:** Christy Lesko
**Marketing Manager:** Yez Alayan
**Director of Production:** Erin Gregg
**Managing Editor:** Scott Disanno
**Associate Managing Editor:** Robert Engelhardt
**Production Manager:** Pat Brown
**Art Director:** Jayne Conte
**Cover Designer:** Bruce Kenselaar

**Permissions Supervisor:** Michael Jo
**Permissions Administrator:** Jenell
**Director, Image Asset Services:** Ar
**Manager, Visual Research:** Karen
**Cover Photo:** © Valery Sibrikov/Fo
**Media Project Manager:** Renata B
**Full-Service Project Management:**
Integra Software Services Pvt. Lt
**Composition:** Integra Software Ser
**Printer/Binder:** Courier Westford
**Cover Printer:** Lehigh-Phoenix

Credits and acknowledgments borrowed from other sources and reproduced, with permission
appear in the Credits section in the end matter of this text.

**Copyright © 2014, 2011, 2006 Pearson Education, Inc.,** All rights reserved. Printed in the Unite
This publication is protected by Copyright, and permission should be obtained from the publis
prohibited reproduction, storage in a retrieval system, or transmission in any form or by any m
mechanical, photocopying, recording, or likewise. To obtain permission(s) to use material from
submit a written request to Pearson Education, Inc., Permissions Department, One Lake Stree
River, New Jersey 07458, or you may fax your request to 201-236-3290.

Many of the designations by manufacturers and sellers to distinguish their products are claimed a
those designations appear in this book, and the publisher was aware of a trademark claim, the de
printed in initial caps or all caps.

**Library of Congress Cataloging-in-Publication Data on file.**

# CONTENTS

**Notation xi**

**Preface xiii**

**Chapter 0 Guide for Readers and Instructors 1**

0.1 Outline of This Book 2
0.2 A Roadmap for Readers and Instructors 3
0.3 Internet and Web Resources 4
0.4 Standards 5

**Chapter 1 Overview 7**

1.1 Computer Security Concepts 9
1.2 The OSI Security Architecture 14
1.3 Security Attacks 15
1.4 Security Services 17
1.5 Security Mechanisms 20
1.6 A Model for Network Security 22
1.7 Recommended Reading 24
1.8 Key Terms, Review Questions, and Problems 25

**PART ONE SYMMETRIC CIPHERS 27**

**Chapter 2 Classical Encryption Techniques 27**

2.1 Symmetric Cipher Model 28
2.2 Substitution Techniques 34
2.3 Transposition Techniques 49
2.4 Rotor Machines 50
2.5 Steganography 52
2.6 Recommended Reading 54
2.7 Key Terms, Review Questions, and Problems 55

**Chapter 3 Block Ciphers and the Data Encryption Standard 61**

3.1 Traditional Block Cipher Structure 63
3.2 The Data Encryption Standard 72
3.3 A DES Example 74

**4.3** Modular Arithmetic 91
**4.4** Groups, Rings, and Fields 99
**4.5** Finite Fields of the Form GF(*p*) 102
**4.6** Polynomial Arithmetic 106
**4.7** Finite Fields of the Form GF($2^n$) 112
**4.8** Recommended Reading 124
**4.9** Key Terms, Review Questions, and Problems 124
Appendix 4A The Meaning of mod 127

**Chapter 5 Advanced Encryption Standard 129**

**5.1** Finite Field Arithmetic 130
**5.2** AES Structure 132
**5.3** AES Transformation Functions 137
**5.4** AES Key Expansion 148
**5.5** An AES Example 151
**5.6** AES Implementation 155
**5.7** Recommended Reading 159
**5.8** Key Terms, Review Questions, and Problems 160
Appendix 5A Polynomials with Coefficients in GF($2^8$) 162
Appendix 5B Simplified AES 164

**Chapter 6 Block Cipher Operation 174**

**6.1** Multiple Encryption and Triple DES 175
**6.2** Electronic Code book 180
**6.3** Cipher Block Chaining Mode 183
**6.4** Cipher Feedback Mode 185
**6.5** Output Feedback Mode 187
**6.6** Counter Mode 189
**6.7** XTS-AES Mode for Block-Oriented Storage Devices 191
**6.8** Recommended Reading 198
**6.9** Key Terms, Review Questions, and Problems 198

**Chapter 7 Pseudorandom Number Generation and Stream Ciphers 202**

**7.1** Principles of Pseudorandom Number Generation 203
**7.2** Pseudorandom Number Generators 210
**7.3** Pseudorandom Number Generation Using a Block Cipher 213
**7.4** Stream Ciphers 219
**7.5** RC4 221

8.5 Discrete Logarithms 244
8.6 Recommended Reading 249
8.7 Key Terms, Review Questions, and Problems 250

**Chapter 9 Public-Key Cryptography and RSA 253**

9.1 Principles of Public-Key Cryptosystems 256
9.2 The RSA Algorithm 264
9.3 Recommended Reading 278
9.4 Key Terms, Review Questions, and Problems 279
Appendix 9A The Complexity of Algorithms 283

**Chapter 10 Other Public-Key Cryptosystems 286**

10.1 Diffie-Hellman Key Exchange 287
10.2 Elgamal Cryptographic System 292
10.3 Elliptic Curve Arithmetic 295
10.4 Elliptic Curve Cryptography 303
10.5 Pseudorandom Number Generation Based on an Asymmetric Ciphe
10.6 Recommended Reading 309
10.7 Key Terms, Review Questions, and Problems 309

**PART THREE CRYPTOGRAPHIC DATA INTEGRITY ALGORITH**

**Chapter 11 Cryptographic Hash Functions 313**

11.1 Applications of Cryptographic Hash Functions 315
11.2 Two Simple Hash Functions 320
11.3 Requirements and Security 322
11.4 Hash Functions Based on Cipher Block Chaining 328
11.5 Secure Hash Algorithm (SHA) 329
11.6 SHA-3 339
11.7 Recommended Reading 351
11.8 Key Terms, Review Questions, and Problems 351

**Chapter 12 Message Authentication Codes 355**

12.1 Message Authentication Requirements 357
12.2 Message Authentication Functions 357
12.3 Requirements for Message Authentication Codes 365
12.4 Security of MACs 367
12.5 MACs Based on Hash Functions: HMAC 368

13.4 NIST Digital Signature Algorithm 401
13.5 Elliptic Curve Digital Signature Algorithm 404
13.6 RSA-PSS Digital Signature Algorithm 407
13.7 Recommended Reading 412
13.8 Key Terms, Review Questions, and Problems 412

PART FOUR MUTUAL TRUST 417

Chapter 14 Key Management and Distribution 417

14.1 Symmetric Key Distribution Using Symmetric Encryption 418
14.2 Symmetric Key Distribution Using Asymmetric Encryption 427
14.3 Distribution of Public Keys 430
14.4 X.509 Certificates 435
14.5 Public-Key Infrastructure 443
14.6 Recommended Reading 445
14.7 Key Terms, Review Questions, and Problems 446

Chapter 15 User Authentication 450

15.1 Remote User-Authentication Principles 451
15.2 Remote User-Authentication Using Symmetric Encryption 454
15.3 Kerberos 458
15.4 Remote User Authentication Using Asymmetric Encryption 476
15.5 Federated Identity Management 478
15.6 Personal Identity Verification 484
15.7 Recommended Reading 491
15.8 Key Terms, Review Questions, and Problems 491

PART FIVE NETWORK AND INTERNET SECURITY 495

Chapter 16 Network Access Control and Cloud Security 495

16.1 Network Access Control 496
16.2 Extensible Authentication Protocol 499
16.3 IEEE 802.1X Port-Based Network Access Control 503
16.4 Cloud Computing 505
16.5 Cloud Security Risks and Countermeasures 512
16.6 Data Protection in the Cloud 514
16.7 Cloud Security as a Service 517
16.8 Recommended Reading 520

**Chapter 18 Wireless Network Security 558**

**18.1** Wireless Security 559
**18.2** Mobile Device Security 562
**18.3** IEEE 802.11 Wireless LAN Overview 566
**18.4** IEEE 802.11i Wireless LAN Security 572
**18.5** Recommended Reading 586
**18.6** Key Terms, Review Questions, and Problems 587

**Chapter 19 Electronic Mail Security 590**

**19.1** Pretty Good Privacy 591
**19.2** S/MIME 599
**19.3** DomainKeys Identified Mail 615
**19.4** Recommended Reading 622
**19.5** Key Terms, Review Questions, and Problems 622
Appendix 19A Radix-64 Conversion 623

**Chapter 20 IP Security 626**

**20.1** IP Security Overview 628
**20.2** IP Security Policy 632
**20.3** Encapsulating Security Payload 638
**20.4** Combining Security Associations 645
**20.5** Internet Key Exchange 649
**20.6** Cryptographic Suites 657
**20.7** Recommended Reading 659
**20.8** Key Terms, Review Questions, and Problems 659

**APPENDICES 661**

**Appendix A Projects for Teaching Cryptography and Network Securi**

**A.1** Sage Computer Algebra Projects 662
**A.2** Hacking Project 663
**A.3** Block Cipher Projects 664
**A.4** Laboratory Exercises 664
**A.5** Research Projects 664
**A.6** Programming Projects 665
**A.7** Practical Security Assessments 665
**A.8** Firewall Projects 666
**A.9** Case Studies 666

A.9 Case Studies 666
A.10 Writing Assignments 666
A.11 Reading/Report Assignments 667
A.12 Discussion Topics 667

## Appendix B Sage Examples 668

B.1 Linear Algebra and Matrix Functionality 669
B.2 Chapter 2: Classical Encryption 670
B.3 Chapter 3: Block Ciphers and the Data Encryption Standard 673
B.4 Chapter 4: Basic Concepts in Number Theory and Finite Fields 677
B.5 Chapter 5: Advanced Encryption Standard 684