

GLOBAL
EDITION



CRYPTOGRAPHY AND NETWORK SECURITY

Principles and Practice

EIGHTH EDITION

WILLIAM STALLINGS



CRYPTOGRAPHY AND NETWORK SECURITY ***PRINCIPLES AND PRACTICE***

EIGHTH EDITION

GLOBAL EDITION

William Stallings



Cryptography and Network Security: Principles and Practice, Global Edition

Table of Contents

Cover

Title Page

Copyright

Dedication

Contents

Notation

Preface

About the Author

Part One: Background

Chapter 1. Information and Network Security Concepts

1.1 Cybersecurity, Information Security, and Network Security

1.2 The OSI Security Architecture

1.3 Security Attacks

1.4 Security Services

1.5 Security Mechanisms

1.6 Cryptography

1.7 Network Security

1.8 Trust and Trustworthiness

1.9 Standards

1.10 Key Terms, Review Questions, and Problems

Chapter 2. Introduction to Number Theory

2.1 Divisibility and the Division Algorithm

Table of Contents

- 2.2 The Euclidean Algorithm
- 2.3 Modular Arithmetic
- 2.4 Prime Numbers
- 2.5 Fermats and Eulers Theorems
- 2.6 Testing for Primality
- 2.7 The Chinese Remainder Theorem
- 2.8 Discrete Logarithms
- 2.9 Key Terms, Review Questions, and Problems
- Appendix 2A The Meaning of Mod

Part Two: Symmetric Ciphers

Chapter 3. Classical Encryption Techniques

- 3.1 Symmetric Cipher Model
- 3.2 Substitution Techniques
- 3.3 Transposition Techniques
- 3.4 Key Terms, Review Questions, and Problems

Chapter 4. Block Ciphers and the Data Encryption Standard

- 4.1 Traditional Block Cipher Structure
- 4.2 The Data Encryption Standard
- 4.3 A DES Example
- 4.4 The Strength of DES
- 4.5 Block Cipher Design Principles
- 4.6 Key Terms, Review Questions, and Problems

Chapter 5. Finite Fields

- 5.1 Groups
- 5.2 Rings
- 5.3 Fields
- 5.4 Finite Fields of the Form $GF(p)$
- 5.5 Polynomial Arithmetic
- 5.6 Finite Fields of the Form $GF(2^n)$

Table of Contents

5.7 Key Terms, Review Questions, and Problems

Chapter 6. Advanced Encryption Standard

6.1 Finite Field Arithmetic

6.2 AES Structure

6.3 AES Transformation Functions

6.4 AES Key Expansion

6.5 An AES Example

6.6 AES Implementation

6.7 Key Terms, Review Questions, and Problems

Appendix 6A Polynomials with Coefficients in GF(28)

Chapter 7. Block Cipher Operation

7.1 Multiple Encryption and Triple DES

7.2 Electronic CodeBook

7.3 Cipher Block Chaining Mode

7.4 Cipher Feedback Mode

7.5 Output Feedback Mode

7.6 Counter Mode

7.7 XTS-AES Mode for Block-Oriented Storage Devices

7.8 Format-Preserving Encryption

7.9 Key Terms, Review Questions, and Problems

Chapter 8. Random Bit Generation and Stream Ciphers

8.1 Principles of Pseudorandom Number Generation

8.2 Pseudorandom Number Generators

8.3 Pseudorandom Number Generation Using a Block Cipher

8.4 Stream Ciphers

8.5 RC4

8.6 Stream Ciphers Using Feedback Shift Registers

8.7 True Random Number Generators

8.8 Key Terms, Review Questions, and Problems

Table of Contents

Part Three: Asymmetric Ciphers

Chapter 9. Public-Key Cryptography and RSA

- 9.1 Principles of Public-Key Cryptosystems
- 9.2 The RSA Algorithm
- 9.3 Key Terms, Review Questions, and Problems

Chapter 10. Other Public-Key Cryptosystems

- 10.1 DiffieHellman Key Exchange
- 10.2 Elgamal Cryptographic System
- 10.3 Elliptic Curve Arithmetic
- 10.4 Elliptic Curve Cryptography
- 10.5 Key Terms, Review Questions, and Problems

Part Four: Cryptographic Data Integrity Algorithms

Chapter 11. Cryptographic Hash Functions

- 11.1 Applications of Cryptographic Hash Functions
- 11.2 Two Simple Hash Functions
- 11.3 Requirements and Security
- 11.4 Secure Hash Algorithm (SHA)
- 11.5 SHA-3
- 11.6 Key Terms, Review Questions, and Problems

Chapter 12. Message Authentication Codes

- 12.1 Message Authentication Requirements
- 12.2 Message Authentication Functions
- 12.3 Requirements for Message Authentication Codes
- 12.4 Security of MACs
- 12.5 MACs Based on Hash Functions: HMAC
- 12.6 MACs Based on Block Ciphers: DAA and CMAC
- 12.7 Authenticated Encryption: CCM and GCM
- 12.8 Key Wrapping
- 12.9 Pseudorandom Number Generation Using Hash Functions and MACs

Table of Contents

12.10 Key Terms, Review Questions, and Problems

Chapter 13. Digital Signatures

13.1 Digital Signatures

13.2 ElGamal Digital Signature Scheme

13.3 Schnorr Digital Signature Scheme

13.4 NIST Digital Signature Algorithm

13.5 Elliptic Curve Digital Signature Algorithm

13.6 RSA-PSS Digital Signature Algorithm

13.7 Key Terms, Review Questions, and Problems

Chapter 14. Lightweight Cryptography and Post-Quantum Cryptography

14.1 Lightweight Cryptography Concepts

14.2 Lightweight Cryptographic Algorithms

14.3 Post-Quantum Cryptography Concepts

14.4 Post-Quantum Cryptographic Algorithms

14.5 Key Terms and Review Questions

Part Five: Mutual Trust

Chapter 15. Cryptographic Key Management and Distribution

15.1 Symmetric Key Distribution Using Symmetric Encryption

15.2 Symmetric Key Distribution Using Asymmetric Encryption

15.3 Distribution of Public Keys

15.4 X.509 Certificates

15.5 Public-Key Infrastructure

15.6 Key Terms, Review Questions, and Problems

Chapter 16. User Authentication

16.1 Remote User-Authentication Principles

16.2 Remote User-Authentication Using Symmetric Encryption

16.3 Kerberos

16.4 Remote User-Authentication Using Asymmetric Encryption

Table of Contents

16.5 Federated Identity Management

16.6 Key Terms, Review Questions, and Problems

Part Six: Network And Internet Security

Chapter 17. Transport-Level Security

17.1 Web Security Considerations

17.2 Transport Layer Security

17.3 HTTPS

17.4 Secure Shell (SSH)

17.5 Review Questions and Problems

Chapter 18. Wireless Network Security

18.1 Wireless Security

18.2 Mobile Device Security

18.3 IEEE 802.11 Wireless Lan Overview

18.4 IEEE 802.11i Wireless Lan Security

18.5 Key Terms, Review Questions, and Problems

Chapter 19. Electronic Mail Security

19.1 Internet Mail Architecture

19.2 Email Formats

19.3 Email Threats and Comprehensive Email Security

19.4 S/MIME

19.5 DNSSEC

19.6 DNS-Based Authentication of Named Entities

19.7 Sender Policy Framework

19.8 DomainKeys Identified Mail

19.9 Domain-Based Message Authentication, Reporting, and Conformance

19.10 Key Terms, Review Questions, and Problems

Chapter 20. IP Security

20.1 IP Security Overview

20.2 IP Security Policy

Table of Contents

- 20.3 Encapsulating Security Payload
- 20.4 Combining Security Associations
- 20.5 Internet Key Exchange
- 20.6 Key Terms, Review Questions, and Problems

Chapter 21. Network Endpoint Security

- 21.1 Firewalls
- 21.2 Intrusion Detection Systems
- 21.3 Malicious Software
- 21.4 Distributed Denial of Service Attacks
- 21.5 Key Terms, Review Questions, and Problems

Chapter 22. Cloud Security

- 22.1 Cloud Computing
- 22.2 Cloud Security Concepts
- 22.3 Cloud Security Risks and Countermeasures
- 22.4 Cloud Security as a Service
- 22.5 An Open-Source Cloud Security Module
- 22.6 Key Terms and Review Questions

Chapter 23. Internet of Things (IoT) Security

- 23.1 The Internet of Things
- 23.2 IoT Security Concepts and Objectives
- 23.3 An Open-Source IoT Security Module
- 23.4 Key Terms and Review Questions

Appendix A. Basic Concepts from Linear Algebra

- A.1 Operations on Vectors and Matrices
- A.2 Linear Algebra Operations over \mathbb{Z}_n

Appendix B. Measures of Secrecy and Security

- B.1 Conditional Probability
- B.2 Perfect Secrecy
- B.3 Information and Entropy

Table of Contents

B.4 Entropy and Secrecy

B.5 Min-Entropy

Appendix C. Data Encryption Standard

Appendix D. Simplified AES

D.1 Overview

D.2 S-AES Encryption and Decryption

D.3 Key Expansion

D.4 The S-Box

D.5 S-AES Structure

Annex D.1 Arithmetic in $GF(2^4)$

Annex D.2 The Mix Column Function

Appendix E. Mathematical Basis of the Birthday Attack

E.1 Related Problem

E.2 The Birthday Paradox

E.3 Useful Inequality

E.4 The General Case of Duplications

E.5 Overlap Between Two Sets

Glossary

References

Index

Acronyms