

PEARSON SERIES IN COMPUTER NETWORKING AND DISTRIBUTED SYSTEMS

THIRD EDITION

NETWORK SECURITY

PRIVATE Communication in a PUBLIC World

**NEW
CONTENT**

Quantum computing,
post-quantum algorithms,
multiparty computation,
fully homomorphic
encryption,
and more!



CHARLIE KAUFMAN • RADIA PERLMAN
MIKE SPECINER • RAY PERLNER



NETWORK SECURITY

PRIVATE Communication in a PUBLIC World

THIRD EDITION

CHARLIE KAUFMAN • RADIA PERLMAN
MIKE SPECINER • RAY PERLNER

◆ Addison-Wesley

Boston • Columbus • New York • San Francisco • Amsterdam • Cape Town
Dubai • London • Madrid • Milan • Munich • Paris • Montreal • Toronto • Delhi • Mexico City
São Paulo • Sydney • Hong Kong • Seoul • Singapore • Taipei • Tokyo

Network Security: Private Communication in a Public World

Table of Contents

Cover

Contents

Acknowledgments

About the Authors

CHAPTER 1 Introduction

1.1 Opinions, Products

1.2 Roadmap to the Book

1.3 Terminology

1.4 Notation

1.5 Cryptographically Protected Sessions

1.6 Active and Passive Attacks

1.7 Legal Issues

1.7.1 Patents

1.7.2 Government Regulations

1.8 Some Network Basics

1.8.1 Network Layers

1.8.2 TCP and UDP Ports

1.8.3 DNS (Domain Name System)

1.8.4 HTTP and URLs

1.8.5 Web Cookies

1.9 Names for Humans

1.10 Authentication and Authorization

Table of Contents

1.10.1 ACL (Access Control List)

1.10.2 Central Administration/Capabilities

1.10.3 Groups

1.10.4 Cross-Organizational and Nested Groups

1.10.5 Roles

1.11 Malware: Viruses, Worms, Trojan Horses

1.11.1 Where Does Malware Come From?

1.11.2 Virus Checkers

1.12 Security Gateway

1.12.1 Firewall

1.12.2 Application-Level Gateway/Proxy

1.12.3 Secure Tunnels

1.12.4 Why Firewalls Dont Work

1.13 Denial-of-Service (DoS) Attacks

1.14 NAT (Network Address Translation)

1.14.1 Summary

CHAPTER 2 Introduction to Cryptography

2.1 Introduction

2.1.1 The Fundamental Tenet of Cryptography

2.1.2 Keys

2.1.3 Computational Difficulty

2.1.4 To Publish or Not to Publish

2.1.5 Earliest Encryption

2.1.6 One-Time Pad (OTP)

2.2 Secret Key Cryptography

2.2.1 Transmitting Over an Insecure Channel

2.2.2 Secure Storage on Insecure Media

2.2.3 Authentication

2.2.4 Integrity Check

Table of Contents

2.3 Public Key Cryptography

2.3.1 Transmitting Over an Insecure Channel

2.3.2 Secure Storage on Insecure Media

2.3.3 Authentication

2.3.4 Digital Signatures

2.4 Hash Algorithms

2.4.1 Password Hashing

2.4.2 Message Integrity

2.4.3 Message Fingerprint

2.4.4 Efficient Digital Signatures

2.5 Breaking an Encryption Scheme

2.5.1 Ciphertext Only

2.5.2 Known Plaintext

2.5.3 Chosen Plaintext

2.5.4 Chosen Ciphertext

2.5.5 Side-Channel Attacks

2.6 Random Numbers

2.6.1 Gathering Entropy

2.6.2 Generating Random Seeds

2.6.3 Calculating a Pseudorandom Stream from the Seed

2.6.4 Periodic Reseeding

2.6.5 Types of Random Numbers

2.6.6 Noteworthy Mistakes

2.7 Numbers

2.7.1 Finite Fields

2.7.2 Exponentiation

2.7.3 Avoiding a Side-Channel Attack

2.7.4 Types of Elements used in Cryptography

2.7.5 Euclidean Algorithm

Table of Contents

2.7.6 Chinese Remainder Theorem

2.8 Homework

CHAPTER 3 Secret Key Cryptography

3.1 Introduction

3.2 Generic Block Cipher Issues

3.2.1 Blocksize, Keysize

3.2.2 Completely General Mapping

3.2.3 Looking Random

3.3 Constructing a Practical Block Cipher

3.3.1 Per-Round Keys

3.3.2 S-boxes and Bit Shuffles

3.3.3 Feistel Ciphers

3.4 Choosing Constants

3.5 Data Encryption Standard (DES)

3.5.1 DES Overview

3.5.2 The Mangler Function

3.5.3 Undesirable Symmetries

3.5.4 Whats So Special About DES?

3.6 3DES (Multiple Encryption DES)

3.6.1 How Many Encryptions?

3.6.1.1 Encrypting Twice with the Same Key

3.6.1.2 Encrypting Twice with Two Keys

3.6.1.3 Triple Encryption with Only Two Keys

3.6.2 Why EDE Rather Than EEE?

3.7 Advanced Encryption Standard (AES)

3.7.1 Origins of AES

3.7.2 Broad Overview

3.7.3 AES Overview

3.7.4 Key Expansion

Table of Contents

3.7.5 Inverse Rounds

3.7.6 Software Implementations of AES

3.8 RC4

3.9 Homework

CHAPTER 4 Modes of Operation

4.1 Introduction

4.2 Encrypting a Large Message

4.2.1 ECB (Electronic Code Book)

4.2.2 CBC (Cipher Block Chaining)

4.2.2.1 Randomized ECB

4.2.2.2 CBC

4.2.2.3 CBC ThreatModifying Ciphertext Blocks

4.2.3 CTR (Counter Mode)

4.2.3.1 Choosing IVs for CTR Mode

4.2.4 XEX (XOR Encrypt XOR)

4.2.5 XTS (XEX with Ciphertext Stealing)

4.3 Generating MACs

4.3.1 CBC-MAC

4.3.1.1 CBC Forgery Attack

4.3.2 CMAC

4.3.3 GMAC

4.3.3.1 GHASH

4.3.3.2 Transforming GHASH into GMAC

4.4 Ensuring Privacy and Integrity Together

4.4.1 CCM (Counter with CBC-MAC)

4.4.2 GCM (Galois/Counter Mode)

4.5 Performance Issues

4.6 Homework

CHAPTER 5 Cryptographic Hashes

Table of Contents

5.1 Introduction

5.2 The Birthday Problem

5.3 A Brief History of Hash Functions

5.4 Nifty Things to Do with a Hash

5.4.1 Digital Signatures

5.4.2 Password Database

5.4.3 Secure Shorthand of Larger Piece of Data

5.4.4 Hash Chains

5.4.5 Blockchain

5.4.6 Puzzles

5.4.7 Bit Commitment

5.4.8 Hash Trees

5.4.9 Authentication

5.4.10 Computing a MAC with a Hash

5.4.11 HMAC

5.4.12 Encryption with a Secret and a Hash Algorithm

5.5 Creating a Hash Using a Block Cipher

5.6 Construction of Hash Functions

5.6.1 Construction of MD4, MD5, SHA-1 and SHA-2

5.6.2 Construction of SHA-3

5.7 Padding

5.7.1 MD4, MD5, SHA-1, and SHA2-256 Message Padding

5.7.2 SHA-3 Padding Rule

5.8 The Internal Encryption Algorithms

5.8.1 SHA-1 Internal Encryption Algorithm

5.8.2 SHA-2 Internal Encryption Algorithm

5.9 SHA-3 fFunction (Also Known as KECCAK-f)

5.10 Homework

CHAPTER 6 First-Generation Public Key Algorithms

Table of Contents

6.1 Introduction

6.2 Modular Arithmetic

6.2.1 Modular Addition

6.2.2 Modular Multiplication

6.2.3 Modular Exponentiation

6.2.4 Fermats Theorem and Eulers Theorem

6.3 RSA

6.3.1 RSA Algorithm

6.3.2 Why Does RSA Work?

6.3.3 Why Is RSA Secure?

6.3.4 How Efficient Are the RSA Operations?

6.3.4.1 Exponentiating with Big Numbers

6.3.4.2 Generating RSA Keys

6.3.4.3 Why a Non-Prime Has Multiple Square Roots of One

6.3.4.4 Having a Small Constant e

6.3.4.5 Optimizing RSA Private Key Operations

6.3.5 Arcane RSA Threats

6.3.5.1 Smooth Numbers

6.3.5.2 The Cube Root Problem

6.3.6 Public-Key Cryptography Standard (PKCS)

6.3.6.1 Encryption

6.3.6.2 The Million-Message Attack

6.3.6.3 Signing

6.4 Diffie-Hellman

6.4.1 MITM (Meddler-in-the-Middle) Attack

6.4.2 Defenses Against MITM Attack

6.4.3 Safe Primes and the Small-Subgroup Attack

6.4.4 ElGamal Signatures

6.5 Digital Signature Algorithm (DSA)

6.5.1 The DSA Algorithm

Table of Contents

6.5.2 Why Is This Secure?

6.5.3 Per-Message Secret Number

6.6 How Secure Are RSA and Diffie-Hellman?

6.7 Elliptic Curve Cryptography (ECC)

6.7.1 Elliptic Curve Diffie-Hellman (ECDH)

6.7.2 Elliptic Curve Digital Signature Algorithm (ECDSA)

6.8 Homework

CHAPTER 7 Quantum Computing

7.1 What Is a Quantum Computer?

7.1.1 A Preview of the Conclusions

7.1.2 First, What Is a Classical Computer?

7.1.3 Qubits and Superposition

7.1.3.1 Example of a Qubit

7.1.3.2 Multi-Qubit States and Entanglement

7.1.4 States and Gates as Vectors and Matrices

7.1.5 Becoming Superposed and Entangled

7.1.6 Linearity

7.1.6.1 No Cloning Theorem

7.1.7 Operating on Entangled Qubits

7.1.8 Unitarity

7.1.9 Doing Irreversible Operations by Measurement

7.1.10 Making Irreversible Classical Operations Reversible

7.1.11 Universal Gate Sets

7.2 Grover's Algorithm

7.2.1 Geometric Description

7.2.2 How to Negate the Amplitude of $|k\rangle$?

7.2.3 How to Reflect All the Amplitudes Across the Mean

7.2.4 Parallelizing Grover's Algorithm

7.3 Shor's Algorithm

Table of Contents

- 7.3.1 Why Exponentiation mod n Is a Periodic Function
- 7.3.2 How Finding the Period of a mod n Lets You Factor n
- 7.3.3 Overview of Shors Algorithm
- 7.3.4 Converting to the Frequency Graph Introduction
- 7.3.5 The Mechanics of Converting to the Frequency Graph
- 7.3.6 Calculating the Period
- 7.3.7 Quantum Fourier Transform

7.4 Quantum Key Distribution (QKD)

- 7.4.1 Why Its Sometimes Called Quantum Encryption
- 7.4.2 Is Quantum Key Distribution Important?

7.5 How Hard Are Quantum Computers to Build?

7.6 Quantum Error Correction

7.7 Homework

CHAPTER 8 Post-Quantum Cryptography

8.1 Signature and/or Encryption Schemes

- 8.1.1 NIST Criteria for Security Levels
- 8.1.2 Authentication
- 8.1.3 Defense Against Dishonest Ciphertext

8.2 Hash-based Signatures

- 8.2.1 Simplest Scheme Signing a Single Bit
- 8.2.2 Signing an Arbitrary-sized Message
- 8.2.3 Signing Lots of Messages
- 8.2.4 Deterministic Tree Generation
- 8.2.5 Short Hashes
- 8.2.6 Hash Chains
- 8.2.7 Standardized Schemes
 - 8.2.7.1 Stateless Schemes

8.3 Lattice-Based Cryptography

- 8.3.1 A Lattice Problem

Table of Contents

8.3.2 Optimization: Matrices with Structure

8.3.3 NTRU-Encryption Family of Lattice Encryption Schemes

8.3.3.1 Bob Computes a (Public, Private) Key Pair

8.3.3.2 How Bob Decrypts to Find m

8.3.3.3 How Does this Relate to Lattices?

8.3.4 Lattice-Based Signatures

8.3.4.1 Basic Idea

8.3.4.2 Insecure Scheme

8.3.4.3 Fixing the Scheme

8.3.5 Learning with Errors (LWE)

8.3.5.1 LWE Optimizations

8.3.5.2 LWE-based NIST Submissions

8.4 Code-based Schemes

8.4.1 Non-cryptographic Error-correcting Codes

8.4.1.1 Invention Step

8.4.1.2 Codeword Creation Step

8.4.1.3 Misfortune Step

8.4.1.4 Diagnosis Step

8.4.2 The Parity-Check Matrix

8.4.3 Cryptographic Public Key Code-based Scheme

8.4.3.1 Niederreiter Optimization

8.4.3.2 Generating a Public Key Pair

8.4.3.3 Using Circulant Matrices

8.5 Multivariate Cryptography

8.5.1 Solving Linear Equations

8.5.2 Quadratic Polynomials

8.5.3 Polynomial Systems

8.5.4 Multivariate Signature Systems

8.5.4.1 Multivariate Public Key Signatures

8.6 Homework

CHAPTER 9 Authentication of People

Table of Contents

9.1 Password-based Authentication

9.1.1 Challenge-Response Based on Password

9.1.2 Verifying Passwords

9.2 Address-based Authentication

9.2.1 Network Address Impersonation

9.3 Biometrics

9.4 Cryptographic Authentication Protocols

9.5 Who Is Being Authenticated?

9.6 Passwords as Cryptographic Keys

9.7 On-Line Password Guessing

9.8 Off-Line Password Guessing

9.9 Using the Same Password in Multiple Places

9.10 Requiring Frequent Password Changes

9.11 Tricking Users into Divulging Passwords

9.12 Lamports Hash

9.13 Password Managers

9.14 Web Cookies

9.15 Identity Providers (IDPs)

9.16 Authentication Tokens

9.16.1 Disconnected Tokens

9.16.2 Public Key Tokens

9.17 Strong Password Protocols

9.17.1 Subtle Details

9.17.2 Augmented Strong Password Protocols

9.17.3 SRP (Secure Remote Password)

9.18 Credentials Download Protocols

9.19 Homework

Table of Contents

CHAPTER 10 Trusted Intermediaries

10.1 Introduction

10.2 Functional Comparison

10.3 Kerberos

10.3.1 KDC Introduces Alice to Bob

10.3.2 Alice Contacts Bob

10.3.3 Ticket Granting Ticket (TGT)

10.3.4 Interrealm Authentication

10.3.5 Making Password-Guessing Attacks Difficult

10.3.6 Double TGT Protocol

10.3.7 Authorization Information

10.3.8 Delegation

10.4 PKI

10.4.1 Some Terminology

10.4.2 Names in Certificates

10.5 Website Gets a DNS Name and Certificate

10.6 PKI Trust Models

10.6.1 Monopoly Model

10.6.2 Monopoly plus Registration Authorities (RAs)

10.6.3 Delegated CAs

10.6.4 Oligarchy

10.6.5 Anarchy Model

10.6.6 Name Constraints

10.6.7 Top-Down with Name Constraints

10.6.8 Multiple CAs for Any Namespace Node

10.6.9 Bottom-Up with Name Constraints

10.6.9.1 Functionality of Up-Links

10.6.9.2 Functionality of Cross-Links

10.6.10 Name Constraints in PKIX Certificates

Table of Contents

10.7 Building Certificate Chains

10.8 Revocation

10.8.1 CRL (Certificate Revocation list)

10.8.2 Online Certificate Status Protocol (OCSP)

10.8.3 Good-Lists vs. Bad-Lists

10.9 Other Information in a PKIX Certificate

10.10 Issues with Expired Certificates

10.11 DNSSEC (DNS Security Extensions)

10.12 Homework

CHAPTER 11 Communication Session Establishment

11.1 One-way Authentication of Alice

11.1.1 Timestamps vs. Challenges

11.1.2 One-Way Authentication of Alice using a Public Key

11.2 Mutual Authentication

11.2.1 Reflection Attack

11.2.2 Timestamps for Mutual Authentication

11.3 Integrity/Encryption for Data

11.3.1 Session Key Based on Shared Secret Credentials

11.3.2 Session Key Based on Public Key Credentials

11.3.3 Session Key Based on One-Party Public Keys

11.4 Nonce Types

11.5 Intentional MITM

11.6 Detecting MITM

11.7 What Layer?

11.8 Perfect Forward Secrecy

11.9 Preventing Forged Source Addresses

11.9.1 Allowing Bob to Be Stateless in TCP

11.9.2 Allowing Bob to Be Stateless in IPsec

Table of Contents

- 11.10 Endpoint Identifier Hiding
- 11.11 Live Partner Reassurance
- 11.12 Arranging for Parallel Computation
- 11.13 Session Resumption/Multiple Sessions
- 11.14 Plausible Deniability
- 11.15 Negotiating Crypto Parameters
 - 11.15.1 Suites vs. à la Carte
 - 11.15.2 Downgrade Attack
- 11.16 Homework

CHAPTER 12 IPsec

- 12.1 IPsec Security Associations
 - 12.1.1 Security Association Database
 - 12.1.2 Security Policy Database
 - 12.1.3 IKE-SAs and Child-SAs
- 12.2 IKE (Internet Key Exchange Protocol)
- 12.3 Creating a Child-SA
- 12.4 AH and ESP
 - 12.4.1 ESP Integrity Protection
 - 12.4.2 Why Protect the IP Header?
 - 12.4.3 Tunnel, Transport Mode
 - 12.4.4 IPv4 Header
 - 12.4.5 IPv6 Header
- 12.5 AH (Authentication Header)
- 12.6 ESP (Encapsulating Security Payload)
- 12.7 Comparison of Encodings
- 12.8 Homework

CHAPTER 13 SSL/TLS and SSH

Table of Contents

13.1 Using TCP

13.2 StartTLS

13.3 Functions in the TLS Handshake

13.4 TLS 1.2 (and Earlier) Basic Protocol

13.5 TLS 1.3

13.7 PKI as Deployed by TLS

13.6 Session Resumption

13.8 SSH (Secure Shell)

13.8.1 SSH Authentication

13.8.2 SSH Port Forwarding

13.9 Homework

CHAPTER 14 Electronic Mail Security

14.1 Distribution Lists

14.2 Store and Forward

14.3 Disguising Binary as Text

14.4 HTML-Formatted Email

14.5 Attachments

14.6 Non-cryptographic Security Features

14.6.1 Spam Defenses

14.7 Malicious Links in Email

14.8 Data Loss Prevention (DLP)

14.9 Knowing Bobs Email Address

14.10 Self-Destruct, Do-Not-Forward,

14.11 Preventing Spoofing of From Field

14.12 In-Flight Encryption

14.13 End-to-End Signed and Encrypted Email

14.14 Encryption by a Server

Table of Contents

- 14.15 Message Integrity
- 14.16 Non-Repudiation
- 14.17 Plausible Deniability
- 14.18 Message Flow Confidentiality
- 14.19 Anonymity
- 14.20 Homework

CHAPTER 15 Electronic Money

- 15.1 ECASH
- 15.2 Offline eCash
 - 15.2.1 Practical Attacks
- 15.3 Bitcoin
 - 15.3.1 Transactions
 - 15.3.2 Bitcoin Addresses
 - 15.3.3 Blockchain
 - 15.3.4 The Ledger
 - 15.3.5 Mining
 - 15.3.6 Blockchain Forks
 - 15.3.7 Why Is Bitcoin So Energy-Intensive?
 - 15.3.8 Integrity Checks: Proof of Work vs. Digital Signatures
 - 15.3.9 Concerns
- 15.4 Wallets for Electronic Currency
- 15.5 Homework

CHAPTER 16 Cryptographic Tricks

- 16.1 Secret Sharing
- 16.2 Blind Signature
- 16.3 Blind Decryption
- 16.4 Zero-Knowledge Proofs

Table of Contents

16.4.1 Graph Isomorphism ZKP

16.4.2 Proving Knowledge of a Square Root

16.4.3 Noninteractive ZKP

16.5 Group Signatures

16.5.1 Trivial Group Signature Schemes

16.5.1.1 Single Shared Key

16.5.1.2 Group Membership Certificate

16.5.1.3 Multiple Group Membership Certificates

16.5.1.4 Blindly Signed Multiple Group Membership Certificates

16.5.2 Ring Signatures

16.5.3 DAA (Direct Anonymous Attestation)

16.5.4 EPID (Enhanced Privacy ID)

16.6 Circuit Model

16.7 Secure Multiparty Computation (MPC)

16.8 Fully Homomorphic Encryption (FHE)

16.8.1 Bootstrapping

16.8.2 Easy-to-Understand Scheme

16.9 Homework

CHAPTER 17 Folklore

17.1 Misconceptions

17.2 Perfect Forward Secrecy

17.3 Change Encryption Keys Periodically

17.4 Don't Encrypt without Integrity Protection

17.5 Multiplexing Flows over One Secure Session

17.5.1 The Splicing Attack

17.5.2 Service Classes

17.5.3 Different Cryptographic Algorithms

17.6 Using Different Secret Keys

17.6.1 For Initiator and Responder in Handshake

Table of Contents

17.6.2 For Encryption and Integrity

17.6.3 In Each Direction of a Secure Session

17.7 Using Different Public Keys

17.7.1 Use Different Keys for Different Purposes

17.7.2 Different Keys for Signing and Encryption

17.8 Establishing Session Keys

17.8.1 Have Both Sides Contribute to the Master Key

17.8.2 Dont Let One Side Determine the Key

17.9 Hash in a Constant When Hashing a Password

17.10 HMAC Rather than Simple Keyed Hash

17.11 Key Derivation

17.12 Use of Nonces in Protocols

17.13 Creating an Unpredictable Nonce

17.14 Compression

17.15 Minimal vs. Redundant Designs

17.16 Overestimate the Size of Key

17.17 Hardware Random Number Generators

17.18 Put Checksums at the End of Data

17.19 Forward Compatibility

17.19.1 Options

17.19.2 Version Numbers

17.19.2.1 Version Number Field Must Not Move

17.19.2.2 Negotiating Highest Version Supported

17.19.2.3 Minor Version Number Field

Glossary

A

B

C

Table of Contents

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Z

Math

M.1 Introduction

M.2 Some definitions and notation

M.3 Arithmetic

M.4 Abstract Algebra

Table of Contents

M.5 Modular Arithmetic

M.5.1 How Do Computers Do Arithmetic?

M.5.2 Computing Inverses in Modular Arithmetic

M.5.2.1 The Euclidean Algorithm

M.5.2.2 The Chinese Remainder Theorem

M.5.3 How Fast Can We Do Arithmetic?

M.6 Groups

M.7 Fields

M.7.1 Polynomials

M.7.2 Finite Fields

M.7.2.1 What Sizes Can Finite Fields Be?

M.7.2.2 Representing a Field

M.8 Mathematics of Rijndael

M.8.1 A Rijndael Round

M.9 Elliptic Curve Cryptography

M.10 Rings

M.11 Linear Transformations

M.12 Matrix Arithmetic

M.12.1 Permutations

M.12.2 Matrix Inverses

M.12.2.1 Gaussian Elimination

M.13 Determinants

M.13.1 Properties of Determinants

M.13.1.1 Adjugate of a Matrix

M.13.2 Proof: Determinant of Product is Product of Determinants

M.14 Homework

Bibliography

Index

Table of Contents