



Applied Cryptography, Second Edition: Protocols, Algorithms, and Source Code in C
by Bruce Schneier
Wiley Computer Publishing, John Wiley & Sons, Inc.
ISBN: 0471128457 Pub Date: 01/01/96

Foreword By Whitfield Diffie

Preface

About the Author

Chapter 1—Foundations

- 1.1 Terminology**
- 1.2 Steganography**
- 1.3 Substitution Ciphers and Transposition Ciphers**
- 1.4 Simple XOR**
- 1.5 One-Time Pads**
- 1.6 Computer Algorithms**
- 1.7 Large Numbers**

Part I—Cryptographic Protocols

Chapter 2—Protocol Building Blocks

- 2.1 Introduction to Protocols**
- 2.2 Communications Using Symmetric Cryptography**
- 2.3 One-Way Functions**
- 2.4 One-Way Hash Functions**
- 2.5 Communications Using Public-Key Cryptography**
- 2.6 Digital Signatures**
- 2.7 Digital Signatures with Encryption**
- 2.8 Random and Pseudo-Random-Sequence Generation**

Chapter 3—Basic Protocols

- 3.1 Key Exchange**
- 3.2 Authentication**
- 3.3 Authentication and Key Exchange**
- 3.4 Formal Analysis of Authentication and Key-Exchange Protocols**
- 3.5 Multiple-Key Public-Key Cryptography**
- 3.6 Secret Splitting**
- 3.7 Secret Sharing**
- 3.8 Cryptographic Protection of Databases**

Chapter 4—Intermediate Protocols

- 4.1 Timestamping Services**
- 4.2 Subliminal Channel**
- 4.3 Undeniable Digital Signatures**
- 4.4 Designated Confirmer Signatures**
- 4.5 Proxy Signatures**
- 4.6 Group Signatures**
- 4.7 Fail-Stop Digital Signatures**
- 4.8 Computing with Encrypted Data**
- 4.9 Bit Commitment**
- 4.10 Fair Coin Flips**
- 4.11 Mental Poker**
- 4.12 One-Way Accumulators**
- 4.13 All-or-Nothing Disclosure of Secrets**

4.14 Key Escrow

Chapter 5—Advanced Protocols

5.1 Zero-Knowledge Proofs

5.2 Zero-Knowledge Proofs of Identity

5.3 Blind Signatures

5.4 Identity-Based Public-Key Cryptography

5.5 Oblivious Transfer

5.6 Oblivious Signatures

5.7 Simultaneous Contract Signing

5.8 Digital Certified Mail

5.9 Simultaneous Exchange of Secrets

Chapter 6—Esoteric Protocols

6.1 Secure Elections

6.2 Secure Multiparty Computation

6.3 Anonymous Message Broadcast

6.4 Digital Cash

Part II—Cryptographic Techniques

Chapter 7—Key Length

7.1 Symmetric Key Length

7.2 Public-Key Key Length

7.3 Comparing Symmetric and Public-Key Key Length

7.4 Birthday Attacks against One-Way Hash Functions

7.5 How Long Should a Key Be?

7.6 Caveat Emptor

Chapter 8—Key Management

8.1 Generating Keys

8.2 Nonlinear Keyspaces

8.3 Transferring Keys

8.4 Verifying Keys

8.5 Using Keys

8.6 Updating Keys

8.7 Storing Keys

8.8 Backup Keys

8.9 Compromised Keys

8.10 Lifetime of Keys

8.11 Destroying Keys

8.12 Public-Key Key Management

Chapter 9—Algorithm Types and Modes

9.1 Electronic Codebook Mode

9.2 Block Replay

9.3 Cipher Block Chaining Mode

9.4 Stream Ciphers

9.5 Self-Synchronizing Stream Ciphers

9.6 Cipher-Feedback Mode

9.7 Synchronous Stream Ciphers

9.8 Output-Feedback Mode

9.9 Counter Mode

9.10 Other Block-Cipher Modes

9.11 Choosing a Cipher Mode

9.12 Interleaving

9.13 Block Ciphers versus Stream Ciphers

Chapter 10—Using Algorithms

- 10.1 Choosing an Algorithm**
- 10.2 Public-Key Cryptography versus Symmetric Cryptography**
- 10.3 Encrypting Communications Channels**
- 10.4 Encrypting Data for Storage**
- 10.5 Hardware Encryption versus Software Encryption**
- 10.6 Compression, Encoding, and Encryption**
- 10.7 Detecting Encryption**
- 10.8 Hiding Ciphertext in Ciphertext**
- 10.9 Destroying Information**

Part III—Cryptographic Algorithms

Chapter 11—Mathematical Background

- 11.1 Information Theory**
- 11.2 Complexity Theory**
- 11.3 Number Theory**
- 11.4 Factoring**
- 11.5 Prime Number Generation**
- 11.6 Discrete Logarithms in a Finite Field**

Chapter 12—Data Encryption Standard (DES)

- 12.1 Background**
- 12.2 Description of DES**
- 12.3 Security of DES**
- 12.4 Differential and Linear Cryptanalysis**
- 12.5 The Real Design Criteria**
- 12.6 DES Variants**
- 12.7 How Secure Is DES Today?**

Chapter 13—Other Block Ciphers

- 13.1 Lucifer**
- 13.2 Madryga**
- 13.3 NewDES**
- 13.4 FEAL**
- 13.5 REDOC**
- 13.6 LOKI**
- 13.7 Khufu and Khafre**
- 13.8 RC2**
- 13.9 IDEA**
- 13.10 MMB**
- 13.11 CA-1.1**
- 13.12 Skipjack**

Chapter 14—Still Other Block Ciphers

- 14.1 GOST**
- 14.2 CAST**
- 14.3 Blowfish**
- 14.4 SAFER**
- 14.5 3-Way**
- 14.6 Crab**
- 14.7 SXAL8/MBAL**
- 14.8 RC5**
- 14.9 Other Block Algorithms**
- 14.10 Theory of Block Cipher Design**
- 14.11 Using one-Way Hash Functions**

14.12 Choosing a Block Algorithm

Chapter 15—Combining Block Ciphers

15.1 Double Encryption

15.2 Triple Encryption

15.3 Doubling the Block Length

15.4 Other Multiple Encryption Schemes

15.5 CDMF Key Shortening

15.6 Whitening

15.7 Cascading Multiple Block Algorithms

15.8 Combining Multiple Block Algorithms

Chapter 16—Pseudo-Random-Sequence Generators and Stream Ciphers

16.1 Linear Congruential Generators

16.2 Linear Feedback Shift Registers

16.3 Design and Analysis of Stream Ciphers

16.4 Stream Ciphers Using LFSRs

16.5 A5

16.6 Hughes XPD/KPD

16.7 Nanoteq

16.8 Rambutan

16.9 Additive Generators

16.10 Gifford

16.11 Algorithm M

16.12 PKZIP

Chapter 17—Other Stream Ciphers and Real Random-Sequence Generators

17.1 RC4

17.2 SEAL

17.3 WAKE

17.4 Feedback with Carry Shift Registers

17.5 Stream Ciphers Using FCSRs

17.6 Nonlinear-Feedback Shift Registers

17.7 Other Stream Ciphers

17.8 System-Theoretic Approach to Stream-Cipher Design

17.9 Complexity-Theoretic Approach to Stream-Cipher Design

17.10 Other Approaches to Stream-Cipher Design

17.11 Cascading Multiple Stream Ciphers

17.12 Choosing a Stream Cipher

17.13 Generating Multiple Streams from a Single Pseudo-Random-Sequence Generator

17.14 Real Random-Sequence Generators

Chapter 18—One-Way Hash Functions

18.1 Background

18.2 Snefru

18.3 N- Hash

18.4 MD4

18.5 MD5

18.6 MD2

18.7 Secure Hash Algorithm (SHA)

18.8 RIPE-MD

18.9 HAVAL

18.10 Other One-Way Hash Functions

18.11 One-Way Hash Functions Using Symmetric Block Algorithms

18.12 Using Public-Key Algorithms

18.13 Choosing a One-Way Hash Function

- 18.14 Message Authentication Codes
- Chapter 19—Public-Key Algorithms**
 - 19.1 Background
 - 19.2 Knapsack Algorithms
 - 19.3 RSA
 - 19.4 Pohlig-Hellman
 - 19.5 Rabin
 - 19.6 ElGamal
 - 19.7 McEliece
 - 19.8 Elliptic Curve Cryptosystems
 - 19.9 LUC
 - 19.10 Finite Automaton Public-Key Cryptosystems
- Chapter 20—Public-Key Digital Signature Algorithms**
 - 20.1 Digital Signature Algorithm (DSA)
 - 20.2 DSA Variants
 - 20.3 Gost Digital Signature Algorithm
 - 20.4 Discrete Logarithm Signature Schemes
 - 20.5 Ong-Schnorr-Shamir
 - 20.6 ESIGN
 - 20.7 Cellular Automata
 - 20.8 Other Public-Key Algorithms
- Chapter 21—Identification Schemes**
 - 21.1 Feige-Fiat-Shamir
 - 21.2 Guillou-Quisquater
 - 21.3 Schnorr
 - 21.4 Converting Identification Schemes to Signature Schemes
- Chapter 22—Key-Exchange Algorithms**
 - 22.1 Diffie-Hellman
 - 22.2 Station-to-Station Protocol
 - 22.3 Shamir's Three-Pass Protocol
 - 22.4 COMSET
 - 22.5 Encrypted Key Exchange
 - 22.6 Fortified Key Negotiation
 - 22.7 Conference Key Distribution and Secret Broadcasting
- Chapter 23—Special Algorithms for Protocols**
 - 23.1 Multiple-Key Public-Key Cryptography
 - 23.2 Secret-Sharing Algorithms
 - 23.3 Subliminal Channel
 - 23.4 Undeniable Digital Signatures
 - 23.5 Designated Confirmer Signatures
 - 23.6 Computing with Encrypted Data
 - 23.7 Fair Coin Flips
 - 23.8 One-Way Accumulators
 - 23.9 All-or-Nothing Disclosure of Secrets
 - 23.10 Fair and Failsafe Cryptosystems
 - 23.11 Zero-Knowledge Proofs of Knowledge
 - 23.12 Blind Signatures
 - 23.13 Oblivious Transfer
 - 23.14 Secure Multiparty Computation
 - 23.15 Probabilistic Encryption
 - 23.16 Quantum Cryptography

Part IV—The Real World

Chapter 24—Example Implementations

- 24.1 IBM Secret-Key Management Protocol**
- 24.2 MITRENET**
- 24.3 ISDN**
- 24.4 STU-III**
- 24.5 Kerberos**
- 24.6 KryptoKnight**
- 24.7 SESAME**
- 24.8 IBM Common Cryptographic Architecture**
- 24.9 ISO Authentication Framework**
- 24.10 Privacy-Enhanced Mail (PEM)**
- 24.11 Message Security Protocol (MSP)**
- 24.12 Pretty Good Privacy (PGP)**
- 24.13 Smart Cards**
- 24.14 Public-Key Cryptography Standards (PKCS)**
- 24.15 Universal Electronic Payment System (UEPS)**
- 24.16 Clipper**
- 24.17 Capstone**
- 24.18 AT&T Model 3600 Telephone Security Device (TSD)**

Chapter 25—Politics

- 25.1 National Security Agency (NSA)**
- 25.2 National Computer Security Center (NCSC)**
- 25.3 National Institute of Standards and Technology (NIST)**
- 25.4 RSA Data Security, Inc.**
- 25.5 Public Key Partners**
- 25.6 International Association for Cryptologic Research (IACR)**
- 25.7 RACE Integrity Primitives Evaluation (RIPE)**
- 25.8 Conditional Access for Europe (CAFE)**
- 25.9 ISO/IEC 9979**
- 25.10 Professional, Civil Liberties, and Industry Groups**
- 25.11 Sci.crypt**
- 25.12 Cypherpunks**
- 25.13 Patents**
- 25.14 U.S. Export Rules**
- 25.15 Foreign Import and Export of Cryptography**
- 25.16 Legal Issues**

Afterword by Matt Blaze

Part V—Source Code

References

Index

Foreword By Whitfield Diffie

The literature of cryptography has a curious history. Secrecy, of course, has always played a central role, but until the First World War, important developments appeared in print in a more or less timely fashion and the field moved forward in much the same way as other specialized disciplines. As late as 1918, one of the most influential cryptanalytic papers of the twentieth century, William F. Friedman's monograph *The Index of Coincidence and Its Applications in Cryptography*, appeared as a