

*"... the best introduction  
to cryptography I've  
ever seen.... The book  
the National Security  
Agency wanted never  
to be published...."*

*—Wired Magazine*

**SECOND  
EDITION**

# **APPLIED CRYPTOGRAPHY**



**Protocols, Algorithms,  
and Source Code in C**

**BRUCE SCHNEIER**

<b>APPLIED CRYPTOGRAPHY .....</b>	<b>2</b>
Errata .....	3
Contents in Brief.....	6
Contents .....	7
<b>PART V SOURCE CODE .....</b>	<b>14</b>
Foreword .....	15
Preface .....	19
<b>How TO READ THIS BOOK .....</b>	<b>20</b>
Acknowledgments .....	22
About the Author .....	23

*from reviews of the first edition of*  
**APPLIED CRYPTOGRAPHY**  
**Protocols, Algorithms, and Source Code in C**

... the definitive text on the subject. . . .”

**-Software Development Magazine**

... good reading for anyone interested in cryptography.”

**-BYTE**

“This book should be on the shelf of any computer professional involved in the use or implementation of cryptography.”

**-IEEE Software**

“... dazzling . . . fascinating. . . . This book **absolutely must** be on your bookshelf . . . .”

**-PC Techniques**

“... comprehensive . . . an encyclopedic work . . . .”

**-The Cryptogram**

“... a fantastic book on cryptography today. It belongs in the library of anyone interested in cryptography or anyone who deals with information security and cryptographic systems.”

**-Computers & Security**

“An encyclopedic survey . . . could well have been subtitled ‘The Joy of Encrypting’ . . . a useful addition to the library of any active or would-be security practitioner.”

**-Cryptologia**

“... encyclopedic . . . readable . . . well-informed . . . picks up where Dorothy Denning’s classic **Cryptography and Data Security** left off a dozen years ago. . . . This book would be a bargain at twice the price.”

**--;login:**

“This is a marvelous resource-the best book on cryptography and its application available today.”

**-Dorothy Denning**  
Georgetown University

“... Schneier’s book is an indispensable reference and resource. . . . I recommend it highly.”

**-Martin Hellman**  
Stanford University

## **Errata**

A list of the errors found in this book along with corresponding corrections is updated periodically. For the most recent electronic version, send email to:

`schneier@counterpane.com`

For the most recent printed version, send a stamped, self-addressed envelope to:

AC Corrections  
Counterpane Systems  
101 E. Minnekaka Parkway  
Minneapolis, MN 55419

Readers are encouraged to distribute electronic or printed versions of this list to other readers of this book.

Publisher: Katherine Schowalter  
Editor: Phil Sutherland  
Assistant Editor: Allison Roarty  
Managing Editor: Robert Aronds  
Text Design & Composition: North Market Street Graphics

Designations used by companies to distinguish their products are often claimed as trademarks. In all instances where John Wiley & Sons, Inc. is aware of a claim, the product names appear in initial capital or all capital letters. Readers, however, should contact the appropriate companies for more complete information regarding trademarks and registration.

This text is printed on acid-free paper.

Copyright © 1996 by Bruce Schneier  
Published by John Wiley & Sons, Inc.

All rights reserved. Published simultaneously in Canada.

This publication is designed to provide accurate and authoritative information in regard to the subject matter covered. It is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional service. If legal advice or other expert assistance is required, the services of a competent professional person should be sought.

In no event will the publisher or author be liable for any consequential, incidental, or indirect damages (including damages for loss of business profits, business interruption, loss of business information, and the like) arising from the use or inability to use the protocols and algorithms in this book, even if the publisher or author has been advised of the possibility of such damages.

Some of the protocols and algorithms in this book are protected by patents and copyrights. It is the responsibility of the reader to obtain all necessary patent and copyright licenses before implementing in software any protocol or algorithm in this book. This book does not contain an exhaustive list of all applicable patents and copyrights.

Some of the protocols and algorithms in this book are regulated under the United States Department of State International Traffic in Arms Regulations. It is the responsibility of the reader to obtain all necessary export licenses before implementing in software for export any protocol or algorithm in this book.

Reproduction or translation of any part of this work beyond that permitted by section 107 or 108 of the 1976 United States Copyright Act without the permission of the copyright owner is unlawful. Requests for permission or further information should be addressed to the Permissions Department, John Wiley & Sons, Inc.

***Library of Congress Cataloging-in-Publication Data:***

Schneier, Bruce

Applied Cryptography Second Edition : protocols, algorithms, and source code in C  
/ Bruce Schneier.

Includes bibliographical references (p. 675).

ISBN 0-471-12845-7 (cloth : acid-free paper). - ISBN

0-471-1 1709-9 (paper : acid-free paper)

1. Computer security. 2. Telecommunication-Security measures.

3. Cryptography. I. Title.

QA76.9.A25S35 1996

005.8'2-dc20

95-12398

CIP

Printed in the United States of America

1 0 9 8 7 6 5

# Contents in Brief

Foreword by Whitfield Diffie

Preface

About the Author

## 1 Foundations

### **Part I Cryptographic Protocols**

2 Protocol Building Blocks

3 Basic Protocols

4 Intermediate Protocols

5 Advanced Protocols

6 Esoteric Protocols

### **Part II Cryptographic Techniques**

7 Key Length

8 Key Management

9 Algorithm Types and Modes

10 Using Algorithms

### **Part III Cryptographic Algorithms**

11 Mathematical Background

12 Data Encryption Standard (DES)

13 Other Block Ciphers

14 Still Other Block Ciphers

15 Combining Block Ciphers

16 Pseudo-Random-Sequence Generators and Stream Ciphers

17 Other Stream Ciphers and Real Random-Sequence Generators

18 One-Way Hash Functions

19 Public-Key Algorithms

20 Public-Key Digital Signature Algorithms

21 Identification Schemes

22 Key-Exchange Algorithms

23 Special Algorithms for Protocols

### **Part IV The Real World**

24 Example Implementations

25 Politics

Afterword by Matt Blaze

### **Part V Source Code**

References

# Contents

**Foreword by Whitfield Diffie xv**

**Preface xix**

**How TO READ THIS BOOK xx**

**ACKNOWLEDGMENTS xxii**

**About the Author xxiii**

## **1 FOUNDATIONS 1**

- 1.1 TERMINOLOGY 1**
- 1.2 STEGANOGRAPHY 9**
- 1.3 SUBSTITUTION CIPHERS AND TRANSPOSITION CIPHERS 10**
- 1.4 SIMPLE XOR 13**
- 1.5 ONE-TIME PADS 15**
- 1.6 COMPUTER ALGORITHMS 17**
- 1.7 LARGE NUMBERS 17**

## **PART I CRYPTOGRAPHIC PROTOCOLS**

### **2 PROTOCOL BUILDING BLOCKS 21**

- 2.1 INTRODUCTION TO PROTOCOLS 21**
- 2.2 COMMUNICATIONS USING SYMMETRIC CRYPTOGRAPHY 28**
- 2.3 ONE-WAY FUNCTIONS 29**
- 2.4 ONE-WAY HASH FUNCTIONS 30**
- 2.5 COMMUNICATIONS USING PUBLIC-KEY CRYPTOGRAPHY 31**
- 2.6 DIGITAL SIGNATURES 34**
- 2.7 DIGITAL SIGNATURES WITH ENCRYPTION 41**
- 2.8 RANDOM AND PSEUDO-RANDOM-SEQUENCE GENERATION 44**

**3 BASIC PROTOCOLS 47**

- 3.1** KEY EXCHANGE **47**
- 3.2** AUTHENTICATION **52**
- 3.3** AUTHENTICATION AND KEY EXCHANGE **56**
- 3.4** FORMAL ANALYSIS OF AUTHENTICATION AND KEY-EXCHANGE PROTOCOLS **65**
- 3.5** MULTIPLE-KEY PUBLIC-KEY CRYPTOGRAPHY **68**
- 3.6** SECRET SPLITTING **70**
- 3.7** SECRET SHARING **71**
- 3.8** CRYPTOGRAPHIC PROTECTION OF DATABASES **73**

**4 INTERMEDIATE PROTOCOLS 75**

- 4.1** TIMESTAMPING SERVICES **75**
- 4.2** SUBLIMINAL CHANNEL **79**
- 4.3** UNDENIABLE DIGITAL SIGNATURES **81**
- 4.4** DESIGNATED CONFIRMER SIGNATURES **82**
- 4.5** PROXY SIGNATURES **83**
- 4.6** GROUP SIGNATURES **84**
- 4.7** FAIL-STOP DIGITAL SIGNATURES **85**
- 4.8** COMPUTING WITH ENCRYPTED DATA **85**
- 4.9** BIT COMMITMENT **86**
- 4.10** FAIR COIN FLIPS **89**
- 4.11** MENTAL POKER **92**
- 4.12** ONE-WAY ACCUMULATORS **95**
- 4.13** ALL-OR-NOTHING DISCLOSURE OF SECRETS **96**
- 4.14** KEY ESCROW **97**

**5 ADVANCED PROTOCOLS 101**

- 5.1** ZERO-KNOWLEDGE PROOFS **101**
- 5.2** ZERO-KNOWLEDGE PROOFS OF IDENTITY **109**
- 5.3** BLIND SIGNATURES **112**
- 5.4** IDENTITY-BASED PUBLIC-KEY CRYPTOGRAPHY **115**
- 5.5** OBLIVIOUS TRANSFER **116**
- 5.6** OBLIVIOUS SIGNATURES **117**
- 5.7** SIMULTANEOUS CONTRACT SIGNING **118**
- 5.8** DIGITAL CERTIFIED MAIL **122**
- 5.9** SIMULTANEOUS EXCHANGE OF SECRETS **123**

**6 ESOTERIC PROTOCOLS 125**

- 6.1** SECURE ELECTIONS **125**
- 6.2** SECURE MULTIPARTY COMPUTATION **134**
- 6.3** ANONYMOUS MESSAGE BROADCAST **137**
- 6.4** DIGITAL CASH **139**



## **PART II CRYPTOGRAPHIC TECHNIQUES**

### **7 KEY LENGTH 151**

- 7.1 SYMMETRIC KEY LENGTH 151**
- 7.2 PUBLIC-KEY KEY LENGTH 158**
- 7.3 COMPARING SYMMETRIC AND PUBLIC-KEY KEY LENGTH 165**
- 7.4 BIRTHDAY ATTACKS AGAINST ONE-WAY HASH FUNCTIONS 165**
- 7.5 HOW LONG SHOULD A KEY BE? 166**
- 7.6 CAVEAT EMPTOR 168**

### **8 KEY MANAGEMENT 169**

- 8.1 GENERATING KEYS 170**
- 8.2 NONLINEAR KEYSACES 175**
- 8.3 TRANSFERRING KEYS 176**
- 8.4 VERIFYING KEYS 178**
- 8.5 USING KEYS 179**
- 8.6 UPDATING KEYS 180**
- 8.7 STORING KEYS 180**
- 8.8 BACKUP KEYS 181**
- 8.9 COMPROMISED KEYS 182**
- 8.10 LIFETIME OF KEYS 183**
- 8.11 DESTROYING KEYS 184**
- 8.12 PUBLIC-KEY KEY MANAGEMENT 185**

### **9 ALGORITHM TYPES AND MODES 189**

- 9.1 ELECTRONIC CODEBOOK MODE 189**
- 9.2 BLOCK REPLAY 191**
- 9.3 CIPHER BLOCK CHAINING MODE 293**
- 9.4 STREAM CIPHERS 197**
- 9.5 SELF-SYNCHRONIZING STREAM CIPHERS 198**
- 9.6 CIPHER-FEEDBACK MODE 200**
- 9.7 SYNCHRONOUS STREAM CIPHERS 202**
- 9.8 OUTPUT-FEEDBACK MODE 203**
- 9.9 COUNTER MODE 205**
- 9.10 OTHER BLOCK-CIPHER MODES 206**
- 9.11 CHOOSING A CIPHER MODE 208**
- 9.12 INTERLEAVING 210**
- 9.13 BLOCK CIPHERS VERSUS STREAM CIPHERS 210**

### **10 USING ALGORITHMS 213**

- 10.1 CHOOSING AN ALGORITHM 214**
- 10.2 PUBLIC-KEY CRYPTOGRAPHY VERSUS SYMMETRIC CRYPTOGRAPHY 216**
- 10.3 ENCRYPTING COMMUNICATIONS CHANNELS 216**
- 10.4 ENCRYPTING DATA FOR STORAGE 220**
- 10.5 HARDWARE ENCRYPTION VERSUS SOFTWARE ENCRYPTION 223**

- 10.6** COMPRESSION, ENCODING, AND ENCRYPTION **226**
- 10.7** DETECTING ENCRYPTION **226**
- 10.8** HIDING CIPHERTEXT IN CIPHERTEXT **227**
- 10.9** DESTROYING INFORMATION **228**

### **PART III CRYPTOGRAPHIC ALGORITHMS**

#### **11 MATHEMATICAL BACKGROUND 233**

- 11.1** INFORMATION THEORY **233**
- 11.2** COMPLEXITY THEORY **237**
- 11.3** NUMBER THEORY **242**
- 11.4** FACTORING **255**
- 11.5** PRIME NUMBER GENERATION **258**
- 11.6** DISCRETE LOGARITHMS IN A FINITE FIELD **261**

#### **12 DATA ENCRYPTION STANDARD (DES) 265**

- 12.1** BACKGROUND **265**
- 12.2** DESCRIPTION OF DES **270**
- 12.3** SECURITY OF DES **278**
- 12.4** DIFFERENTIAL AND LINEAR CRYPTANALYSIS **285**
- 12.5** THE REAL DESIGN CRITERIA **293**
- 12.6** DES VARIANTS **294**
- 12.7** How SECURE Is DES TODAY? **300**

#### **13 OTHER BLOCK CIPHERS 303**

- 13.1** LUCIFER **303**
- 13.2** MADRYGA **304**
- 13.3** NEWDES **306**
- 13.4** FEAL **308**
- 13.5** REDOC **311**
- 13.6** LOKI **314**
- 13.7** KHUFU AND KHAFRE **316**
- 13.8** RC2 **318**
- 13.9** IDEA **319**
- 13.10** MMB **325**
- 13.11** CA-1.1 **327**
- 13.12** SKIPJACK **328**

#### **14 STILL OTHER BLOCK CIPHERS 331**

- 14.1** GOST **331**
- 14.2** CAST **334**
- 14.3** BLOWFISH **336**
- 14.4** SAFER **339**
- 14.5** 3-WAY **341**

<b>14.6</b>	<b>CRAB</b>	<b>342</b>
<b>14.7</b>	<b>SXAL8/MBAL</b>	<b>344</b>
<b>14.8</b>	<b>RC5</b>	<b>344</b>
<b>14.9</b>	OTHER BLOCK ALGORITHMS	<b>346</b>
<b>14.10</b>	THEORY OF BLOCK CIPHER DESIGN	<b>346</b>
<b>14.11</b>	USING ONE-WAY HASH FUNCTIONS	351
<b>14.12</b>	CHOOSING A BLOCK ALGORITHM	354
<b>15 COMBINING BLOCK CIPHERS</b>		<b>357</b>
<b>15.1</b>	DOUBLE ENCRYPTION	<b>357</b>
<b>15.2</b>	TRIPLE ENCRYPTION	<b>358</b>
<b>15.3</b>	DOUBLING THE BLOCK LENGTH	<b>363</b>
<b>15.4</b>	OTHER MULTIPLE ENCRYPTION SCHEMES	<b>363</b>
<b>15.5</b>	<b>CDMF</b> KEY SHORTENING	<b>366</b>
<b>15.6</b>	WHITENING	<b>366</b>
<b>15.7</b>	CASCADING MULTIPLE BLOCK ALGORITHMS	<b>367</b>
<b>15.8</b>	COMBINING MULTIPLE BLOCK ALGORITHMS	<b>368</b>
<b>16 PSEUDO-RANDOM-SEQUENCE GENERATORS AND STREAM CIPHERS</b>		<b>369</b>
<b>16.1</b>	LINEAR CONGRUENTIAL GENERATORS	<b>369</b>
<b>16.2</b>	LINEAR FEEDBACK SHIFT REGISTERS	<b>372</b>
<b>16.3</b>	DESIGN AND ANALYSIS OF STREAM CIPHERS	<b>379</b>
<b>16.4</b>	STREAM CIPHERS USING <b>LFSRs</b>	<b>381</b>
<b>16.5</b>	<b>A5</b>	<b>389</b>
<b>16.6</b>	HUGHES <b>XPD/KPD</b>	<b>389</b>
<b>16.7</b>	<b>NANOTEQ</b>	<b>390</b>
<b>16.8</b>	<b>RAMBUTAN</b>	<b>390</b>
<b>16.9</b>	ADDITIVE GENERATORS	<b>390</b>
<b>16.10</b>	<b>GIFFORD</b>	<b>392</b>
<b>16.11</b>	ALGORITHM <b>M</b>	<b>393</b>
<b>16.12</b>	<b>PKZIP</b>	<b>394</b>
<b>17 OTHER STREAM CIPHERS AND REAL RANDOM-SEQUENCE GENERATORS</b>		<b>397</b>
<b>17.1</b>	<b>RC4</b>	<b>397</b>
<b>17.2</b>	<b>SEAL</b>	<b>398</b>
<b>17.3</b>	<b>WAKE</b>	<b>400</b>
<b>17.4</b>	FEEDBACK WITH CARRY SHIFT REGISTERS	<b>402</b>
<b>17.5</b>	STREAM CIPHERS USING <b>FCSRs</b>	<b>405</b>
<b>17.6</b>	NONLINEAR-FEEDBACK <b>SHIFT</b> REGISTERS	<b>412</b>
<b>17.7</b>	OTHER STREAM CIPHERS	413
<b>17.8</b>	SYSTEM-THEORETIC APPROACH TO STREAM-CIPHER DESIGN	<b>415</b>
<b>17.9</b>	COMPLEXITY-THEMATIC APPROACH TO STREAM-CIPHER DESIGN	<b>416</b>
<b>17.10</b>	OTHER APPROACHES TO STREAM-CIPHER DESIGN	418

<b>17.11</b>	<b>CASCADING MULTIPLE STREAM CIPHERS</b>	<b>419</b>
<b>17.12</b>	<b>CHOOSING A STREAM CIPHER</b>	<b>420</b>
<b>17.13</b>	<b>GENERATING MULTIPLE STREAMS FROM A SINGLE PSEUDO-RANDOM-SEQUENCE GENERATOR</b>	<b>420</b>
<b>17.14</b>	<b>REAL RANDOM-SEQUENCE GENERATORS</b>	<b>421</b>
 <b>18 ONE-WAY HASH FUNCTIONS 429</b>		
<b>18.1</b>	<b>BACKGROUND</b>	<b>429</b>
<b>18.2</b>	<b>SNEFRU</b>	<b>431</b>
<b>18.3</b>	<b>N-HASH</b>	<b>432</b>
<b>18.4</b>	<b>MD4</b>	<b>435</b>
<b>18.5</b>	<b>MD5</b>	<b>436</b>
<b>18.6</b>	<b>MD2</b>	<b>441</b>
<b>18.7</b>	<b>SECURE HASH ALGORITHM (SHA)</b>	<b>441</b>
<b>18.8</b>	<b>RIPE-MD</b>	<b>445</b>
<b>18.9</b>	<b>HAVAL</b>	<b>445</b>
<b>18.10</b>	<b>OTHER ONE-WAY HASH FUNCTIONS</b>	<b>446</b>
<b>18.11</b>	<b>ONE-WAY HASH FUNCTIONS USING SYMMETRIC BLOCK ALGORITHMS</b>	<b>446</b>
<b>18.12</b>	<b>USING PUBLIC-KEY ALGORITHMS</b>	<b>455</b>
<b>18.13</b>	<b>CHOOSING A ONE-WAY HASH FUNCTION</b>	<b>455</b>
<b>18.14</b>	<b>MESSAGE AUTHENTICATION CODES</b>	<b>455</b>
 <b>19 PUBLIC-KEY ALGORITHMS 461</b>		
<b>19.1</b>	<b>BACKGROUND</b>	<b>461</b>
<b>19.2</b>	<b>KNAPSACK ALGORITHMS</b>	<b>462</b>
<b>19.3</b>	<b>RSA</b>	<b>466</b>
<b>19.4</b>	<b>POHLIG-HELLMAN</b>	<b>474</b>
<b>19.5</b>	<b>RABIN</b>	<b>475</b>
<b>19.6</b>	<b>ELGAMAL</b>	<b>476</b>
<b>19.7</b>	<b>McELIECE</b>	<b>479</b>
<b>19.8</b>	<b>ELLIPTIC CURVE CRYPTOSYSTEMS</b>	<b>480</b>
<b>19.9</b>	<b>LUC</b>	<b>481</b>
<b>19.10</b>	<b>FINITE AUTOMATON PUBLIC-KEY CRYPTOSYSTEMS</b>	<b>482</b>
 <b>20 PUBLIC-KEY DIGITAL SIGNATURE ALGORITHMS 483</b>		
<b>20.1</b>	<b>DIGITAL SIGNATURE ALGORITHM (DSA)</b>	<b>483</b>
<b>20.2</b>	<b>DSA VARIANTS</b>	<b>494</b>
<b>20.3</b>	<b>GOST DIGITAL SIGNATURE ALGORITHM</b>	<b>495</b>
<b>20.4</b>	<b>DISCRETE LOGARITHM SIGNATURE SCHEMES</b>	<b>496</b>
<b>20.5</b>	<b>ONG-SCHNORR-SHAMIR</b>	<b>498</b>
<b>20.6</b>	<b>ESIGN</b>	<b>499</b>
<b>20.7</b>	<b>CELLULAR AUTOMATA</b>	<b>500</b>
<b>20.8</b>	<b>OTHER PUBLIC-KEY ALGORITHMS</b>	<b>500</b>
 <b>21 IDENTIFICATION SCHEMES 503</b>		
<b>21.1</b>	<b>FEIGE-FIAT-SHAMIR</b>	<b>503</b>

<b>21.2</b>	<b>GUILLOU-QUISQUATER</b>	<b>508</b>
<b>21.3</b>	<b>SCHNORR</b>	<b>510</b>
<b>21.4</b>	<b>CONVERTING IDENTIFICATION SCHEMES TO SIGNATURE SCHEMES</b>	<b>512</b>

## **22 KEY-EXCHANGE ALGORITHMS 513**

<b>22.1</b>	<b>DIFFIE-HELLMAN</b>	<b>513</b>
<b>22.2</b>	<b>STATION-TO-STATION PROTOCOL</b>	<b>516</b>
<b>22.3</b>	<b>SHAMIR'S THREE-PASS PROTOCOL</b>	<b>516</b>
<b>22.4</b>	<b>COMSET</b>	<b>517</b>
<b>22.5</b>	<b>ENCRYPTED KEY EXCHANGE</b>	<b>518</b>
<b>22.6</b>	<b>FORTIFIED KEY NEGOTIATION</b>	<b>522</b>
<b>22.7</b>	<b>CONFERENCE KEY DISTRIBUTION AND SECRET BROADCASTING</b>	<b>523</b>

## **23 SPECIAL ALGORITHMS FOR PROTOCOLS 527**

<b>23.1</b>	<b>MULTIPLE-KEY PUBLIC-KEY CRYPTOGRAPHY</b>	<b>527</b>
<b>23.2</b>	<b>SECRET-SHARING ALGORITHMS</b>	<b>528</b>
<b>23.3</b>	<b>SUBLIMINAL CHANNEL</b>	<b>531</b>
<b>23.4</b>	<b>UNDENIABLE DIGITAL SIGNATURES</b>	<b>536</b>
<b>23.5</b>	<b>DESIGNATED CONFIRMER SIGNATURES</b>	<b>539</b>
<b>23.6</b>	<b>COMPUTING WITH ENCRYPTED DATA</b>	<b>540</b>
<b>23.7</b>	<b>FAIR COIN FLIPS</b>	<b>541</b>
<b>23.8</b>	<b>ONE-WAY ACCUMULATORS</b>	<b>543</b>
<b>23.9</b>	<b>ALL-OR-NOTHING DISCLOSURE OF SECRETS</b>	<b>543</b>
<b>23.10</b>	<b>FAIR AND FAILSAFE CRYPTOSYSTEMS</b>	<b>546</b>
<b>23.11</b>	<b>ZERO-KNOWLEDGE PROOFS OF KNOWLEDGE</b>	<b>548</b>
<b>23.12</b>	<b>BLIND SIGNATURES</b>	<b>549</b>
<b>23.13</b>	<b>OBLMOUS TRANSFER</b>	<b>550</b>
<b>23.14</b>	<b>SECURE MULTIPARTY COMPUTATION</b>	<b>551</b>
<b>23.15</b>	<b>PROBABILISTIC ENCRYPTION</b>	<b>552</b>
<b>23.16</b>	<b>QUANTUM CRYPTOGRAPHY</b>	<b>554</b>

## **PART IV THE REAL WORLD**

### **24 EXAMPLE IMPLEMENTATIONS 561**

<b>24.1</b>	<b>IBM SECRET-KEY MANAGEMENT PROTOCOL</b>	<b>561</b>
<b>24.2</b>	<b>MITRENET</b>	<b>562</b>
<b>24.3</b>	<b>ISDN</b>	<b>563</b>
<b>24.4</b>	<b>STU-III</b>	<b>565</b>
<b>24.5</b>	<b>KERBEROS</b>	<b>566</b>
<b>24.6</b>	<b>KRYPTOKNIGHT</b>	<b>571</b>
<b>24.7</b>	<b>SESAME</b>	<b>572</b>
<b>24.8</b>	<b>IBM COMMON CRYPTOGRAPHIC ARCHITECTURE</b>	<b>573</b>
<b>24.9</b>	<b>ISO AUTHENTICATION FRAMEWORK</b>	<b>574</b>
<b>24.10</b>	<b>PRIVACY-ENHANCED MAIL (PEM)</b>	<b>577</b>
<b>24.11</b>	<b>MESSAGE SECURITY PROTOCOL (MSP)</b>	<b>584</b>

<b>24.12</b>	<b>PRETTY GOOD PRIVACY (PGP)</b>	<b>584</b>
<b>24.13</b>	<b>SMART CARDS</b>	<b>587</b>
<b>24.14</b>	<b>PUBLIC-KEY CRYPTOGRAPHY STANDARDS (PKCS)</b>	<b>588</b>
<b>24.15</b>	<b>UNIVERSAL ELECTRONIC PAYMENT SYSTEM (UEPS)</b>	<b>589</b>
<b>24.16</b>	<b>CLIPPER</b>	<b>591</b>
<b>24.17</b>	<b>CAPSTONE 5</b>	<b>93</b>
<b>24.18</b>	<b>AT&amp;T MODEL 3600 TELEPHONE SECURITY DEVICE (TSD)</b>	<b>594</b>
 <b>25 POLITICS 597</b>		
<b>25.1</b>	<b>NATIONAL SECURITY AGENCY (NSA)</b>	<b>597</b>
<b>25.2</b>	<b>NATIONAL COMPUTER SECURITY CENTER (NCSC)</b>	<b>599</b>
<b>25.3</b>	<b>NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST)</b>	<b>600</b>
<b>25.4</b>	<b>RSA DATA SECURITY, INC.</b>	<b>603</b>
<b>25.5</b>	<b>PUBLIC KEY PARTNERS</b>	<b>604</b>
<b>25.6</b>	<b>INTERNATIONAL ASSOCIATION FOR CRYPTOGRAPHIC RESEARCH (IACR)</b>	<b>605</b>
<b>25.7</b>	<b>RACE INTEGRITY PRIMITIVES EVALUATION (RIPE)</b>	<b>605</b>
<b>25.8</b>	<b>CONDITIONAL ACCESS FOR EUROPE (CAFE)</b>	<b>606</b>
<b>25.9</b>	<b>ISO/IEC 9979</b>	<b>607</b>
<b>25.10</b>	<b>PROFESSIONAL, CIVIL LIBERTIES, AND INDUSTRY GROUPS</b>	<b>608</b>
<b>25.11</b>	<b>SCI.CRYPT</b>	<b>608</b>
<b>25.12</b>	<b>CYPHERPUNKS</b>	<b>609</b>
<b>25.13</b>	<b>PATENTS</b>	<b>609</b>
<b>25.14</b>	<b>U.S. EXPORT RULES</b>	<b>620</b>
<b>25.15</b>	<b>FOREIGN IMPORT AND EXPORT OF CRYPTOGRAPHY</b>	<b>617</b>
<b>25.16</b>	<b>LEGAL ISSUES</b>	<b>618</b>

***Afterword by Matt Blaze 619***

## PART V SOURCE CODE

***Source Code 623***

***References 675***

# 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 research report of the private Riverbank Laboratories [577]. And this, despite the fact that the work had been done as part of the war effort. In the same year Edward H. Hebern of Oakland, California filed the first patent for a rotor machine [710], the device destined to be a mainstay of military cryptography for nearly 50 years.

After the First World War, however, things began to change. U.S. Army and Navy organizations, working entirely in secret, began to make fundamental advances in cryptography. During the thirties and forties a few basic papers did appear in the open literature and several treatises on the subject were published, but the latter were farther and farther behind the state of the art. By the end of the war the transition was complete. With one notable exception, the public literature had died. That exception was Claude Shannon's paper "The Communication Theory of Secrecy Systems," which appeared in the ***Bell System Technical Journal*** in 1949 [1432]. It was similar to Friedman's 1918 paper, in that it grew out of wartime work of Shannon's. After the Second World War ended it was declassified, possibly by mistake.

From 1949 until 1967 the cryptographic literature was barren. In that year a different sort of contribution appeared: David Kahn's history, ***The Codebreakers*** [794]. It didn't contain any new technical ideas, but it did contain a remarkably complete history of what had gone before, including mention of some things that the government still considered secret. The significance of ***The Codebreakers*** lay not just in its remarkable scope, but also in the fact that it enjoyed good sales and made tens of thousands of people, who had never given the matter a moment's thought, aware of cryptography. A trickle of new cryptographic papers began to be written.

At about the same time, Horst Feistel, who had earlier worked on identification friend or foe devices for the Air Force, took his lifelong passion for cryptography to the IBM Watson Laboratory in Yorktown Heights, New York. There, he began development of what was to become the U.S. Data Encryption Standard; by the early 1970s several technical reports on this subject by Feistel and his colleagues had been made public by IBM [1482,1484,552].

This was the situation when I entered the field in late 1972. The cryptographic literature wasn't abundant, but what there was included some very shiny nuggets.

Cryptology presents a difficulty not found in normal academic disciplines: the need for the proper interaction of cryptography and cryptanalysis. This arises out of the fact that in the absence of real communications requirements, it is easy to propose a system that appears unbreakable. Many academic designs are so complex that the would-be cryptanalyst doesn't know where to start; exposing flaws in these designs is far harder than designing them in the first place. The result is that the competitive process, which is one strong motivation in academic research, cannot take hold.

When Martin Hellman and I proposed public-key cryptography in 1975 [496], one of the indirect aspects of our contribution was to introduce a problem that does not even appear easy to solve. Now an aspiring cryptosystem designer could produce something that would be recognized as clever-something that did more than just turn meaningful text into nonsense. The result has been a spectacular increase in the number of people working in cryptography, the number of meetings held, and the number of books and papers published.

In my acceptance speech for the Donald E. Fink award-given for the best expository paper to appear in an IEEE journal-which I received jointly with Hellman in 1980, I told the audience that in writing "Privacy and Authentication," I had an experience that I suspected was rare even among the prominent scholars who populate the IEEE awards ceremony: I had written the paper I had wanted to study, but could not find, when I first became seriously interested in cryptography. Had I been able to go to the Stanford bookstore and pick up a modern cryptography text, I would probably have learned about the field years earlier. But the only things available in the fall of 1972 were a few classic papers and some obscure technical reports.

The contemporary researcher has no such problem. The problem now is choosing where to start among the thousands of papers and dozens of books. The contemporary researcher, yes, but what about the contemporary programmer or engineer who merely wants to use cryptography? Where does that person turn? Until now, it has been necessary to spend long hours hunting out and then studying the research literature before being able to design the sort of cryptographic utilities glibly described in popular articles.

This is the gap that Bruce Schneier's *Applied Cryptography* has come to fill. Beginning with the objectives of communication security and elementary examples of programs used to achieve these objectives, Schneier gives us a panoramic view of the fruits of 20 years of public research. The title says it all; from the mundane objective of having a secure conversation the very first time you call someone to the possibilities of digital money and cryptographically secure elections, this is where you'll find it.



Not satisfied that the book was about the real world merely because it went all the way down to the code, Schneier has included an account of the world in which cryptography is developed and applied, and discusses entities ranging from the International Association for Cryptologic Research to the NSA.

When public interest in cryptography was just emerging in the late seventies and early eighties, the National Security Agency (NSA), America's official cryptographic organ, made several attempts to quash it. The first was a letter from a long-time NSA employee allegedly, avowedly, and apparently acting on his own. The letter was sent to the IEEE and warned that the publication of cryptographic material was a violation of the International Traffic in Arms Regulations (ITAR). This viewpoint turned out not even to be supported by the regulations themselves—which contained an explicit exemption for published material—but gave both the public practice of cryptography and the 1977 Information Theory Workshop lots of unexpected publicity.

A more serious attempt occurred in 1980, when the NSA funded the American Council on Education to examine the issue with a view to persuading Congress to give it legal control of publications in the field of cryptography. The results fell far short of NSA's ambitions and resulted in a program of voluntary review of cryptographic papers; researchers were requested to ask the NSA's opinion on whether disclosure of results would adversely affect the national interest before publication.

As the eighties progressed, pressure focused more on the practice than the study of cryptography. Existing laws gave the NSA the power, through the Department of State, to regulate the export of cryptographic equipment. As business became more and more international and the American fraction of the world market declined, the pressure to have a single product in both domestic and offshore markets increased. Such single products were subject to export control and thus the NSA acquired substantial influence not only over what was exported, but also over what was sold in the United States.

As this is written, a new challenge confronts the public practice of cryptography. The government has augmented the widely published and available Data Encryption Standard, with a secret algorithm implemented in tamper-resistant chips. These chips will incorporate a codified mechanism of government monitoring. The negative aspects of this "key-escrow" program range from a potentially disastrous impact on personal privacy to the high cost of having to add hardware to products that had previously encrypted in software. So far key escrow products are enjoying less than stellar sales and the scheme has attracted widespread negative comment, especially from the independent cryptographers. Some people, however, see more future in programming than politicking and have redoubled their efforts to provide the world with strong cryptography that is accessible to public scrutiny.

A sharp step back from the notion that export control law could supersede the First Amendment seemed to have been taken in 1980 when the **Federal Register** announcement of a revision to ITAR included the statement: "... provision has been added to make it clear that the regulation of the export of technical data does not purport to interfere with the First Amendment rights of individuals." But the fact that tension between the First Amendment and the export control laws has not

gone away should be evident from statements at a conference held by RSA Data Security. NSA's representative from the export control office expressed the opinion that people who published cryptographic programs were "in a grey area" with respect to the law. If that is so, it is a grey area on which the first edition of this book has shed some light. Export applications for the book itself have been granted, with acknowledgement that published material lay beyond the authority of the Munitions Control Board. Applications to export the enclosed programs on disk, however, have been denied.

The shift in the NSA's strategy, from attempting to control cryptographic research to tightening its grip on the development and deployment of cryptographic products, is presumably due to its realization that all the great cryptographic papers in the world do not protect a single bit of traffic. Sitting on the shelf, this volume may be able to do no better than the books and papers that preceded it, but sitting next to a workstation, where a programmer is writing cryptographic code, it just may.

Whitfield Diffie  
Mountain View, CA

# Preface

There are two kinds of cryptography in this world: cryptography that will stop your kid sister from reading your files, and cryptography that will stop major governments from reading your files. This book is about the latter.

If I take a letter, lock it in a safe, hide the safe somewhere in New York, then tell you to read the letter, that's not security. That's obscurity. On the other hand, if I take a letter and lock it in a safe, and then give you the safe along with the design specifications of the safe and a hundred identical safes with their combinations so that you and the world's best safecrackers can study the locking mechanism-and you still can't open the safe and read the letter-that's security.

For many years, this sort of cryptography was the exclusive domain of the military. The United States' National Security Agency (NSA), and its counterparts in the former Soviet Union, England, France, Israel, and elsewhere, have spent billions of dollars in the very serious game of securing their own communications while trying to break everyone else's. Private individuals, with far less expertise and budget, have been powerless to protect their own privacy against these governments.

During the last 20 years, public academic research in cryptography has exploded. While classical cryptography has been long used by ordinary citizens, computer cryptography was the exclusive domain of the world's militaries since World War II. Today, state-of-the-art computer cryptography is practiced outside the secured walls of the military agencies. The layperson can now employ security practices that can protect against the most powerful of adversaries-security that may protect against military agencies for years to come.

Do average people really need this kind of security? Yes. They may be planning a political campaign, discussing taxes, or having an illicit affair. They may be designing a new product, discussing a marketing strategy, or planning a hostile business takeover. Or they may be living in a country that does not respect the rights of privacy of its citizens. They may be doing something that they feel shouldn't be illegal,

but is. For whatever reason, the data and communications are personal, private, and no one else's business.

This book is being published in a tumultuous time. In 1994, the Clinton administration approved the Escrowed Encryption Standard (including the Clipper chip and Fortezza card) and signed the Digital Telephony bill into law. Both of these initiatives try to ensure the government's ability to conduct electronic surveillance.

Some dangerously Orwellian assumptions are at work here: that the government has the right to listen to private communications, and that there is something wrong with a private citizen trying to keep a secret from the government. Law enforcement has always been able to conduct court-authorized surveillance if possible, but this is the first time that the people have been forced to take active measures to **make themselves available** for surveillance. These initiatives are not simply government proposals in some obscure area; they are preemptive and unilateral attempts to usurp powers that previously belonged to the people.

Clipper and Digital Telephony do not protect privacy; they force individuals to unconditionally trust that the government will respect their privacy. The same law enforcement authorities who illegally tapped Martin Luther King Jr.'s phones can easily tap a phone protected with Clipper. In the recent past, local police authorities have either been charged criminally or sued civilly in numerous jurisdictions—Maryland, Connecticut, Vermont, Georgia, Missouri, and Nevada—for conducting illegal wiretaps. It's a poor idea to deploy a technology that could some day facilitate a police state.

The lesson here is that it is insufficient to protect ourselves with laws; we need to protect ourselves with mathematics. Encryption is too important to be left solely to governments.

This book gives you the tools you need to protect your own privacy; cryptography products may be declared illegal, but the information will never be.

## How to Read This Book

I wrote ***Applied Cryptography*** to be both a lively introduction to the field of cryptography and a comprehensive reference. I have tried to keep the text readable without sacrificing accuracy. This book is not intended to be a mathematical text. Although I have not deliberately given any false information, I do play fast and loose with theory. For those interested in formalism, there are copious references to the academic literature.

Chapter 1 introduces cryptography, defines many terms, and briefly discusses pre-computer cryptography.

Chapters 2 through 6 (Part I) describe cryptographic protocols: what people can do with cryptography. The protocols range from the simple (sending encrypted messages from one person to another) to the complex (flipping a coin over the telephone) to the esoteric (secure and anonymous digital money exchange). Some of these protocols are obvious; others are almost amazing. Cryptography can solve a lot of problems that most people never realized it could.

Chapters 7 through 10 (Part II) discuss cryptographic techniques. All four chapters in this section are important for even the most basic uses of cryptography. Chapters 7 and 8 are about keys: how long a key should be in order to be secure, how to generate keys, how to store keys, how to dispose of keys, and so on. Key management is the hardest part of cryptography and often the Achilles' heel of an otherwise secure system. Chapter 9 discusses different ways of using cryptographic algorithms, and Chapter 10 gives the odds and ends of algorithms: how to choose, implement, and use algorithms.

Chapters 11 through 23 (Part III) list algorithms. Chapter 11 provides the mathematical background. This chapter is only required if you are interested in public-key algorithms. If you just want to implement DES (or something similar), you can skip ahead. Chapter 12 discusses DES: the algorithm, its history, its security, and some variants. Chapters 13, 14, and 15 discuss other block algorithms; if you want something more secure than DES, skip to the section on IDEA and triple-DES. If you want to read about a bunch of algorithms, some of which may be more secure than DES, read the whole chapter. Chapters 16 and 17 discuss stream algorithms. Chapter 18 focuses on one-way hash functions; MD5 and SHA are the most common, although I discuss many more. Chapter 19 discusses public-key encryption algorithms, Chapter 20 discusses public-key digital signature algorithms, Chapter 21 discusses public-key identification algorithms, and Chapter 22 discusses public-key key exchange algorithms. The important algorithms are RSA, DSA, Fiat-Shamir, and Diffie-Hellman, respectively. Chapter 23 has more esoteric public-key algorithms and protocols; the math in this chapter is quite complicated, so wear your seat belt.

Chapters 24 and 25 (Part IV) turn to the real world of cryptography. Chapter 24 discusses some of the current implementations of these algorithms and protocols, while Chapter 25 touches on some of the political issues surrounding cryptography. These chapters are by no means intended to be comprehensive.

Also included are source code listings for 10 algorithms discussed in Part III. I was unable to include all the code I wanted to due to space limitations, and cryptographic source code cannot otherwise be exported. (Amazingly enough, the State Department allowed export of the first edition of this book with source code, but denied export for a computer disk with the exact same source code on it. Go figure.) An associated source code disk set includes much more source code than I could fit in this book; it is probably the largest collection of cryptographic source code outside a military institution. I can only send source code disks to U.S. and Canadian citizens living in the U.S. and Canada, but hopefully that will change someday. If you are interested in implementing or playing with the cryptographic algorithms in this book, get the disk. See the last page of the book for details.

One criticism of this book is that its encyclopedic nature takes away from its readability. This is true, but I wanted to provide a single reference for those who might come across an algorithm in the academic literature or in a product. For those who are more interested in a tutorial, I apologize. A lot is being done in the field; this is the first time so much of it has been gathered between two covers. Even so, space considerations forced me to leave many things out. I covered topics that I felt were important, practical, or interesting. If I couldn't cover a topic in depth, I gave references to articles and papers that did.

I have done my best to hunt down and eradicate all errors in this book, but many have assured me that it is an impossible task. Certainly, the second edition has far fewer errors than the first. An errata listing is available from me and will be periodically posted to the Usenet newsgroup sci.crypt. If any reader finds an error, please let me know. I'll send the first person to find each error in the book a free copy of the source code disk.

### Acknowledgments

The list of people who had a hand in this book may seem unending, but all are worthy of mention. I would like to thank Don Alvarez, Ross Anderson, Dave Balenson, Karl Barrus, Steve Bellovin, Dan Bernstein, Eli Biham, Joan Boyar, Karen Cooper, Whit Diffie, Joan Feigenbaum, Phil Karn, Neal Koblitz, Xuejia Lai, Tom Leranthe, Mike Markowitz, Ralph Merkle, Bill Patton, Peter Pearson, Charles Pfleeger, Ken Pizzini, Bart Preneel, Mark Riordan, Joachim Schurman, and Marc Schwartz for reading and editing all or parts of the first edition; Marc Vauclair for translating the first edition into French; Abe Abraham, Ross Anderson, Dave Banisar, Steve Bellovin, Eli Biham, Matt Bishop, Matt Blaze, Gary Carter, Jan Camenisch, Claude Crepeau, Joan Daemen, Jorge Davila, Ed Dawson, Whit Diffie, Carl Ellison, Joan Feigenbaum, Niels Ferguson, Matt Franklin, Rosario Gennaro, Dieter Gollmann, Mark Goresky, Richard Graveman, Stuart Haber, Jingman He, Bob Hogue, Kenneth Iversen, Markus Jakobsson, Burt Kaliski, Phil Karn, John Kelsey, John Kennedy, Lars Knudsen, Paul Kocher, John Ladwig, Xuejia Lai, Arjen Lenstra, Paul Leyland, Mike Markowitz, Jim Massey, Bruce McNair, William Hugh Murray, Roger Needham, Clif Neuman, Kaisa Nyberg, Luke O'Connor, Peter Pearson, Rene Peralta, Bart Preneel, Yisrael Radai, Matt Robshaw, Michael Roe, Phil Rogaway, Avi Rubin, Paul Rubin, Selwyn Russell, Kazue Sako, Mahmoud Salmasizadeh, Markus Stadler, Dmitry Titov, Jimmy Upton, Marc Vauclair, Serge Vaudénay, Gideon Yuval, Glen Zorn, and several anonymous government employees for reading and editing all or parts of the second edition; Lawrie Brown, Leisa Condie, Joan Daemen, Peter Gutmann, Alan Insley, Chris Johnston, John Kelsey, Xuejia Lai, Bill Leininger, Mike Markowitz, Richard Outerbridge, Peter Pearson, Ken Pizzini, Colin Plumb, RSA Data Security, Inc., Michael Roe, Michael Wood, and Phil Zimmermann for providing source code; Paul MacNerland for creating the figures for the first edition; Karen Cooper for copyediting the second edition; Beth Friedman for proofreading the second edition; Carol Kennedy for indexing the second edition; the readers of sci.crypt and the Cypherpunks mailing list for commenting on ideas, answering questions, and finding errors in the first edition; Randy Seuss for providing Internet access; Jeff Duntemann and Jon Erickson for helping me get started; assorted random Insleys for the impetus, encouragement, support, conversations, friendship, and dinners; and AT&T Bell Labs for firing me and making this all possible. All these people helped to create a far better book than I could have created alone.

Bruce Schneier  
Oak Park, Ill.  
schneier@counterpane.com

# About the Author

BRUCE SCHNEIER is president of Counterpane Systems, an Oak Park, Illinois consulting firm specializing in cryptography and computer security. Bruce is also the author of ***E-Mail Security*** (John Wiley & Sons, 1995) and ***Protect Your Macintosh*** (Peachpit Press, 1994); and has written dozens of articles on cryptography for major magazines. He is a contributing editor to Dr. Dobb's ***Joournal***, where he edits the "Algorithms Alley" column, and a contributing editor to ***Computer and Communications Security Reviews***. Bruce serves on the board of directors of the International Association for Cryptologic Research, is a member of the Advisory Board for the Electronic Privacy Information Center, and is on the program committee for the New Security Paradigms Workshop. In addition, he finds time to give frequent lectures on cryptography, computer security, and privacy.