ARTECH HOUSE

COMPUTER SECURITY SERIES

# *Contemporary* Cryptography

ROLF OPPLIGER

# Contemporary Cryptography

For quite a long time, computer security was a rather narrow field of study that was populated mainly by theoretical computer scientists, electrical engineers, and applied mathematicians. With the proliferation of open systems in general, and of the Internet and the World Wide Web (WWW) in particular, this situation has changed fundamentally. Today, computer and network practitioners are equally interested in computer security, since they require technologies and solutions that can be used to secure applications related to electronic commerce. Against this background, the field of computer security has become very broad and includes many topics of interest. The aim of this series is to publish state-of-the-art, high standard technical books on topics related to computer security. Further information about the series can be found on the WWW at the following URL:

http://www.esecurity.ch/serieseditor.html

Also, if you'd like to contribute to the series by writing a book about a topic related to computer security, feel free to contact either the Commissioning Editor or the Series Editor at Artech House.

For a listing of recent titles in the *Artech House Computer Security Library*,
turn to the back of this book.

# Contemporary Cryptography

Rolf Oppliger

ARTECH
HOUSE
BOSTON | LONDON
artechhouse.com

**Library of Congress Cataloging-in-Publication Data**
Oppliger, Rolf.
Contemporary cryptography/Rolf Oppliger.
p. cm. —(Artech House computer security series)
Includes bibliographical references and index.
ISBN 1-58053-642-5
1. Cryptography. I. Title. II. Series.

Z103.O66 2005 2005043576
652′.8–dc22

**British Library Cataloguing in Publication Data**
Oppliger, Rolf
Contemporary cryptography. —(Artech House computer security series)
1. Data encryption (Computer science) 2. Cryptography
I. Title
005.8′2

ISBN 1-58053-642-5
**Cover design by Yekaterina Ratner**

**© 2005 ARTECH HOUSE, INC.**
**685 Canton Street**
**Norwood, MA 02062**

All rights reserved. Printed and bound in the United States of America. No part of this book may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without permission in writing from the publisher. All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Artech House cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

International Standard Book Number: 1-58053-642-5

10 9 8 7 6 5 4 3 2 1

*To my family*

# Contents


Foreword xv

Preface xix

References xxiii

Acknowledgments xxv

Chapter 1 Introduction 1
1.1 Cryptology 1
1.2 Cryptographic Systems 3
1.2.1 Classes of Cryptographic Systems 7
1.2.2 Secure Cryptographic Systems 8
1.2.3 Side Channel and Related Attacks 12
1.3 Historical Background Information 14
1.4 Outline of the Book 16
References 18

Chapter 2 Cryptographic Systems 21
2.1 Unkeyed Cryptosystems 21
2.1.1 One-Way Functions 21
2.1.2 Cryptographic Hash Functions 23
2.1.3 Random Bit Generators 25
2.2 Secret Key Cryptosystems 26
2.2.1 Symmetric Encryption Systems 27
2.2.2 Message Authentication Codes 28
2.2.3 PRBGs 30
2.2.4 PRFs 31
2.3 Public Key Cryptosystems 32
2.3.1 Asymmetric Encryption Systems 32
2.3.2 DSSs 35

2.3.3 Key Agreement 39
2.3.4 Entity Authentication 41
2.3.5 Secure Multiparty Computation 41
2.4 Final Remarks 42
References 42

**I MATHEMATICAL FUNDAMENTALS 45**

Chapter 3 Discrete Mathematics 47
3.1 Algebraic Basics 47
3.1.1 Preliminary Remarks 48
3.1.2 Algebraic Sructures 51
3.1.3 Homomorphisms and Isomorphisms 60
3.1.4 Permutations 61
3.2 Integer Arithmetic 63
3.2.1 Integer Division 63
3.2.2 Common Divisors and Multiples 65
3.2.3 Euclidean Algorithms 66
3.2.4 Prime Numbers 71
3.2.5 Factorization 77
3.2.6 Euler's Totient Function 79
3.3 Modular Arithmetic 81
3.3.1 Modular Congruence 81
3.3.2 Modular Exponentiation 84
3.3.3 Chinese Remainder Theorem 86
3.3.4 Fermat's Little Theorem 88
3.3.5 Euler's Theorem 89
3.3.6 Finite Fields Modulo Irreducible Polynomials 89
3.3.7 Quadratic Residuosity 91
3.3.8 Blum Integers 98
3.4 Elliptic Curves 99
3.5 Final Remarks 101
References 102

Chapter 4 Probability Theory 103
4.1 Basic Terms and Concepts 103
4.2 Random Variables 109
4.2.1 Probability Distributions 111
4.2.2 Marginal Distributions 113

4.2.3 Conditional Probability Distributions 114
4.2.4 Expectation 115
4.2.5 Independence of Random Variables 117
4.2.6 Markov's Inequality 118
4.2.7 Variance and Standard Deviation 119
4.2.8 Chebyshev's Inequality 121
4.3 Final Remarks 122
References 123

Chapter 5 Information Theory 125
5.1 Introduction 125
5.2 Entropy 129
5.2.1 Joint Entropy 132
5.2.2 Conditional Entropy 133
5.2.3 Mutual Information 135
5.3 Redundancy 136
5.4 Key Equivocation and Unicity Distance 138
5.5 Final Remarks 139
References 140

Chapter 6 Complexity Theory 141
6.1 Preliminary Remarks 141
6.2 Introduction 143
6.3 Asymptotic Order Notation 146
6.4 Efficient Computations 147
6.5 Computational Models 150
6.6 Complexity Classes 154
6.6.1 Complexity Class $\mathcal{P}$ 154
6.6.2 Complexity Classes $\mathcal{NP}$ and co$\mathcal{NP}$ 154
6.6.3 Complexity Class $\mathcal{PP}$ and Its Subclasses 159
6.7 Final Remarks 163
References 164

**II UNKEYED CRYPTOSYSTEMS 167**

Chapter 7 One-Way Functions 169
7.1 Introduction 169
7.2 Candidate One-Way Functions 172
7.2.1 Discrete Exponentiation Function 173
7.2.2 RSA Function 176

7.2.3 Modular Square Function 179
7.3 Integer Factorization Algorithms 180
7.3.1 Special-Purpose Algorithms 181
7.3.2 General-Purpose Algorithms 183
7.3.3 State of the Art 185
7.4 Algorithms for Computing Discrete Logarithms 186
7.4.1 Generic Algorithms 187
7.4.2 Special-Purpose Algorithms 187
7.4.3 State of the Art 188
7.5 Hard-Core Predicates 188
7.6 Elliptic Curve Cryptography 190
7.7 Final Remarks 191
References 192

Chapter 8 Cryptographic Hash Functions 195
8.1 Introduction 195
8.2 Merkle-Damgård Construction 199
8.3 Exemplary Cryptographic Hash Functions 201
8.3.1 MD4 204
8.3.2 MD5 209
8.3.3 SHA-1 211
8.4 Final Remarks 214
References 216

Chapter 9 Random Bit Generators 219
9.1 Introduction 219
9.2 Realizations and Implementations 221
9.2.1 Hardware-Based Random Bit Generators 221
9.2.2 Software-Based Random Bit Generators 222
9.2.3 Deskewing Techniques 223
9.3 Statistical Randomness Testing 223
9.4 Final Remarks 224
References 225

**III SECRET KEY CRYPTOSYSTEMS 227**

Chapter 10 Symmetric Encryption Systems 229
10.1 Introduction 229
10.1.1 Examples 230
10.1.2 Classes of Symmetric Encryption Systems 232

10.1.3 Secure Symmetric Encryption Systems 233
10.1.4 Evaluation Criteria 235
10.2 Block Ciphers 236
10.2.1 DES 238
10.2.2 AES 255
10.2.3 Modes of Operation 269
10.3 Stream Ciphers 277
10.4 Perfectly Secure Encryption 281
10.5 Final Remarks 287
References 288

Chapter 11 Message Authentication Codes 291
11.1 Introduction 291
11.2 Computationally Secure MACs 294
11.2.1 MACs Using Symmetric Encryption Systems 295
11.2.2 MACs Using Keyed Hash Functions 296
11.2.3 MACs Using PRFs 300
11.2.4 MACs Using Families of Universal Hash Functions 304
11.3 Information-Theoretically Secure MACs 305
11.4 Final Remarks 307
References 307

Chapter 12 Pseudorandom Bit Generators 309
12.1 Introduction 309
12.2 Cryptographically Secure PRBG 313
12.2.1 Blum-Micali PRBG 316
12.2.2 RSA PRBG 317
12.2.3 BBS PRBG 317
12.3 Final Remarks 318
References 319

Chapter 13 Pseudorandom Functions 321
13.1 Introduction 321
13.2 Constructions 325
13.2.1 PRF-Based PRBG 325
13.2.2 PRBG-Based PRF 326
13.3 Random Oracle Model 327
13.4 Final Remarks 329
References 229

**IV PUBLIC KEY CRYPTOSYSTEMS 331**

Chapter 14 Asymmetric Encryption Systems 333
14.1 Introduction 333
14.2 Basic Systems 336
14.2.1 RSA 336
14.2.2 Rabin 347
14.2.3 ElGamal 353
14.3 Secure Systems 359
14.3.1 Probabilistic Encryption 359
14.3.2 Optimal Asymmetric Encryption Padding 362
14.4 Identity-Based Encryption 363
14.5 Final Remarks 365
References 365

Chapter 15 Digital Signature Systems 369
15.1 Introduction 369
15.2 Basic Systems 372
15.2.1 RSA 373
15.2.2 ElGamal 378
15.2.3 DSA 384
15.3 Secure Systems 388
15.3.1 PSS 389
15.3.2 PSS-R 391
15.4 One-Time Signature Systems 393
15.5 Digital Signatures for Streams 395
15.6 Variations 399
15.6.1 Blind Signatures 399
15.6.2 Undeniable Signatures 400
15.6.3 Fail-Stop Signatures 400
15.7 Final Remarks 401
References 401

Chapter 16 Key Establishment 405
16.1 Introduction 405
16.2 Key Distribution Protocols 406
16.2.1 Merkle's Puzzles 406
16.2.2 Shamir's Three-Pass Protocol 408
16.2.3 Asymmetric Encryption-Based Key Distribution Protocol 411

16.3 Key Agreement Protocols 411
16.4 Quantum Cryptography 414
16.4.1 Basic Principles 414
16.4.2 Quantum Key Exchange Protocol 416
16.5 Final Remarks 419
References 420

Chapter 17 Entity Authentication 423
17.1 Introduction 423
17.2 Authentication Technologies 424
17.2.1 Proof by Possession 425
17.2.2 Proof by Knowledge 426
17.2.3 Proof by Property 430
17.2.4 Proof by Location 431
17.3 Zero-Knowledge Authentication Protocols 432
17.3.1 Preliminary Remarks 432
17.3.2 Fiat-Shamir 434
17.3.3 Guillou-Quisquater 436
17.3.4 Schnorr 438
17.3.5 Turning Interactive Proofs of Knowledge into DSSs 439
17.4 Final Remarks 440
References 440

Chapter 18 Secure Multiparty Computation 443
18.1 Introduction 443
18.2 Major Results 446
18.3 Final Remarks 446
References 447

**V EPILOGUE 449**

Chapter 19 Key Management 451
19.1 Introduction 451
19.2 Key Life Cycle 453
19.2.1 Key Generation 453
19.2.2 Key Distribution 453
19.2.3 Key Storage 454
19.2.4 Key Destruction 454
19.3 Secret Sharing 455
19.4 Key Recovery 457

19.5 Public Key Infrastructure 460
19.6 Final Remarks 463
References 464

Chapter 20 Conclusions 467
20.1 Unkeyed Cryptosystems 467
20.2 Secret Key Cryptosystems 469
20.3 Public Key Cryptosystems 470
20.4 Final Remarks 471

Chapter 21 Outlook 473
21.1 Theoretical Viewpoint 474
21.2 Practical Viewpoint 476
References 477

Appendix A Abbreviations and Acronyms 479

Appendix B Mathematical Notation 485

About the Author 491

Index 493

# Foreword

Assume for a moment that everything in this book was known for decades but not widely published. If I owned this book in the early 1980s, some governments would consider me dangerous (certainly more dangerous than anyone reasonably considers me now). The reason? Cryptography—the ability to encipher messages—was considered an instrument of war and espionage. Some countries (the USA included) considered export of cryptographic mechanisms to be in the same category of crime as smuggling nuclear weapons! This was despite the fact that cryptology has been studied and practiced for thousands of years around the world.

In 2005, a mere twenty years later, things are somewhat less extreme, and I have shelves full of books on cryptography. However, many governments still fear the spread of encryption and thus severely restrict (or prohibit) its use within their borders. This is despite its regular use billions of times per day in everything from banking networks to medical records to cable TV systems to Internet commerce over the WWW, as well as governmental uses.

Why is knowledge of cryptography so often feared by those in authority? One explanation may be that it is because cryptography can be used to hide criminal behavior, espionage, and political activities. More generally, it helps to remove information from the purview of the state, and this can be threatening to governments whose survival is based on restricting citizens' knowledge. Information can be used or misused in so many ways it is no wonder that protecting it is of widespread interest.

At its heart, cryptography is concerned with information, whether stored as data, or communicated to others. In turn, information and communication undergird nearly everything we do. Commerce is driven by communication of finance and sales, research is based on data acquisition and reference, and government functions on the collection and processing of records. Entertainment is encoded information, whether presented as music, paintings, or the performance of a play. Civilization is enabled by our ability to communicate information to each other, and to store it for later use. Even something as commonplace as currency would be useless unless it conveyed meaning of denomination and validity. Of course, personal relationships

also require some level of communication, too—imagine conveying "I love you" to those people special in your life without any shared means of communication!

At its very heart, life itself is based on information storage and processing: the DNA in genes encodes information governing how organisms are constructed and operate. Recently, there were reports from the world of physics about new conjectures on the permanence of black holes that revolved around their effect on information.[1] Some students of psychology and philosophy believe that consciousness and behavior are predetermined by the events of the past—basically, the complex processing of information. Others believe that if we can simply capture the "information state" of the brain in an appropriately-advanced computer, we can transfer our "minds" outside our bodies.[2]

The more deeply you pursue this trail of information, the more connections one finds. It is clear that our ability to store and communicate information is fundamental to much more than most of us realize. Furthermore, knowing some of that information at the right time can provide tremendous advantage, whether it is in personal relationships, commercial enterprise, or acts by nation-state leaders. It therefore follows that means of protecting that information from disclosure or alteration are often as valuable as the information itself—if not more so.

It is here that cryptography comes into play. With good cryptography, we may be able to protect sensitive information; without it, we are all disadvantaged. It should thus be no surprise that so many organizations have tried to restrict cryptography such that they were the sole practitioners. History continues to show that such efforts seem destined to (eventually) fail. For uses good and ill, cryptography is around to stay.

You hold in your hands a multifarious work that exists against that backdrop. As with the role of information, the more you examine this book, the more facets you will discover.

For instance, if you read this book carefully, you will find it to be a comprehensive and detailed tutorial on cryptographic algorithms and protocols, along with supporting mathematics and statistics. As such, you can expand your knowledge of an important area that is also related to computing and communications. What's more, you can inform yourself about a broad range of issues, from historically significant ciphers to very current research results.

As with other works by Rolf Oppliger, this book is nicely organized and the contents are clearly presented. Each section of the book contains numerous references to important related literature. This combination provides an outstanding

1 See, for instance, "Hawking cracks black hole paradox" by Jenny Hogan in *New Scientist*, July 14, 2004.

2 cf. *In the Age of Spiritual Machines: When Computers Exceed Human Intelligence* by Ray Kurzweil, Penguin Putnam, 2000.

reference work for anyone pursuing scholarly work in the field. Thus, this book is one that will occupy a spot on your bookshelf—and ensure that it doesn't collect dust while there, as I have found so many other books do.

If you're a teacher, you now have a powerful textbook that can be used to prepare students for everything from basic comprehension of cryptographic concepts to reasonably advanced research in the field. As such, this is a much-needed instrument of pedagogy. This is the book colleagues and I wish we had over the last decade when teaching our graduate cryptography class; luckily, now we have it, and you do too.

Cryptography can be an enabler of subversion, of civil disobedience, and of criminal enterprise. It can also be used to safeguard protection of basic human rights, promote privacy, and enhance lawful commerce. Cryptography is an incredibly powerful set of technologies. A sound understanding of cryptographic techniques is not sufficient to guarantee information protection, but it is necessary, whether in computer processing, telecommunications, or database management. As our reliance on computing and network grows, our need for sound cryptography will also grow, and we all will need to have a better understanding of its uses and limitations.

When Rolf set out to write this book, I doubt he considered how it might be used by readers to do so many things. When you started reading it, you probably didn't have wide-ranging motives, either. And when I agreed to write the foreword, I was unsure what the book would be like. But now I know what you will shortly discover: Rolf has done a wonderful job of making so much important information accessible. He is thus a dangerous person, at least in the sense of "dangerous" that I employed at the beginning of this essay, and we should congratulate him for it. Enjoy.

—Gene Spafford[3]
January 2005

3 Eugene H. Spafford is the Executive Director of the Center for Education and Research in Information Assurance and Security at Purdue University in the USA. He is also a professor of Computer Sciences, a professor of Electrical and Computer Engineering, a professor of Philosophy (courtesy), and a professor of Communication (courtesy).

# Preface

*Necessity is the mother of invention,*
*and computer networks are the mother of modern cryptography.*

— Ronald L. Rivest[4]

With the current ubiquity of computer networks and distributed systems in general, and the Internet in particular, cryptography has become an enabling technology to secure the information infrastructure(s) we are building, using, and counting on in daily life. This is particularly true for modern cryptography.[5] The important role of (modern) cryptography is, for example, pointed out by the quote given above. As explained later in this book, the quoted cryptographer—Ronald L. Rivest—is one of the pioneers of modern cryptography and has coinvented the widely deployed Rivest, Shamir, Adleman (RSA) public key cryptosystem.

Due to its important role, computer scientists, electrical engineers, and applied mathematicians should all be educated in the basic principles and applications of cryptography. Cryptography is a tool, and as such it can provide security only if it is used properly. If it is not used properly, then it may fail to provide security in the first place. It may even be worse than not using it at all, because users think that they are protected, whereas in reality this is not the case (this may lead to incorrect user behavior).

There are several books that can be used for educational purposes (e.g., [1–16] itemized in chronological order). Among these books, I particularly recommend [5, 9, 10, 12, 14] to teach classes,[6] [3] to serve as a handy reference for cryptographic algorithms and protocols (also available electronically on the Internet),[7] and [16] to provide an overview about practically relevant cryptographic standards. After having

4 In: "Cryptography as Duct Tape," a short note written to the Senate Commerce and Judiciary Committees in opposition to mandatory key recovery proposals on June 12, 1997 (the note is available electronically at http://theory.lcs.mit.edu/∼rivest/ducttape.txt).

5 In Chapter 1, we explain what modern cryptography really means and how it differs from classical cryptography.

6 Prior to this book, I used to recommend [10] as a textbook for cryptography.

7 http://www.cacr.math.uwaterloo.ca/hac

spent a considerable amount of time compiling and writing a manuscript that can be used to lecture and teach classes on contemporary cryptography, I decided to turn the manuscript into a book and to publish it in Artech House's computer security series.[8] The present book is the result of this endevour.

More often than not, mathematicians care about theoretical concepts and models without having applications in mind. On the other side, computer scientists and electrical engineers often deal with applications without having studied and properly understood the underlying mathematical fundamentals and principles. Against this background, *Contemporary Cryptography* tries to build a bridge and fill the gap between these two communities. As such, it is intended to serve the needs of mathematicians who want to be educated in contemporary cryptography as a possible application of their field(s) of study, as well as computer scientists and electrical engineers who want to be educated in the relevant mathematical fundamentals and principles. Consequently, the target audience for *Contemporary Cryptography* includes all of them: mathematicians, computer scientists, and electrical engineers, both in research and practice. Furthermore, computer practitioners, consultants, and information officers should also gain insight into the fascinating and quickly evolving field.

*Contemporary Cryptography* is written to be comprehensive and tutorial in nature. The book starts with two chapters that introduce the topic and briefly overview the cryptographic systems (or cryptosystems) in use today. After a thorough introduction of the mathematical fundamentals and principles that are at the heart of contemporary cryptography (Part I), the cryptographic systems are addressed in detail and defined in a mathematically precise sense. The cryptographic systems are discussed in three separate parts, addressing unkeyed cryptosystems (Part II), secret key cryptosystems (Part III), and public key cryptosystems (Part IV). Part IV also includes cryptographic protocols that make use of public key cryptography. Finally, the book finishes with an epilogue (Part V) and two appendixes.

Each chapter is intended to be comprehensive (on its own) and includes a list of references that can be used for further study. Where necessary and appropriate, I have also added some uniform resource locators (URLs) as footnotes to the text. The URLs point to corresponding information pages on the World Wide Web (WWW). While care has been taken to ensure that the URLs are valid now, unfortunately—due to the dynamic nature of the Internet and the WWW—I cannot guarantee that these URLs and their contents remain valid forever. In regard to the URLs, I apologize for any information page that may have been removed or replaced since the writing and publishing of the book. To make the problem less severe, I have not included URLs I expect to be removed or replaced anytime soon.

8 http://www.esecurity.ch/serieseditor.html

Readers who like to experiment with cryptographic systems are invited to download, install, and play around with some of the many software packages that have been written and are available for demonstrational and educational purposes. Among these packages, I particularly recommend *CrypTool*. CrypTool is a demonstration and reference program for cryptography that is publicly and freely available[9] and that provides insight into the basic working principles of the cryptographic algorithms and protocols in use today.

If you want to implement and market some of the cryptographic techniques or systems addressed in this book, then you must must be very cautious and note that the entire field of cryptography is tied up in patents and corresponding patent claims. Consequently, you must make sure that you have an appropriate license or a good lawyer (or both).

In either case, regulations for the use and export of cryptographic products (see, for example, Bert-Jaap Koops' Crypto Law Survey)[10] differ in different countries. For example, France had regulations for the use of cryptographic techniques until recently, and some countries—especially in the Far East—still have. On the other side, some countries require specific data to be encrypted according to certain standards or best practices. This is particularly true for personal and medical data. With regard to the export of cryptographic products, the situation is even more involved. For example, since 1996 the U.S. export controls on cryptographic products are administered by the Bureau of Industry and Security (BIS) of the Department of Commerce (DoC). Rules governing exports and reexports of cryptographic products are found in the Export Administration Regulations (EAR). If a U.S. company wants to sell a cryptographic product overseas, it must have export approval according to the EAR. In January 2000, the DoC published a regulation implementing the White House's announcement of a new framework for U.S. export controls on encryption items.[11] The policy was in response to the changing global market, advances in technology, and the need to give U.S. industry better access to these markets, while continuing to provide essential protections for national security. The regulation enlarged the use of license exceptions, implemented the changes agreed to at

9 http://www.cryptool.com or http://www.cryptool.org

10 http://rechten.uvt.nl/koops/cryptolaw

11 The announcement was made on September 16, 1999.

the Wassenaar Arrangement[12] on export controls for conventional arms and dual-use goods and technologies in December 1998, and eliminated the deemed export rule for encryption technology. In addition, new license exception provisions were created for certain types of encryption, such as source code and toolkits. Some countries are exempted from the regulation (i.e., Cuba, Iran, Iraq, Libya, North Korea, Sudan, and Syria). We are not going to address legal issues regarding the use and export of cryptographic products in this book.[13] But note again that you may talk to a lawyer before you use and/or export cryptographic products.

Last, but not least, it is important to note that *Contemporary Cryptography* addresses only the materials that are published and available in the open literature. These materials are, for example, presented and discussed at the conferences[14] held by the International Association for Cryptologic Research (IACR).[15] There may (or may not) be additional and complementary materials available in the backyards of secret services and intelligence agencies. These materials are subject to speculations and rumors; sometimes they even provide the starting point for bestselling books and movies. *Contemporary Cryptography* does not speculate about these materials. It is, however, important to note and always keep in mind that these materials may still exist and that their mere existence may make this book or parts of it obsolete (once their existence becomes publicly known). For example, the notion of public key cryptography was invented by employees of a British intelligence agency a few years before it was published in the open literature (see Section 1.3). Also, the data encryption standard (DES) was designed to make it resistant against differential cryptanalysis—a cryptanalytical attack against symmetric encryption systems that was discussed in the public literature almost two decades after the standardization of the DES (see Section 10.2.1.4). There are certainly many other (undocumented) examples to illustrate this point.

12 The Wassenaar Arrangement is a treaty originally negotiated in July 1996 and signed by 31 countries to restrict the export of dual-use goods and technologies to specific countries considered to be dangerous. The countries that have signed the Wassenaar Arrangement include the former Coordinating Committee for Multilateral Export Controls (COCOM) member and cooperating countries, as well as some new countries such as Russia. The COCOM was an international munitions control organization that also restricted the export of cryptography as a dual-use technology. It was formally dissolved in March 1994. More recently, the Wassenaar Arrangement was updated. The participating countries of the Wassenaar Arrangement are Argentina, Australia, Austria, Belgium, Bulgaria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Japan, Luxembourg, The Netherlands, New Zealand, Norway, Poland, Portugal, Republic of Korea, Romania, Russian Federation, Slovakia, Spain, Sweden, Switzerland, Turkey, Ukraine, the United Kingdom, and the United States. Further information on the Wassenaar Arrangement can be found at http://www.wassenaar.org.

13 There are usually no regulations for the import of cryptographic products.

14 The three major annual conferences are CRYPTO, EUROCRYPT, and ASIACRYPT.

15 http://www.iacr.org

I hope that *Contemporary Cryptography* serves your needs. Also, I would like to take the opportunity to invite you as a reader to let me know your opinions and thoughts. If you have something to correct or add, please let me know. If I have not expressed myself clearly, please let me know. I appreciate and sincerely welcome any comment or suggestion in order to update the book in future editions and to turn it into an appropriate reference book that can be used for educational purposes. The best way to reach me is to send a message to rolf.oppliger@esecurity.ch. You can also visit the book's home page at http://www.esecurity.ch/Books/cryptography.html. I use this page to periodically post errata lists, additional information, and complementary material related to the topic of the book (e.g., slides that can be used to lecture and teach introductory courses on contemporary cryptography). I'm looking forward to hearing from you in one way or another.

## References

[1] Koblitz, N.I., *A Course in Number Theory and Cryptography*, 2nd edition. Springer-Verlag, New York, 1994.

[2] Schneier, B., *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, 2nd edition. John Wiley & Sons, New York, 1996.

[3] Menezes, A., P. van Oorschot, and S. Vanstone, *Handbook of Applied Cryptography*. CRC Press, Boca Raton, FL, 1996.

[4] Luby, M., *Pseudorandomness and Cryptographic Applications*. Princeton Computer Science Notes, Princeton, NJ, 1996.

[5] Buchmann, J.A., *Introduction to Cryptography*. Springer-Verlag, New York, 2000.

[6] Garrett, P.B., *Making, Breaking Codes: Introduction to Cryptology*. Prentice Hall PTR, Upper Saddle River, NJ, 2001.

[7] Mollin, R.A., *An Introduction to Cryptography*. Chapman & Hall/CRC, Boca Raton, FL, 2001.

[8] Goldreich, O., *Foundations of Cryptography: Volume 1, Basic Tools*. Cambridge University Press, Cambridge, UK, 2001.

[9] Delfs, H., and H. Knebl, *Introduction to Cryptography: Principles and Applications*. Springer-Verlag, New York, 2002.

[10] Stinson, D., *Cryptography: Theory and Practice*, 2nd edition. Chapman & Hall/CRC, Boca Raton, FL, 2002.

[11] Mollin, R.A., *RSA and Public-Key Cryptography*. Chapman & Hall/CRC, Boca Raton, FL, 2002.

[12] Smart, N., *Cryptography, An Introduction*. McGraw-Hill Education, UK, 2003.

[13] Ferguson, N., and B. Schneier, *Practical Cryptography*. John Wiley & Sons, New York, 2003.

sample content of Contemporary Cryptography, Second Edition: 2 (Artech House Computer Security Series)

- click The King of Torts
- **read online The Third Life of Grange Copeland**
- Successful Remembering and Successful Forgetting: A Festschrift in Honor of Robert A. Bjork book
- click The Green Hills of Earth and The Menace from Earth pdf, azw (kindle), epub, doc, mobi
- download online Mind Scrambler (John Ceepak, Book 5) pdf, azw (kindle)
- **click And Then You Die**

- http://transtrade.cz/?ebooks/Fragile-Empire--How-Russia-Fell-in-and-out-of-Love-with-Vladimir-Putin.pdf
- http://junkrobots.com/ebooks/The-Chronicles-of-King-Rolen-s-Kin-Trilogy-Box-Set--The-King-s-Bastard--The-Uncrowned-King--The-Usurper--King-Ro
- http://weddingcellist.com/lib/Successful-Remembering-and-Successful-Forgetting--A-Festschrift-in-Honor-of-Robert-A--Bjork.pdf
- http://wind-in-herleshausen.de/?freebooks/The-Green-Hills-of-Earth-and-The-Menace-from-Earth.pdf
- http://schrolf.de/books/Unnatural-Death--Lord-Peter-Wimsey-Mysteries-.pdf
- http://patrickvincitore.com/?ebooks/And-Then-You-Die.pdf