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

685 Canton Street
Norwood, MA 02062

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

10 9 8 7 6 5 4 3 2 1

To my family

Contents

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.