

Understanding and Applying Cryptography and Data Security

Adam J. Elbirt



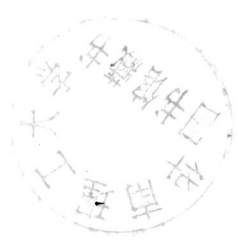
CRC Press
Taylor & Francis Group

AN AUERBACH BOOK

TP 309
E37

Understanding and Applying Cryptography and Data Security

Adam J. Elbirt



E2010000141



CRC Press
Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business
AN AUERBACH BOOK

Auerbach Publications
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

© 2009 by Taylor & Francis Group, LLC
Auerbach is an imprint of Taylor & Francis Group, an Informa business

No claim to original U.S. Government works
Printed in the United States of America on acid-free paper
10 9 8 7 6 5 4 3 2 1

International Standard Book Number-13: 978-1-4200-6160-4 (Hardcover)

This book contains information obtained from authentic and highly regarded sources. Reasonable efforts have been made to publish reliable data and information, but the author and publisher cannot assume responsibility for the validity of all materials or the consequences of their use. The authors and publishers have attempted to trace the copyright holders of all material reproduced in this publication and apologize to copyright holders if permission to publish in this form has not been obtained. If any copyright material has not been acknowledged please write and let us know so we may rectify in any future reprint.

Except as permitted under U.S. Copyright Law, no part of this book may be reprinted, reproduced, transmitted, or utilized in any form by any electronic, mechanical, or other means, now known or hereafter invented, including photocopying, microfilming, and recording, or in any information storage or retrieval system, without written permission from the publishers.

For permission to photocopy or use material electronically from this work, please access www.copyright.com (<http://www.copyright.com/>) or contact the Copyright Clearance Center, Inc. (CCC), 222 Rosewood Drive, Danvers, MA 01923, 978-750-8400. CCC is a not-for-profit organization that provides licenses and registration for a variety of users. For organizations that have been granted a photocopy license by the CCC, a separate system of payment has been arranged.

Trademark Notice: Product or corporate names may be trademarks or registered trademarks, and are used only for identification and explanation without intent to infringe.

Library of Congress Cataloging-in-Publication Data

Elbirt, Adam J.

Understanding and applying cryptography and data security / Adam J. Elbirt.
p. cm.

Includes bibliographical references and index.

ISBN 978-1-4200-6160-4 (alk. paper)

1. Computer security. 2. Cryptography. I. Title.

QA76.9.A25E43 2008

005.8--dc22

2008028154

Visit the Taylor & Francis Web site at
<http://www.taylorandfrancis.com>

and the Auerbach Web site at
<http://www.auerbach-publications.com>

Understanding and Applying Cryptography and Data Security

Architecting Secure Software Systems

Asoke K. Talukder and Manish Chaitanya
ISBN: 978-1-4200-8784-0

Building an Effective Information Security Policy Architecture

Sandy Bacik
ISBN: 978-1-4200-5905-2

Business Resumption Planning, Second Edition

Leo A. Wrobel
ISBN: 978-0-8493-1459-9

CISO Leadership: Essential Principles for Success

Todd Fitzgerald and Micki Krause
ISBN: 978-0-8493-7943-7

CISO Soft Skills: Securing Organizations Impaired by Employee Politics, Apathy, and Intolerant Perspectives

Ron Collette, Michael Gentile, and Skye Gentile
ISBN: 978-1-4200-8910-3

Critical Infrastructure: Understanding Its Component Parts, Vulnerabilities, Operating Risks, and Interdependencies

Tyson Macaulay
ISBN: 978-1-4200-6835-1

Cyber Fraud: Tactics, Techniques and Procedures

Rick Howard
ISBN: 978-1-4200-9127-4

Enterprise Systems Backup and Recovery: A Corporate Insurance Policy

Preston de Guise
ISBN: 978-1-4200-7639-4

How to Complete a Risk Assessment in 5 Days or Less

Thomas R. Peltier
ISBN: 978-1-4200-6275-5

How to Develop and Implement a Security Master Plan

Timothy Giles
ISBN: 978-1-4200-8625-6

HOWTO Secure and Audit Oracle 10g and 11g

Ron Ben-Natan
ISBN: 978-1-4200-8412-2

Information Assurance Architecture

Keith D. Willett
ISBN: 978-0-8493-8067-9

Information Security Management Handbook, Sixth Edition, Volume 3

Harold F. Tipton and Micki Krause, Editors
ISBN: 978-1-4200-9092-5

Information Security Management Metrics: A Definitive Guide to Effective Security Monitoring and Measurement

W. Krag Brotby
ISBN: 978-1-4200-5285-5

Information Technology Control and Audit, Third Edition

Sandra Senft and Frederick Gallegos
ISBN: 978-1-4200-6550-3

Intelligent Network Video: Understanding Modern Video Surveillance Systems

Fredrik Nilsson
ISBN: 978-1-4200-6156-7

IT Auditing and Sarbanes-Oxley Compliance: Key Strategies for Business Improvement

Dimitris N. Chorafas
ISBN: 978-1-4200-8617-1

Malicious Bots: An Inside Look into the Cyber-Criminal Underground of the Internet

Ken Dunham and Jim Melnick
ISBN: 978-1-4200-6903-7

Oracle Identity Management: Governance, Risk, and Compliance Architecture, Third Edition

Marlin B. Pohlman
ISBN: 978-1-4200-7247-1

Profiling Hackers: The Science of Criminal Profiling as Applied to the World of Hacking

Raoul Chiesa, Stefania Ducci, and Silvio Ciappi
ISBN: 978-1-4200-8693-5

Security in an IPv6 Environment

Daniel Minoli and Jake Kouns
ISBN: 978-1-4200-9229-5

Security Software Development: Assessing and Managing Security Risks

Douglas A. Ashbaugh
ISBN: 978-1-4200-6380-6

Software Deployment, Updating, and Patching

Bill Stackpole and Patrick Hanrion
ISBN: 978-0-8493-5800-5

Terrorist Recognition Handbook: A Practitioner's Manual for Predicting and Identifying Terrorist Activities, Second Edition

Malcolm Nance
ISBN: 978-1-4200-7183-2

21st Century Security and CPTED: Designing for Critical Infrastructure Protection and Crime Prevention

Randall I. Atlas
ISBN: 978-1-4200-6807-8

Understanding and Applying Cryptography and Data Security

Adam J. Elbirt
ISBN: 978-1-4200-6160-4

AUERBACH PUBLICATIONS

www.auerbach-publications.com

To Order Call: 1-800-272-7737 • Fax: 1-800-374-3401

E-mail: orders@crcpress.com

Dedication

To Danielle, Jacob, and Rachel — the impossible became real because of you. You are the shining lights of my life and bring joy to my heart.

About the Author

Adam J. Elbirt is a Senior Member of Technical Staff at the Charles Stark Draper Laboratory, Inc. He is also a member of the Eta Kappa Nu and Sigma Chi honorary societies.

Elbirt has given seminars for such prestigious universities as Worcester Polytechnic Institute, the New Jersey Institute of Technology, and the University of Massachusetts Lowell. He was a founding member of the Center for Network and Information Security and recently completed a six-year term as a professor of computer science at the University of Massachusetts Lowell.

Prior to joining the Charles Stark Draper Laboratory, Elbirt held senior engineering positions at Viewlogic Systems and NTRU Cryptosystems. He holds a doctor of philosophy degree from Worcester Polytechnic Institute where he performed his research in the area of reconfigurable hardware architectures designed to accelerate cryptographic algorithms. Elbirt has published numerous articles in journals and conference proceedings and many of

his implementations broke previous encryption throughput performance records for symmetric-key algorithms.

Acknowledgments

I would like to deeply thank Christof Paar, chair for Communication Security of the Horst Görtz Institut for IT Security at the Ruhr-Universität Bochum. Christof was my advisor and mentor at Worcester Polytechnic Institute from 1998 through 2002, and much of my lecture notes and thus the topics examined in this textbook are based on his rigorous and comprehensive lectures, examples, and practical implementation knowledge. It is through Christof's guidance and love for cryptography and information security that I first became interested in these areas and I would like to express my heartfelt appreciation to him.

I would also like to extend my thanks to Ralph Spencer Poore, Managing Partner of PiR Squared Consulting LLP, for his time and effort spent reviewing the text.

Contents

1	Introduction	1
1.1	A Brief History of Cryptography and Data Security	1
1.2	Cryptography and Data Security in the Modern World	2
1.3	Existing Texts	4
1.4	Book Organization	5
1.5	Supplements	8
2	Symmetric-Key Cryptography	9
2.1	Cryptosystem Overview	10
2.2	The Modulo Operator	13
2.3	Greatest Common Divisor	19
2.4	The Ring Z_m	20

2.5 Homework Problems 22

3 Symmetric-Key Cryptography: Substitution Ciphers 25

3.1 Basic Cryptanalysis 25

3.2 Shift Ciphers 30

3.3 Affine Ciphers 33

3.4 Homework Problems 41

4 Symmetric-Key Cryptography: Stream Ciphers 49

4.1 Random Numbers 52

4.2 The One-Time Pad 53

4.3 Key Stream Generators 56

4.3.1 Linear Feedback Shift Registers 57

4.3.2 Clock Controlled Shift Register Key Stream
Generators 68

4.3.3 Attacks Against LFSRs 70

4.4 Real-World Applications 73

4.5 Homework Problems 74

- 5 Symmetric-Key Cryptography: Block Ciphers 83**
 - 5.1 The Data Encryption Standard 84
 - 5.1.1 Feistel Networks 84
 - 5.1.2 Cryptosystem 87
 - 5.1.3 Modes of Operation 99
 - 5.1.3.1 Electronic Code Book Mode 99
 - 5.1.3.2 Cipher Block Chaining Mode 101
 - 5.1.3.3 Propagating Cipher Block Chaining Mode 105
 - 5.1.3.4 Cipher Feedback Mode 107
 - 5.1.3.5 Output Feedback Mode 109
 - 5.1.3.6 Counter Mode 111
 - 5.1.4 Key Whitening 112
 - 5.1.5 Efficient Implementation 113
 - 5.1.6 Attacks Against DES 117
 - 5.1.6.1 Weak and Semi-Weak Keys 118
 - 5.1.6.2 Exhaustive Key Search 120

5.1.6.3	Meet-In-The-Middle	122
5.1.6.4	S-Box Design Criteria	126
5.1.7	Homework Problems	128
5.2	The Advanced Encryption Standard	139
5.2.1	Galois Field Mathematics	140
5.2.2	Cryptosystem	146
5.2.3	Modes of Operation	157
5.2.3.1	Cipher-Based Message Authentica- tion Code Mode	158
5.2.3.2	Counter with Cipher Block Chaining- Message Authentication Code Mode	164
5.2.4	Efficient Implementation	173
5.2.5	Attacks Against AES	183
5.2.6	Homework Problems	186
6	Public-Key Cryptography	195
6.1	Issues with Symmetric-Key Cryptosystems	195
6.2	Public-Key Cryptosystem Overview	196

6.3	One-Way Functions	199
6.4	The Euclidean Algorithm	200
6.5	The Extended Euclidean Algorithm	202
6.6	Euler's Phi Function	211
6.7	Euler's Theorem	213
6.8	Fermat's Little Theorem	214
6.9	Homework Problems	216
7	Public-Key Cryptography: RSA	223
7.1	Cryptosystem	223
7.2	Efficient Implementation	228
7.2.1	Parameter Selection	228
7.2.2	Exponentiation	230
7.2.3	The Chinese Remainder Theorem	253
7.2.4	Multi-Precision Arithmetic	266
7.2.4.1	Addition	267
7.2.4.2	Multiplication	268
7.2.4.3	Squaring	272

7.2.4.4	Montgomery Arithmetic	274
7.2.4.5	Inversion	283
7.2.5	The Karatsuba-Ofman Multiplication Algorithm	285
7.2.6	Performance	289
7.3	Attacks	295
7.4	Homework Problems	298
8	Public-Key Cryptography: Discrete Logarithms	313
8.1	Cyclic Groups	313
8.2	The Discrete Logarithm Problem	324
8.3	Diffie-Hellman Key Agreement Protocol	326
8.4	Efficient Implementation	330
8.5	ElGamal Encryption	332
8.6	Attacks	338
8.6.1	Shank's Algorithm	338
8.6.2	Pollard's Rho Method	342
8.6.3	The Pohlig-Hellman Algorithm	354

- 8.6.4 The Index Calculus Method 362
- 8.7 Homework Problems 379
- 9 Public-Key Cryptography: Elliptic Curves 395**
 - 9.1 Cryptosystem 395
 - 9.2 Diffie-Hellman Key Agreement Protocol 413
 - 9.3 Efficient Implementation 416
 - 9.4 Menezes-Vanstone Encryption 420
 - 9.5 Attacks 428
 - 9.6 Homework Problems 429
- 10 Cryptographic Components 437**
 - 10.1 Digital Signatures 437
 - 10.1.1 RSA 440
 - 10.1.2 ElGamal 444
 - 10.1.3 Elliptic Curves 453
 - 10.1.4 Efficient Implementation 465
 - 10.1.5 Homework Problems 465

10.2 Hash Functions	471
10.2.1 The Birthday Paradox	476
10.2.2 Algorithms	482
10.2.2.1 Block Cipher Based Algorithms	483
10.2.2.2 MD4	485
10.2.2.3 MD5	489
10.2.2.4 Secure Hash Algorithm	495
10.2.2.5 RIPEMD-160	515
10.2.3 Efficient Implementation	524
10.2.4 Homework Problems	525
10.3 Message Authentication Codes	528
10.3.1 Algorithms	530
10.3.1.1 Block Cipher Based Algorithms	531
10.3.1.2 Hash Function Based Algorithms	533
10.3.2 Efficient Implementation	534
10.3.3 Homework Problems	534

11 Cryptographic Protocols

537