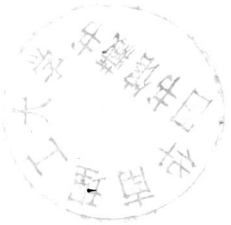
Understanding and Applying Cryptography and Data Security

Adam J. Elbirt

CRC Press
Taylor & Francis Group
AN AUERBACH BOOK

Understanding and Applying Cryptography and Data Security

Adam J. Elbirt



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

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)

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

OTHER INFORMATION SECURITY BOOKS FROM AUERBACH

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 Goßrtz Institut for IT Security at the Ruhr-Universitaßt 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