Cryptography FOR DUMMIES®

by Chey Cobb, CISSP

WILEY
Wiley Publishing, Inc.

Cryptography FOR DUMMIES®

Cryptography For Dummies®
Published by
Wiley Publishing, Inc.
111 River Street
Hoboken, NJ 07030-5774

Published by Wiley Publishing, Inc., Indianapolis, Indiana

Published simultaneously in Canada

Library of Congress Control Number: 2003105686

ISBN: 0764541889

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

1O/QY/QR/QU/IN

About the Author

Chey Ewertz Cobb, CISSP, began working in computer security in 1989. Since then she has managed her own computer security consulting company, Cobb Associates, working for such clients as Apple Computers and Sun Microsystems. She later worked for the government, creating a secure network at Cape Canaveral, assisting in the security at Patrick Air Force Base, and later as a technical security officer for the National Reconnaissance Office (NRO), which is more secretive than the NSA.

During her work in security, she had the opportunity to evaluate and manage cryptosystems for private industry and the U.S. Intelligence Agencies.

Chey now writes books on computer security (*Computer Security Handbook, 4th Edition* and *Network Security For Dummies*), writes articles for magazines, and speaks at computer security conferences.

Dedication

To R. W. Ewertz, Jr. He was my role model and inspiration when things got tough.

Acknowledgments

First of all, let me thank Andrea Boucher and Melody Layne who saw me through thick and thin and never lost faith in me (at least they never let on that they did!). I enjoy working with them both, and any writer who has the opportunity to work with them should count himself/herself lucky!

Secondly, I want to thank Dave Brussin, Ryan Upton, Josh Beneloh, Jon Callas, and Dave Del Torto for setting me on the correct path when my explanations strayed. Thanks so much for lending me your brainwork!

Last, but not least, Stephen. My love, my life, and my everything.

Publisher's Acknowledgments

We're proud of this book; please send us your comments through our online registration form located at www.dummies.com/register/.

Some of the people who helped bring this book to market include the following:

Acquisitions, Editorial, and Media Development

Project Editor: Andrea C. Boucher

Acquisitions Editor: Melody Layne

Technical Editor: Tim Crothers

Editorial Manager: Carol Sheehan

Media Development Manager: Laura VanWinkle

Media Development Supervisor: Richard Graves

Editorial Assistant: Amanda Foxworth

Cartoons: Rich Tennant (www.the5thwave.com)

Production

Project Coordinator: Maridee Ennis

Layout and Graphics: Joyce Haughey, Andrea Dahl, Stephanie D. Jumper, Jacque Schneider, Melanee Wolven

Proofreaders: Andy Hollandbeck, Carl William Pierce, TECHBOOKS Production Services

Indexer: TECHBOOKS Production Services

Publishing and Editorial for Technology Dummies

Richard Swadley, Vice President and Executive Group Publisher

Andy Cummings, Vice President and Publisher

Mary C. Corder, Editorial Director

Publishing for Consumer Dummies

Diane Graves Steele, Vice President and Publisher

Joyce Pepple, Acquisitions Director

Composition Services

Gerry Fahey, Vice President of Production Services

Debbie Stailey, Director of Composition Services

Contents at a Glance

Table of Contents