



CRYPTOGRAPHY DECRYPTED







CRYPTOGRAPHY DECRYPTED

H. X. Mel
Doris Baker

Math Appendix by Steve Burnett
Foreword by John Kinyon

◆ Addison-Wesley

Boston • San Francisco • New York • Toronto • Montreal
London • Munich • Paris • Madrid
Capetown • Sydney • Tokyo • Singapore • Mexico City



Many of the designations used by manufacturers and sellers to distinguish their products are claimed as trademarks. Where those designations appear in this book, and Addison-Wesley was aware of a trademark claim, the designations have been printed with initial capital letters or in all capitals.

Screen shots reprinted by permission from Microsoft Corporation.

The author(s) and publisher have taken care in the preparation of this book, but make no expressed or implied warranty of any kind and assume no responsibility for errors or omissions. No liability is assumed for incidental or consequential damages in connection with or arising out of the use of the information or programs contained herein.

The publisher offers discounts on this book when ordered in quantity for bulk purchases and special sales. For more information, please contact:

U.S. Corporate and Government Sales
(800) 382-3419
corpsales@pearsontechgroup.com

For sales outside of the U.S., please contact:

International Sales
(317) 581-3793
international@pearsontechgroup.com

Visit Addison-Wesley on the Web: www.awprofessional.com

Library of Congress Cataloging-in-Publication Data

Mel, H.X., 1948-

Cryptography decrypted / H. X. Mel, Doris M. Baker; math appendix by Steve Burnett;
foreword by John Kinyon.

p. cm.

Includes bibliographical references and index.

ISBN 0-201-61647-5

1. Computer security. 2. Cryptography. I. Baker, Doris M. II. Title.

QA76.9.A25 M44 2000

005.8'2—dc21

00-046878

Copyright © 2001 by Cary Meltzer and Doris Baker

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form, or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior consent of the publisher. Printed in the United States of America. Published simultaneously in Canada.

For information on obtaining permission for use of material from this work, please submit a written request to:

Pearson Education, Inc.
Rights and Contracts Department
75 Arlington Street, Suite 300
Boston, MA 02116
Fax: (617) 848-7047

ISBN 0-201-61647-5

Text printed on recycled paper

5 6 7 8 9 10—PH—0807060504

Fifth printing, May 2004








*For Max Samuel—
who showed us a good hiding place is hard to find*





KEY POINTS

PARTS	CHAPTER	MAJOR TOPICS
 Part I: Secret Key Cryptography	1-4	Cryptographic methods are separate from cryptographic keys Strong cryptographic methods are secure Best feasible attack is to try each possible key
	5	DES was secure, but technology has weakened it
	6	History leading to modern cryptography
	7	Secret key assurances: confidentiality, authentication, and integrity
	8	Secret key sharing problems
 Part II: Public Key	9	Foundation of public key cryptography: easy and hard problems
	10	Public key encryption assurance: confidentiality
	11	Simple cryptographic arithmetic
	12	Private key encryption assurances: authentication, integrity, and nonrepudiation
	13	Detecting message modification with message digests
	14	Message digest assurances: one-wayness and collision resistance
 Part III: Key Distribution	15	Comparing secret key, public key, and message digests
	16	Digital certificates are signed public keys
	17	X.509 digital certificates, certificate authorities, and certificate revocation
 Part IV: Real World Systems	18	Pretty Good Privacy (PGP) digital certificates PGP compared to X.509
	19-21	Examples of real world systems (secure email, SSL, IPsec)
 Appendixes	22	Some cryptographic attacks
	23	Protecting your keys with smartcards
	A	Mathematics underlying public key technology
	B	Additional IPsec details



CONTENTS

Foreword	xv
Preface	xvii
Introduction	xix
Part I Secret Key Cryptography	1
Chapter 1 Locks and Keys	3
Locks and Combinations	3
Defining Cryptographic Terms	5
Making and Solving Puzzles	6
Review	6
Chapter 2 Substitution and Caesar's Cipher	7
Cryptanalysis of Caesar's Cipher	10
Empowering the Masses	11
The Importance of Separating the Method and the Key	12
Adding Keys	13
<i>A Weakness of Caesar's Ciphers: The Failure to</i>	
<i>Hide Linguistic Patterns</i>	14
More Complex Substitution: Vigenère's Cipher	15
Review	19
Chapter 3 Transposition Ciphers: Moving Around	21
Patterns and Cryptanalysis	22
Adding Complexity	23
Computer Transposition	25
Combining Substitution and Transposition	26
Review	28



Chapter 4	Diffuse and Confuse: How Cryptographers Win the End Game	29
	Diffusion	29
	<i>The Polybius Cipher</i>	30
	The Principle of Confusion	33
	Cryptographic Locks and Keys	34
	Review	35
Chapter 5	DES Isn't Strong Anymore	37
	The Historical Need for an Encryption Standard	37
	Cycling Through Computer Keys	40
	Double and Triple DES	41
	DES (and Other Block Cipher) Modes	42
	The Avalanche Effect	42
	Supplement: Binary Numbers and Computer Letters	43
	Review	44
Chapter 6	Evolution of Cryptography: Going Global	45
	Early Cryptography	46
	Commercial and Military Needs	48
	Entering the Computer Age	49
	Review	51
Chapter 7	Secret Key Assurances	53
	Confidentiality	54
	Authentication	55
	<i>An Authentication Attack</i>	57
	Not Really Random Numbers	57
	Integrity	59
	<i>Using the MAC for Message Integrity Assurance</i>	60
	<i>Why Bother Using a Message Authentication Code?</i>	62
	<i>File and MAC Compression</i>	62
	Nonrepudiation: Secret Keys Can't Do It	63
	Review	64
Chapter 8	Problems with Secret Key Exchange	65
	The Problem and the Traditional Solution	66
	Using a Trusted Third Party	68
	Key Distribution Center and Key Recovery	70



Problems with Using a Trusted Third Party	71
<i>Growth in the Number of Secret Keys</i>	71
<i>Trust and Lifetime</i>	72
Review	72
Part II Public Key Cryptography	75
Chapter 9 Pioneering Public Key: Public Exchange of Secret Keys	77
The Search for an Innovative Key Delivery Solution	77
Developing an Innovative Secret Key Delivery Solution	77
<i>First Attempt: A Database of Key/Serial Number Pairs</i>	78
<i>Second Attempt: An Encrypted Database of Key/Serial Number Pairs</i>	79
<i>Merkle's Insight: Individually Encrypted Key/Serial Number Pairs</i>	80
<i>Black Hat's Frustrating Problem</i>	81
<i>The Key to Public Key Technology</i>	82
A New Solution: Diffie-Hellman-Merkle Key Agreement	84
<i>Alice and Bob Openly Agree on a Secret Key</i>	84
<i>Problems with the Diffie-Hellman Method</i>	86
Separate Encryption and Decryption Keys	86
Review	88
Chapter 10 Confidentiality Using Public Keys	89
New Twists on Old Security Issues	89
Confidentiality Assurances	92
Distribution of Public Keys	92
Two-Way Confidentiality	94
Review	95
Chapter 11 Making Public Keys: Math Tricks	97
Alice's Easy Problem	98
Grade School Math Tricks	100
More Grade School Math	101
Division and Remainders: Modular Math	103
Modular Inverses	106
Using Modular Inverses to Make a Public Key	109
Putting It All Together	110
<i>Giving BlackHat a Difficult, Time-Consuming Problem</i>	110
<i>Trapdoor to the Easy Problem</i>	111



Knapsack Cryptography	112
Modulo Calculations	112
Exercise: Find Which Numbers Sum to 103	112
Review	113
Chapter 12 Creating Digital Signatures Using the Private Key	115
Written and Digital Signature Assurances	116
Reviewing and Comparing Authentication	117
<i>Secret Key Authentication</i>	117
<i>Private Key Authentication</i>	117
Authentication and Integrity Using Private and Secret Keys	119
Private Key Authentication Methods	120
<i>RSA</i>	120
<i>DSA</i>	121
<i>Signing Terminology</i>	122
Nonrepudiation	122
Assurances in Both Directions	123
Summary of Public Key Assurances	123
<i>Public Key Means Public / Private Key</i>	124
<i>Assurance Initiated</i>	124
Compressing before Signing	124
Review	125
Chapter 13 Hashes: Non-keyed Message Digests	127
Detecting Unintentional Modifications	129
Detecting Intentional Modifications	131
Signing the Message Digest	133
<i>Detecting BlackHat's Forgery</i>	135
Replay Attacks	136
Supplement: Unsuccessfully Imitating a Message Digest	137
Review	138
Chapter 14 Message Digest Assurances	141
Two Message Digest Flavors	141
Non-keyed Message Digest Assurances	143
<i>One-wayness</i>	143
<i>Collision Resistance</i>	143
<i>Weak Collision Resistance</i>	144
<i>Examples of One-way and Weak Collision Resistance</i>	145
<i>Strong Collision Resistance</i>	147



Non-keyed Digest Implementations	150
Keyed Message Digest Assurances	151
<i>A MAC Made with DES</i>	151
<i>DES-MAC Security</i>	152
Message Digest Compression	154
Digest Speed Comparisons	155
Hashed MAC	155
Review	156

Chapter 15 Comparing Secret Key, Public Key, and Message Digests 157

Encryption Speed	157
Key Length	158
Ease of Key Distribution	158
Cryptographic Assurances	159
<i>Symmetric (Secret) Key</i>	159
<i>Asymmetric (Public) Key</i>	159
Review	161

Part III Distribution of Public Keys 163

Chapter 16 Digital Certificates 165

Verifying a Digital Certificate	167
Attacking Digital Certificates	167
<i>Attacking the Creator of the Digital Certificate</i>	168
<i>Malicious Certificate Creator</i>	168
<i>Attacking the Digital Certificate User</i>	168
<i>The Most Devastating Attack</i>	168
Understanding Digital Certificates: A Familiar Comparison	169
<i>Issuer and Subject</i>	169
<i>Issuer Authentication</i>	169
<i>Transfer of Trust from the Issuer to the Subject</i>	170
<i>Issuer's Limited Liability</i>	171
<i>Time Limits</i>	171
<i>Revoking Trust</i>	171
<i>More than One Certificate</i>	172
<i>Fees for Use</i>	172
The Needs of Digital Certificate Users	172
Getting Your First Public Key	173
Certificates Included in Your Browser	174
Review	174

Chapter 17	X.509 Public Key Infrastructure	177
	Why Use X.509 Certificate Management?	178
	What Is a Certificate Authority?	179
	<i>Application, Certification, and Issuance</i>	179
	<i>Certificate Revocation</i>	181
	<i>Polling and Pushing: Two CRL Delivery Models</i>	182
	Building X.509 Trust Networks	182
	<i>Root Certificates</i>	183
	<i>More Risks and Precautions</i>	187
	<i>Distinguished Names</i>	188
	<i>Certification Practice Statement</i>	189
	X.509 Certificate Data	189
	<i>Challenge Response Protocol</i>	190
	Review	190
Chapter 18	Pretty Good Privacy and the Web of Trust	193
	The History of PGP	193
	Comparing X.509 and PGP Certificates	194
	Building Trust Networks	196
	<i>Bob Validates Alice's Key</i>	196
	<i>Casey Validates Alice's Key Sent by Bob</i>	197
	<i>Dawn Validates Alice's Key Sent by Casey via Bob</i>	198
	<i>Web of Trust</i>	200
	PGP Certificate Repositories and Revocation	200
	Compatibility of X.509 and PGP	201
	Review	201
Part IV	Real-World Systems	203
	E-mail Cryptographic Parameters	204
	Negotiation of SSL and IPsec Cryptographic Parameters	204
	User Initiation of Cryptographic E-mail, SSL, and IPsec	205
Chapter 19	Secure E-mail	207
	Generic Cryptographic E-mail Messages	207
	Invoking Cryptographic Services	209
	Confidentiality and Authentication	211
	<i>Choosing Services</i>	211
	<i>Positioning Services</i>	212
	Deterring E-mail Viruses	213
	Review	213



Chapter 20	Secure Socket Layer and Transport Layer Security	215
	History of SSL	216
	Overview of an SSL Session	216
	An SSL Session in Detail	218
	<i>Hello and Negotiate Parameters</i>	219
	<i>Key Agreement (Exchange)</i>	221
	<i>Authentication</i>	222
	<i>Confidentiality and Integrity</i>	223
	TLS Variations	224
	<i>Anonymous Diffie-Hellman</i>	224
	<i>Fixed and Ephemeral Diffie-Hellman</i>	225
	Comparing TLS, SSL v3, and SSL v2	225
	<i>A Big Problem with SSL v2</i>	225
	<i>A Possible Problem with TLS and SSL</i>	225
	Generating Shared Secrets	226
	Bob Authenticates Himself to AliceDotComStocks	227
	Review	227
Chapter 21	IPsec Overview	229
	Enhanced Security	229
	Key Management	230
	<i>Manual Distribution</i>	231
	<i>Automated Distribution</i>	231
	IPsec Part 1: User Authentication and Key Exchange	
	Using IKE	232
	<i>SSL/TLS and IPsec Key Agreement</i>	232
	<i>Security Association</i>	232
	<i>Phases</i>	233
	<i>IKE Nomenclature</i>	235
	<i>Benefits of Two-Phase Key Exchange</i>	235
	IPsec Part 2: Bulk Data Confidentiality and Integrity for	
	Message or File Transport	237
	<i>Protocol and Mode</i>	238
	<i>ESP Examples</i>	241
	<i>AH Examples</i>	243
	<i>Management Control</i>	244
	Implementation Incompatibilities and Complications	245
	Review	246
Chapter 22	Cryptographic Gotchas	247
	Replay Attack	247

Man-in-the-Middle Attack	247
Finding Your Keys in Memory	249
Does Confidentiality Imply Integrity?	249
<i>Example 1: Substituting a Forged Key</i>	250
<i>Example 2: Cut-and-Paste Attack</i>	250
Public Key as a Cryptanalysis Tool	251
<i>Example 1: The Chosen Plaintext Attack</i>	251
<i>Public Key Cryptographic Standards</i>	253
<i>Example 2: The Bleichenbacher Attack</i>	253
BlackHat Uses Bob's RSA Private Key	253
Review	257
Chapter 23 Protecting Your Keys	259
Smart Cards	259
<i>Types of Smart Cards</i>	260
<i>What's Inside a Smart Card</i>	261
<i>Protections and Limitations</i>	261
<i>Smart Card Attacks</i>	261
Review	262
Epilogue	263
Appendix A Public Key Mathematics (and Some Words on Random Numbers)	267
Appendix B (A Few) IPsec Details	321
Bibliography	337
Index	345



FOREWORD

e-Everything

Every January for the past 10 years, members of a cult from all over the world have headed to Silicon Valley for a summit. In the early years, only a few cryptographers, mathematicians, and forward thinkers in the relatively new field of computer security showed up for this then-obscure event, known as the RSA Security Conference. Imagine, if you will, a group of distinguished eggheads and computer nerds getting together to talk about cryptographic algorithms and how they might one day be used to solve security problems.

In Internet years, that first event was a very long time ago. A decade for everyday people, it was an Internet generation for those of us involved with computer technology. The problems were small and often theoretical then. We couldn't imagine the looming frenzied pace of change, the way the World Wide Web (World Wide what?—it wouldn't be invented for another year) would explode, and the e-izing of everything and anything. With those changes came what those original visionaries predicted: e-fraud, e-theft, e-vandalism, e-scams, e-viruses, and e-everything-else bad along with e-everything good.

Nowadays, there are dozens of computer security conferences and exhibits. Even so, our understanding of cryptography is weak, often only abstract. Practical applications of cryptography are just beginning to become commonplace. These solutions are still young. It is a struggle for an information technology professional, and often an information protection professional, to understand how security technology works and how to apply cryptography appropriately to solve real business problems.

The RSA Security Conference is bigger than ever. Hidden among the product demos, sales pitches, and seminars, interesting technical papers are still presented. It was at RSA 2000 that I met the joyful and energetic H. X. Mel. Like many others, he and Doris Baker had a vision of how to improve security. Their vision, however, was not product implementation, but education—to make cryptography understandable to the people who need it. Their book, this book, is more than “Alice and Bob” diagrams and yet less than a tome full of math.

xv



Instead, it is filled with examples of the principles behind today's solutions, explained with an interesting historical perspective.

Even after 10 years working in the field of information protection for a major electronics manufacturing company, I learned a lot from this book. I think you will, too.

—John Kinyon





PREFACE

A Tool for Everyone

In the past, cryptography was used mainly to secure the communications of the powerful and influential, the military and royalty. But the widespread use of computers, and the attacks to which they are vulnerable, has expanded the need for secure communications around the globe. This book describes the protection afforded by modern computer cryptographic systems and explains how the pace of modern technology requires continuing attention to the security of those systems.

The advent of computers changed a great many things, but not the fundamentals of cryptography. Through stories and pictures, *Cryptography Decrypted* presents cryptography's evolution into a modern-day science, laying out patterns from the past that are applicable today. It also gives you a thorough understanding of terms that are destined to become as much a part of our language and life as *megabyte* and *Internet*. As you begin to think about controlling various aspects of your life using wired or wireless communication, on line all the time, your understanding of cryptography—its benefits and its pitfalls—will make you feel a little more in control of a rapidly changing world.

Because rapid advances in the speed of hardware will continue to threaten the security of current cryptographic methods, it's essential that you choose appropriate techniques and perform ongoing assessment if you want to maintain your digital security. You can make such choices and assessments only if you know the basic concepts of cryptography. *Cryptography Decrypted* offers you that knowledge through visual representation of difficult concepts, an easy-to-use reference for reviewing key cryptographic terminology, and instructive historical information.

You need little or no background in cryptography to read this book. Neither does it require technical or math genius. It's designed so that anyone from CIOs to self-taught computer enthusiasts—and everyone in between—can pick up this book without any knowledge of encryption and find it fascinating, understandable, and instructive.



If you have some understanding of computer cryptography, *Cryptography Decrypted* is systematic and comprehensive enough to solidify your knowledge. It provides a simple description of the component parts of secret key and public key cryptography. (Those who already understand and don't wish to cover any more material about secret key cryptography may choose to read only Parts II through IV, bypassing Part I.)

Throughout the book, we use images to clarify cryptographic terms. After explaining the basic cryptographic components, we describe real-world cryptographic systems, some possible attacks on those systems, and ways to protect your keys.

The book provides a historical framework on which to build your understanding of how and why computer cryptography works. After a discussion of how cryptography has evolved into an essential Internet tool, we analyze secret key exchange problems and then explain the evolution of public key cryptography, with its solution to the key exchange problem. Along the way we explain some simple background on the math tricks that make public key cryptography secure.

Traditionally, those who have thoroughly understood cryptography have been trained as mathematicians or scientists. Our goal here is to explain computer cryptography with rather little discussion of math. If the esoteric details aren't of immediate concern to you, you can skip Chapter 11 ("Making Public Keys: Math Tricks"), Chapter 14 ("Message Digest Assurances"), and the appendixes without diminishing your understanding of the basic concepts.

Appendix A describes some aspects of public key mathematics, including inverses, primes, the Fermat test, Diffie-Hellman, DSA, elliptic curve, and pseudo-random number generation. Appendix B provides details of IPsec, a security system introduced in Chapter 21.

Acknowledgments

It was no small task to wade through and distill the technical and historical material to write a cryptography book that would be understandable to a broad audience. We could not have done it without the considerable help we received from conscientious reviewers who left no stone unturned. They included Paul Brown, Sheila Frankel, Russ Housley, Doug Hughes, John Kinyon, Marcus Leech, Greg Rose, Ben Rosengart, Anton Stiglic, David Youd, and Neal Ziring.

Of course, we might never have gotten through the many months of creation and rewrite without our editors, Tyrrell Albaugh, Karen Gettman, Betsy Hardinger, Mary Hart, and Lisa Hernandez, who helped us stay focused on the light at the end of the tunnel.

Our heartfelt thanks to them all.



INTRODUCTION

Welcome to the Front Line

If your computer is connected to or transmits over an electronic network, your data is on the front line. Attackers are getting more competent by the month, and their attacks more intrusive, virulent, and widespread—from Melissa to the Love Bug to the unknown virus that ate your hard drive.

Although few of us leave our valuables unlocked, few of us know how to use cryptographic locks to secure our digital possessions. By the time you finish reading this book, you will.

Most governments, including those of Canada, China, France, Saudi Arabia, and the United States, consider cryptographic tools to be munitions of war, so it's reasonable to think of potential attacks on your data as a kind of war. Your opponent is anyone who wants to read, modify, or destroy your private documents.

In large part, this is a book about the cryptographic keys and methods you use to safeguard your digital possessions. Figure I-1 shows cryptographic keys and the symbols we use to portray them. Part I of this book explains secret keys

A Devastating Opponent

In World War II the German Observation Service—Beobachtungs-Dienst, or B-Dienst—was a small group of codebreakers who played a powerful role in the Battle of the Atlantic. B-Dienst uncovered the positions of Allied convoys that German submarines then destroyed, devastating the Allied Atlantic forces from 1941 to 1943. For example, during three days in March 1943, the Germans sank 21 Allied vessels while losing only one submarine. Better communications security and new technologies such as sonar helped the Allies turn the tide.

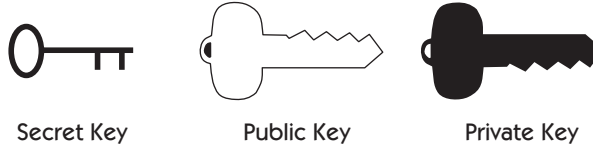


Figure I-1 Cryptographic keys used in this book.

and secret key methods. Part II describes public and private keys and public key methods. Part III explains how keys are distributed, and Part IV shows how three real-world systems—secure mail, Secure Socket Layer (SSL), and Internet Protocol Security (IPsec)—use cryptographic keys and methods.

Need a Quick Read?

Chapters 3, 4, 11, and 14 contain details that can be skimmed or skipped. Chapters 3 and 4 show cryptographic techniques that strengthen secret key methods. Chapter 11 explains a simple math trick to make public/private keys. Chapter 14 illustrates some cryptographic tools used to identify message tampering.