

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
RSA	120
DSA	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
Public Key Cryptographic Standards	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