

NETWORK SECURITY PRIVATE Communication in a PUBLIC World Second Edition This page is intentionally left blank NETWORK SECURITY PRIVATE Communication in a PUBLIC World
 CHARLIE KAUFMAN • RADIA PERLMAN • MIKE SPECINER Second Edition Authorized adaptation from the United States edition, entitled Network Security: Private Communication in a Public World, Second Edition, ISBN 978-01-304-6019-6, by Kaufman, Charlie; Perlman, Radia; Speciner, Mike; published by Pearson Education, Inc, Copyright © 2002. Indian Subcontinent Adaptation Copyright © 2017 Pearson India Education Services Pvt. Ltd This book is sold subject to the condition that it shall not, by way of trade or otherwise, be lent, resold, hired out, or otherwise circulated without the publisher's prior written consent in any form of binding or cover other than that in which it is published and without a similar condition including this condition being imposed on the subsequent purchaser and without limiting the rights under copyright reserved above, no part of this publication may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording or otherwise), without the prior written permission of both the copyright owner and the publisher of this book. ISBN 978-93-325-7821-0 e-ISBN 978-93-325-8600-0 First Impression This edition is manufactured in India and is authorized for sale only in India, Bangladesh, Bhutan, Pakistan, Nepal, Sri Lanka and the Maldives. Circulation of this edition outside of these territories is UNAUTHORIZED. Published by Pearson India Education Services Pvt. Ltd, CIN: U72200TN2005PTC057128. Formerly known as TutorVista Global Pvt. Ltd, licensee of Pearson Education in South Asia. Head Office: A-8 (A), 7th Floor, Knowledge Boulevard, Sector 62, Noida 201 309, Uttar Pradesh, India. Registered Office: 4th Floor, Software Block, Elnet Software City, TS-140, Block 2 & 9, Rajiv Gandhi Salai, Taramani, Chennai 600 113, Tamil Nadu, India. Fax: 080-30461003, Phone: 080-30461060 www.pearson.co.in, Email id: companysecretary.india@pearson.com Printed in India Si spy net work, big fedjaw iog link kyxogy This page is intentionally left blank vii CONTENTS xxvii xxxiii Preface 1 1.1.1 OSI Reference Model1 1.1.2 IP, UDP, and TCP2 1.1.3 Directory Service3 1.1.4 Replicated Services5 1.1.5 Packet Switching5 1.1.6 Network Components6 1.1.7 Destinations: Ultimate and Next-Hop7 1.1.8 Address Structure8 1.2 Active vs. Passive Attacks9 1.3 Layers and Cryptography9 1.4 Authorization9 1.5 Tempest10 1.6 Key Escrow for Law Enforcement11 1.7 Key Escrow for Careless Users13 1.8 Viruses, Worms, Trojan Horses13 1.8.1 Where Do They Come From?14 1.8.2 Spreading Pests from Machine to Machine17 1.8.3 Virus Checkers18 1.8.4 What Can We Do Today?19 1.8.5 Wish List for the Future20 1.9 The

Multi-level Model of Security	21
1.9.1 Mandatory (Nondiscretionary) Access Controls	22
1.9.2 Levels of Security	23
1.9.3 Mandatory Access Control Rules	23
1.9.4 Covert Channels	24
1.9.5 The Orange Book	26
1.9.6 Successors to the Orange Book	29
1.1 Primer on Networking.....	1 1.10
Legal Issues	
30 1.10.1 Patents	
.....30 1.10.2 Export Controls	31
PART 1 - CRYPTOGRAPHY CHAPTER 2 Introduction to Cryptography	35
2.1 What Is Cryptography?	35
2.1.1 Computational Difficulty	36
2.1.2 To Publish or Not to Publish....	37
2.1.3 Secret Codes.....	38
2.2 Breaking an Encryption Scheme....	
.....39 2.2.1 Ciphertext Only	39
.....39 2.2.2 Known Plaintext.	40
2.2.3 Chosen Plaintext.....	40
2.3 Types of Cryptographic Functions.....	41
2.4 Secret Key Cryptography	
..... 41 2.4.1 Security Uses of Secret Key Cryptography	41
2.4.2 Transmitting Over an Insecure Channel ...	42
2.4.3 Secure Storage on Insecure Media... ..	42
2.4.4 Authentication	42
2.4.5 Integrity Check.....	43
2.5 Public Key Cryptography.....	44
2.5.1 Security Uses of Public Key Cryptography	46
2.5.2 Transmitting Over an Insecure Channel	46
2.5.3 Secure Storage on Insecure Media....	46
2.5.4 Authentication	47
2.5.5 Digital Signatures.....	48
2.6 Hash Algorithms	
.....48 2.6.1 Password Hashing	49
.....49 2.6.2 Message Integrity	50
.....50 2.6.3 Message Fingerprint	50
2.6.4 Downline Load Security	51
2.6.5 Digital Signature Efficiency	51
2.7 Homework.....	
.....51 CHAPTER 3 Secret Key	

Cryptography	53
3.1 Introduction	53
3.2 Generic Block Encryption	53
3.3 Data Encryption Standard (DES)	56
3.3.1 DES Overview	58
3.3.2 The Permutations of the Data	60
3.3.3 Generating the Per-Round Keys	61
3.3.4 A DES Round	63
3.3.5 The Mangler Function	64
3.3.6 Weak and Semi-Weak Keys	68
3.3.7 What's So Special About DES?	68
3.4 International Data Encryption Algorithm (IDEA)	69
3.4.1 Primitive Operations	69
3.4.2 Key Expansion	71
3.4.3 One Round	72
3.4.3.1 Odd Round	72
3.4.3.2 Even Round	73
3.4.4 Inverse Keys for Decryption	74
3.4.5 Does IDEA Work?	75
3.5 Advanced Encryption Standard (AES)	75
3.5.1 Basic Structure	76
3.5.2 Primitive Operations	78
3.5.2.1 What about the inverse cipher?	81
3.5.3 Key Expansion	83
3.5.4 Rounds	84
3.5.5 Inverse Rounds	85
3.5.6 Optimization	85
3.6 RC4	86
3.7 Homework	86 x
CONTENTS CHAPTER 4 Modes of Operation	89
4.1 Introduction	89
4.2 Encrypting a Large Message	89
4.2.1 Electronic Code Book (ECB)	90
4.2.2 Cipher Block Chaining (CBC)	91
4.2.2.1 CBC Threat 1—Modifying Ciphertext Blocks	93
4.2.2.2 CBC Threat 2—Rearranging Ciphertext Blocks	94
4.2.3 Output Feedback Mode (OFB)	95
4.2.4 Cipher Feedback Mode (CFB)	96
4.2.5 Counter Mode (CTR)	98
4.3 Generating MACs	99
4.3.1 Ensuring Privacy and Integrity Together	100
4.3.2 CBC with a Weak Cryptographic Checksum	101
4.3.3 CBC Encryption and CBC Residue with Related Keys	102
4.3.4 CBC with a Cryptographic Hash	102
4.3.5 Offset Codebook Mode (OCB)	102
4.4 Multiple	

Encryption DES.....	103 4.4.1
How Many Encryptions?.....	105 4.4.1.1
Encrypting Twice with the Same Key	105 4.4.1.2
Encrypting Twice with Two Keys.....	105 4.4.1.3
Encryption with only Two Keys.....	106 4.4.2
CBC Outside vs. Inside	107 4.5
Homework.....	
.....	108
CHAPTER 5 Hashes and Message Digests	111
5.1 Introduction	
.....	111
5.2 Nifty Things to Do with a Hash	115 5.2.1
Authentication	117 5.2.2
Computing a MAC with a Hash..	117 5.2.3
Encryption with a Message Digest	119 5.2.3.1
Generating a One-Time Pad	119 5.2.3.2
Mixing In the Plaintext	120
CONTENTS xi	5.2.4
Using Secret Key for a Hash.....	120 5.2.4.1
UNIX Password Hash.	120 5.2.4.2
Hashing Large Messages	121
5.3 MD2	
.....	122 5.3.1
MD2 Padding	123 5.3.2
MD2 Checksum Computation....	123 5.3.3
MD2 Final Pass	125 5.4
MD4	127
5.4.1 MD4 Message Padding	127
5.4.2 Overview of MD4 Message Digest Computation ...	127
5.4.3 MD4 Message Digest Pass 1	129
5.4.4 MD4 Message Digest Pass 2.....	129
5.4.5 MD4 Message Digest Pass 3.....	130
5.5 MD5 ..	
..	130 5.5.1
MD5 Message Padding	
.....	131 5.5.2
Overview of MD5 Message Digest Computation	131 5.5.3
MD5 Message Digest Pass 1.....	
.....	132 5.5.4
MD5 Message Digest Pass 2.....	
.....	132 5.5.5
MD5 Message Digest Pass 3..	
.....	133 5.5.6
MD5 Message Digest Pass 4.....	133 5.6
SHA-1.....	
.....	134
5.6.1 SHA-1 Message Padding	134
5.6.2 Overview of SHA-1 Message Digest Computation .	134
5.6.3 SHA-1 Operation on a 512-bit Block	135
5.7 HMAC.....	
.....	136 5.8
Homework.....	
.....	137
CHAPTER 6 Public Key Algorithms	141
6.1 Introduction	
.....	141 6.2
Modular Arithmetic	
.....	142 6.2.1
Modular	

Addition	142	6.2.2 Modular
Multiplication	143	6.2.3 Modular
Exponentiation.....	145	6.3 RSA
.....		
.....	146	6.3.1 RSA Algorithm.....
.....	146	6.3.2 Why Does RSA Work?
.....	147	6.3.3 Why Is RSA
Secure?.....	147	6.3.4 How Efficient
Are the RSA Operations?	148	6.3.4.1 Exponentiating
with Big Numbers	148	6.3.4.2 Generating RSA Keys.
.....	150	6.3.4.2.1 Finding Big Primes p and q
.....	150	6.3.4.2.2 Finding d and e
.....	152	6.3.4.3 Having a Small Constant
e.....	152	6.3.4.4 Optimizing RSA Private Key
Operations	154	6.3.5 Arcane RSA Threats.....
.....	155	6.3.5.1 Smooth Numbers ..
.....	155	6.3.5.2 The Cube Root Problem
.....	156	6.3.6 Public-Key Cryptography
Standard (PKCS).....	157	6.3.6.1 Encryption.....
.....	157	6.3.6.2 Encryption—Take 2..
.....	158	6.3.6.3 Signing
.....	159	6.4 Diffie-Hellman
.....	160	6.4.1 The
Bucket Brigade/Man-in-the-Middle Attack	161	6.4.2
Defenses Against Man-in-the-Middle Attack	163	6.4.2.1
Published Diffie-Hellman Numbers	163	6.4.2.2
Authenticated Diffie-Hellman	163	6.4.3
Encryption with Diffie-Hellman.	164	6.4.4
ElGamal Signatures	164	6.4.5
Diffie-Hellman Details—Safe Primes	165	6.5
Digital Signature Standard (DSS)		
.....	166	6.5.1 The DSS Algorithm.....
.....	166	6.5.2 Why Does the Verification
Procedure Work?.....	168	6.5.3 Why Is This
Secure?.....	168	6.5.4 The DSS
Controversy.....	169	6.5.5 Per-
Message Secret Number	170	xii
CONTENTS CONTENTS xiii		
6.6 How Secure Are RSA and Diffie-Hellman?		
.....	171	6.7 Elliptic Curve Cryptography
(ECC).....	172	6.8 Zero Knowledge Proof
Systems.....	173	6.8.1 Zero
Knowledge Signatures	175	6.9
Homework Problems.....		
.....	176	179 7.1 Password-Based
Authentication.....	179	7.1.1 Off-
vs. On-Line Password Guessing	181	7.1.2 Storing
User Passwords.....	181	7.2 Address-
Based Authentication.....	183	

7.2.1 Network Address Impersonation.	185
7.3 Cryptographic Authentication Protocols ...	
.....	186
7.4 Who Is Being Authenticated?	
.....	187
7.5 Passwords as	
Cryptographic Keys	187
7.6	
Eavesdropping and Server Database Reading	
.....	188
7.7 Trusted Intermediaries	
.....	190
7.7.1	
KDCs.....	191
7.7.2	
Certification Authorities (CAs).....	192
7.7.3	
Certificate Revocation	193
7.7.4	
Multiple Trusted Intermediaries ..	194
7.7.4.1	
Multiple KDC Domains.....	194
7.7.4.2 Multiple	
CA Domains.....	196
7.8 Session Key	
Establishment.....	197
7.9	
Delegation.....	
.....	198
7.10 Homework	
.....	200
CHAPTER 8	
201 8.1 Passwords	
.....	202
8.2 On-Line Password Guessing	
.....	202
8.3 Off-Line Password	
Guessing.....	205
8.4 How Big	
Should a Secret Be?	207
8.5	
Eavesdropping	
.....	208
8.6 Passwords and Careless	
Users.....	209
8.6.1 Using a	
Password in Multiple Places	210
8.6.2 Requiring	
Frequent Password Changes	210
8.6.3 A Login	
Trojan Horse to Capture Passwords.....	211
8.6.4 Non-Login	
Use of Passwords.....	212
8.7 Initial	
Password Distribution.....	213
8.8 Authentication Tokens.....	
.....	214
8.9 Physical Access	
.....	217
8.10	
Biometrics.....	
.....	217
8.11 Homework	
.....	219
CHAPTER 9	
221 9.1 Login Only.....	
.....	222
9.1.1 Shared Secret	
.....	222
9.1.2 One-Way	
Public Key.....	226
9.2 Mutual	
Authentication.....	228
9.2.1 Reflection Attack.....	228
9.2.2 Password Guessing.....	230
9.2.3 Public Keys.....	231
9.2.4 Timestamps.....	232
9.3 Integrity/Encryption for Data	
.....	233
9.3.1 Shared Secret	

.....	233	9.3.2 Two-Way
Public Key Based Authentication	235	9.3.3 One-Way
Public Key Based Authentication	236	9.3.4 Privacy and
Integrity	236	9.4 Mediated
Authentication (with KDC).....	238	9.4.1 Needham-Schroeder
.....	239	9.4.2 Expanded Needham-Schroeder ..
.....	241	9.4.3 Otway-Rees
.....	242	9.5 Nonce
Types.....	244	
xiv CONTENTS CONTENTS xv		9.6 Picking Random Numbers
.....	246	9.7 Performance
Considerations	248	9.8
Authentication Protocol Checklist		
.....	249	9.9
Homework.....		
.....	252	CHAPTER 10 Strong Password
Protocols	255	10.1 Introduction
.....	255	10.2 Lamport's
Hash.....	256	10.3
Strong Password		
Protocols.....	259	10.3.1 The
Basic Form.....	259	10.3.2
Subtle Details	260	10.3.3
Augmented Strong Password Protocols	262	10.3.4
SRP (Secure Remote Password)	263	10.4
Strong Password Credentials Download Protocols.....		
.....	264	10.5 Homework.....
.....	265	PART 3 - STANDARDS CHAPTER 11
Kerberos V4	269	11.1 Introduction
.....	269	11.2 Tickets and Ticket-Granting
Tickets.....	270	11.3 Configuration
.....	271	11.4
Logging Into the Network		
.....	272	11.4.1 Obtaining a Session Key and
TGT.....	372	11.4.2 Alice Asks to Talk to a Remote
Node.	273	11.5 Replicated
KDCs.....	276	11.6
Realms.....		
.....	277	11.7 Interrealm Authentication ..
.....	278	11.8 Key Version
Numbers	279	11.9
Encryption for Privacy and Integrity.....		
.....	280	11.10 Encryption for Integrity
Only.....	282	11.11 Network Layer
Addresses in Tickets	283	11.12
Message Formats.....		
.....	284	xvi 11.12.1 Tickets
.....	286	11.12.2 Authenticators

.....	287	11.12.3
Credentials.....	288	
11.12.4 AS_REQ.....	290	
11.12.5 TGS_REQ	290	
11.12.6 AS_REP and TGS_REP.....	291	
11.12.7 Error Reply from KDC.....	293	
11.12.8 AP_REQ.....	293	
11.12.9 AP_REP.....	294	
11.12.10 Encrypted Data (KRB_PRV)	295	
11.12.11 Integrity-Checked Data (SAFE).....	295	
11.12.12 AP_ERR	297	
11.13 Homework		
.....;	298	
CHAPTER 12 Kerberos V5	299	
12.1 ASN.1		
.....	299	12.2
Names.....		
.....	301	12.3 Delegation of
Rights.....	301	12.4
Ticket Lifetimes.....		
.....	304	12.4.1 Renewable
Tickets.....	304	12.4.2 Postdated
Tickets.....	305	12.5 Key Versions
.....	306	12.6
Making Master Keys in Different Realms Different.....	306	
12.7 Optimizations		
.....	307	12.8 Cryptographic
Algorithms.....	307	12.8.1
Integrity-Only Algorithms.....	309	12.8.1.1
rsa-md5-des.....	308	12.8.1.2 des-
mac	309	12.8.1.3 des-mac-
k.....	310	12.8.1.4 rsa-md4-
des.....	310	12.8.1.5 rsa-md4-des-k
.....	310	12.8.2 Encryption for Privacy
and Integrity.....	311	12.9
Hierarchy of Realms.....		
.....	311	12.10 Evading Password-
Guessing Attacks	314	12.11 Key Inside
Authenticator.....	315	12.12
Double TGT		
Authentication.....	315	12.13
PKINIT—Public Keys for Users.....	316	
12.12 KDC Database		
.....	317	12.15 Kerberos V5 Messages
.....	318	12.15.1
Authenticator	318	12.15.2
Ticket	319	12.15.3
AS_REQ.....	319	12.15.4
TGS_REQ.....	321	12.15.5

AS_REP.....	322 12.15.6
TGS_REP	324 12.15.7
AP_REQ.....	324 12.15.8
AP_REP.....	325 12.15.9
KRB_SAFE.....	325 12.15.10
KRB_PRIV.....	326 12.15.11
KRB_CRED	326 12.15.12
KRB_ERROR	327 12.16
Homework.....	
.....	331 CHAPTER 13 333
13.1 Introduction	
.....	333 13.2 Some
Terminology.....	334
13.3 PKI Trust Models	
.....	334 13.3.1 Monopoly
Model.....	334 13.3.2 Monopoly
plus Registration Authorities (RAs) ...	335 13.3.3 Delegated
CAs.....	335 13.3.4
Oligarchy.....	336 13.3.5
Anarchy Model.....	337 13.3.6
Name Constraints	338 13.3.7
Top-Down with Name Constraints	338 xviii
13.3.8 Bottom-Up with Name Constraints.....	339
13.3.9 Relative Names	342
13.3.10 Name Constraints in Certificates.....	342
13.3.11 Policies in Certificates....	343
13.4	
Revocation.....	
.344 13.4.1 Revocation Mechanisms	
.....	345 13.4.1.1 Delta CRLs
.....	345 13.4.1.2 First Valid Certificate
.....	346 13.4.2 OLRs Schemes
.....	346 13.4.3 Good-lists vs. Bad-lists
.....	347 13.5 Directories and PKI.....
.....	348 13.5.1 Store
Certificates with Subject or Issuer?	349 13.5.2 Finding
Certificate Chains ...	350 13.6 PKIX and
X.509.....	351 13.6.1
Names.....	351 13.6.2
OIDs	352 13.6.3
Specification of Time	353 13.7
X.509 and PKIX Certificates	
.....	353 13.7.1 X.509 and PKIX CRLs.....
.....	357 13.8 Authorization Futures.....
.....	357 13.8.1 ACL (Access
Control List)	358 13.8.2 Central
Administration/Capabilities.....	358 13.8.3 Groups
.....	359 13.8.3.1

Cross-Organizational and Nested Groups	359	13.8.4 Roles...
.....	360	13.8.5
Anonymous Groups.....	362	13.9
Homework.....	363	CHAPTER 14 Real-time
Communication Security 365 14.1 What Layer?	365	14.2 Session Key
Establishment.....	368	14.3
Perfect Forward Secrecy.....	369	CONTENTS CONTENTS xix 14.4 PFS-Foilage
.....	371	14.5 Denial-of-
Service/Clogging Protection	372	14.5.1
Cookies	372	14.5.2
Puzzles.....	373	14.6
Endpoint Identifier Hiding	374	14.7 Live Partner Reassurance
.....	375	14.8 Arranging for
Parallel Computation... ..	377	14.9
Session Resumption.....	378	14.10 Plausible Deniability
.....	378	14.11 Data Stream
Protection.....	379	14.12
Negotiating Crypto Parameters	381	14.13 Easy Homework
.....	382	14.14
Homework	382	CHAPTER 15 IPSEC: AH And
ESP 385 15.1 Overview of IPsec	385	15.1.1 Security Associations
.....	385	15.1.2 Security Association
Database ..	386	15.1.3 Security Policy
Database.....	386	15.1.4 AH and
ESP.....	386	15.1.5 Tunnel,
Transport Mode.....	387	15.1.6 Why
Protect the IP Header?	389	15.2 IP and
IPv6	389	
15.2.1 NAT (Network Address Translation).....	390	
15.2.2 Firewalls	391	
15.2.3 IPv4 Header	392	
15.2.4 IPv6 Header	393	
15.3 AH (Authentication Header)	394	15.3.1 Mutable, Immutable
.....	395	15.3.2 Mutable but
Predictable.....	396	15.4 ESP
(Encapsulating Security Payload).....	397	
15.5 So, Do We Need AH?	398	xx 15.6 Comparison of Encodings
.....	399	15.7 Easy Homework

.....	400 15.8
Homework	
.....	400 CHAPTER 16 IPsec: IKE 403
16.1 Photuris.....	
.....	404 16.2 SKIP
.....	405
16.3 History of IKE.....	
.....	406 16.4 IKE Phases
.....	407 16.5
Phase 1 IKE.....	
.....	408 16.5.1 Aggressive Mode
and Main Mode	408 16.5.2 Key Types
.....	410 16.5.3 Proof of
Identity	411 16.5.4 Cookie
Issues.....	412 16.5.5
Negotiating Cryptographic Parameters	413 16.5.6
Session Keys	414 16.5.7
Message IDs	416 16.5.8
Phase 2/Quick Mode	416 16.5.9
Traffic Selectors	416
16.5.10 The IKE Phase 1 Protocols.....	417
16.5.10.1 Public Signature Keys, Main Mode.....	417 16.5.10.2
Public Signature Keys, Aggressive Mode	418 16.5.10.3 Public
Encryption Key, Main Mode, Original .	419 16.5.10.4 Public Encryption Key, Aggressive Mode,
Original	420 16.5.10.5 Public Encryption Key, Main Mode, Revised..
.....	420 16.5.10.6 Public Encryption Key, Aggressive Mode, Revised
.....	421 16.5.10.7 Shared Secret Key, Main Mode.....
.....	421 16.5.10.8 Shared Secret Key, Aggressive Mode ..
.....	422 16.6 Phase-2 IKE: Setting up IPsec SAs.....
.....	424 16.7 ISAKMP/IKE
Encoding.....	425 16.7.1
Fixed Header	427 16.7.2
Payload Portion of ISAKMP Messages	429
CONTENTS CONTENTS xxi 16.7.3 SA Payload.....	
.....	429 16.7.3.1 Ps and Ts within the SA
Payload.....	430 16.7.3.2 Payload Length in SA, P, and T
Payloads.....	430 16.7.3.3 Type of Next Payload
.....	430 16.7.3.4 SA Payload Fields
.....	431 16.7.4 P Payload.....
.....	432 16.7.5 T Payload.....
.....	433 16.7.6 KE Payload.....
.....	434 16.7.7 ID
Payload.....	434 16.7.8
Cert Payload	435 16.7.9
Certificate Request Payload ...	436 16.7.10
Hash/Signature/Nonce Payloads	436 16.7.11
Notify Payload.....	436 16.7.12
Vendor ID Payload.....	437 16.8

Homework.....	
.....	438
PART 4 -	
ELECTRONIC MAIL CHAPTER 17 Electronic Mail Security	441
17.1 Distribution	
Lists.....	441
17.2	
Store and Forward	
.....	444
17.3 Security Services for Electronic	
Mail	445
17.4 Establishing	
Keys.....	446
17.4.1	
Establishing Public Keys.....	
.....	447
17.4.2 Establishing Secret	
Keys.....	447
17.5	
Privacy.....	
.....	448
17.5.1 End-to-End	
Privacy	448
17.5.2 Privacy with	
Distribution List Exploders.....	449
17.6 Authentication of	
the Source.....	450
17.6.1 Source	
Authentication Based on Public Key Technology	450
17.6.2 Source	
Authentication Based on Secret Keys	451
17.6.3 Source	
Authentication with Distribution Lists....	452
xxii	
17.7 Message	
Integrity	452
17.7.1 Message Integrity without Source Authentication	453
17.8 Non-Repudiation	
.....	454
17.8.1 Non-Repudiation	
Based on Public Key Technology	454
17.8.2 Plausible Deniability	
Based on Public Key Technology	454
17.8.3 Non-Repudiation with	
Secret Keys.....	455
17.9 Proof of Submission	
.....	456
17.10 Proof of	
Delivery.....	456
17.11	
Message Flow Confidentiality	
.....	457
17.12	
Anonymity.....	
.....	457
17.13 Containment	
.....	459
17.14	
Annoying Text Format Issues	
.....	459
17.14.1 Disguising Data as Text ..	
.....	461
17.15 Names and	
Addresses.....	463
17.16	
Verifying When a Message Was Really Sent	464
17.16.1 Preventing Backdating	464
17.16.2 Preventing Postdating.....	465
17.17 Homework.....	
.....	465
CHAPTER 18 PEM & S/MIME	469
18.1 Introduction	
.....	469
18.2 Structure of a PEM	
Message.....	470
18.3	
Establishing Keys.....	
.....	473
18.4 Some PEM	
History.....	474
18.5	

PEM Certificate Hierarchy.....	476
.....	476
18.6 Certificate Revocation Lists (CRLs)	478
18.7 Reformatting Data to Get Through Mailers	479
18.8 General Structure of a PEM Message ..	480
18.9 Encryption	481
.....	481
18.10 Source Authentication and Integrity Protection	482
.....	483
18.11 Multiple Recipients	483
18.12 Bracketing PEM Messages.....	484
CONTENTS CONTENTS xxiii	
18.13 Forwarding and Enclosures	487
.....	487
18.13.1 Forwarding a Message.....	487
18.14 Unprotected Information	489
.....	489
18.15 Message Formats	490
.....	490
18.15.1 ENCRYPTED, Public Key Variant.....	491
18.15.2 ENCRYPTED, Secret Key Variant.....	494
18.15.3 MIC-ONLY or MIC-CLEAR, Public Key Variant	496
18.15.4 MIC-ONLY and MIC-CLEAR, Secret Key Variant	497
18.15.5 CRL-RETRIEVAL-REQUEST	498
18.15.6 CRL	498
18.16 DES-CBC as MIC Doesn't Work.....	498
18.17 Differences in S/MIME.....	501
.....	501
18.18 S/MIME Certificate Hierarchy	504
.....	504
18.18.1 S/MIME with a Public Certifier	504
18.18.2 S/MIME with an Organizational Certifier.....	504
18.18.3 S/MIME with Certificates from Any Old CA ...	504
18.19 Homework	505
CHAPTER 19 PGP (Pretty Good Privacy) 507	
19.1 Introduction	507
.....	507
19.2 Overview	508
19.3 Key Distribution	509
.....	509
19.4 Efficient Encoding.....	511
19.5 Certificate and Key Revocation.....	512
.....	512
19.6 Signature Types	513
.....	513
19.7 Your Private Key.....	513
19.8 Key Rings	514
.....	514
19.9 Anomalies.....	514
.....	514
19.9.1 File Name	514
.....	514
19.9.2 People Names	515
.....	515
19.10 Object Formats	515
.....	515
19.10.1 Message Formats	516
.....	516
19.10.2	

Primitive Object Formats ..	517	xxiv	PART
5 - LEFTOVERS CHAPTER 20 Firewalls	525		
20.1 Packet Filters	528		
20.2 Application Level Gateway.....	529		
20.3 Encrypted Tunnels.....	531		
20.4 Comparisons.....	532		
20.5 Why Firewalls Don't Work.....	532		
20.6 Denial-of-Service Attacks	533		
20.7 Should Firewalls Go Away?	534		
CHAPTER 21 More Security Systems	535		
21.1 NetWare V3.....	535		
21.2 NetWare V4.....	537		
21.2.1 NetWare's Guillou-Quisquater Authentication Scheme	540		
21.3 KryptoKnight	542		
21.3.1 KryptoKnight Tickets.....	543		
21.3.2 Authenticators	544		
21.3.3 Nonces vs. Timestamps.....	544		
21.3.4 Data Encryption.....	545		
21.4 DASS/SPX	545		
21.4.1 DASS Certification Hierarchy .	545		
21.4.2 Login Key.....	546		
21.4.3 DASS Authentication Handshake	548		
21.4.4 DASS Authenticators	548		
21.4.5 DASS Delegation	549		
21.4.6 Saving Bits	549		
21.5 Lotus Notes Security	550		
21.5.1 ID Files.....	551		
21.5.2 Coping with Export Controls	552		
21.5.3 Certificates for Hierarchical Names.....	553		
21.5.4 Certificates for Flat Names	554		
21.5.5 Lotus Notes Authentication....	556		
21.5.6 The Authentication Long-Term Secret	556		
21.5.7 Mail	557		
21.5.8 Certification Revocation	557		
21.6 DCE Security.....	557		
21.7 Microsoft Windows Security	562		
21.7.1 LAN Manager and NTLM	562		
21.7.2 Windows 2000 Kerberos.....	564		
21.8 Network Denial of Service	566		
21.8.1 Robust Broadcast.....	566		
21.8.2 Robust Packet Delivery.....	568		
21.9 Clipper			

.....	569
21.9.1 Key Escrow	572
21.10 Homework.....	
.....	573
Folklore 575	22.1 Perfect Forward Secrecy.....
.....	575
.....	22.2 Change Keys Periodically
.....	576
Flows over a Single SA	22.3 Multiplexing
.....	577
Splicing Attack.....	22.3.1 The
.....	577
Service Classes	22.3.2
.....	578
Different Cryptographic Algorithms	22.3.3
.....	578
Different Keys in the Two Directions	22.4 Use
.....	579
22.5 Use Different Secret Keys for Encryption vs. Integrity Protection	
.....	579
.....	22.6 Use Different Keys for Different Purposes
.....	580
Encryption.....	22.7 Use Different Keys for Signing vs.
.....	580
to the Master Key	22.8 Have Both Sides Contribute
.....	581
Determine the Key ..	22.9 Don't Let One Side
.....	581
Constant When Hashing a Password.....	22.10 Hash in a
.....	582
HMAC Rather than Simple MD.....	22.11
.....	583
22.12 Key Expansion.....	
.....	583
.....	22.13 Randomly Chosen
IVs.....	584
.....	22.14 Use of
Nonces in Protocols	585
22.15 Don't Let Encrypted Data Begin with a Constant.....	xxvi
.....	585
.....	22.16 Don't Let Encrypted Data Begin with a
Predictable Value	586
.....	22.17 Compress Data Before
Encrypting It ...	586
.....	22.18 Don't Do
Encryption Only	587
22.19	
Avoiding Weak Keys	
.....	587
.....	22.20 Minimal vs. Redundant
Designs.....	588
.....	22.21 Overestimate
the Size of Key	588
22.22	
Hardware Random Number Generators	
.....	589
.....	22.23 Timing Attacks
.....	589
.....	22.24 Put
Checksums at the End of Data ...	590
22.25 Forward Compatibility	
.....	591
.....	22.25.1 Options
.....	591
.....	22.25.2 Version
Numbers.....	592
.....	22.25.2.1
Version Number Field Must Not Move.....	592
.....	22.25.2.2
Negotiating Highest Version Supported.....	592
.....	22.25.2.3 Minor
Version Number Field	593
.....	22.25.3 Vendor Options
.....	594
22.26 Negotiating	
Parameters	594
22.27	
Homework.....	
.....	595
.....	597
.....	607
.....	625
.....	Bibliography

Glossary Index Online Chapters CHAPTER 23 Number Theory 641 CHAPTER 24 Math with AES and Elliptic Curves 653 CHAPTER 25 SSL/TLS 669 CHAPTER 26 Web Issues 691 CONTENTS xxviii PREFACE

It was a dark and stormy night. Somewhere in the distance a dog howled. A shiny object caught Alice's eye. A diamond cufflink! Only one person in the household could afford diamond cufflinks! So it was the butler, after all! Alice had to warn Bob. But how could she get a message to him without alerting the butler? If she phoned Bob, the butler might listen on an extension. If she sent a carrier pigeon out the window with the message taped to its foot, how would Bob know it was Alice that was sending the message and not Trudy attempting to frame the butler because he spurned her advances? That's what this book is about. Not much character development for Alice and Bob, we're afraid; nor do we really get to know the butler. But we do discuss how to communicate securely over an insecure medium. What do we mean by communicating securely? Alice should be able to send a message to Bob that only Bob can understand, even though Alice can't avoid having others see what she sends. When Bob receives a message, he should be able to know for certain that it was Alice who sent the message, and that nobody tampered with the contents of the message in the time between when Alice launched the message and Bob received it. What do we mean by an insecure medium? Well, in some dictionary or another, under the definition of "insecure medium" should be a picture of the Internet. The world is evolving towards interconnecting every computer, and people talk about connecting household appliances as well, all into some wonderful global internetwork. How wonderful! You'd be able to send electronic mail to anyone in the world. You'd also be able to control your nuclear power plant with simple commands sent across the network while you were vacationing in Fiji. Or sunny Libya. Or historic Iraq. Inside the network the world is scary. There are links that eavesdroppers can listen in on. Information needs to be forwarded through packet switches, and these switches can be reprogrammed to listen to or modify data in transit. The situation might seem hopeless, but we may yet be saved by the magic of mathematics, and in particular cryptography, which can take a message and transform it into a bunch of numbers known as ciphertext. The ciphertext is unintelligible gibberish except to someone who knows the secret to reversing the transformation. Cryptography allows us to disguise our data so that eavesdroppers gain no information from listening to the information as transmitted. Cryptography also allows us to create an unforgeable message and detect if it has been modified in transit. One method of accomplishing this is with a digital signature, a number associated with a message and its sender that can be verified as authentic by others, but can only be generated by the sender. This should seem astonishing. How can there be a number which you can verify but not generate? A person's handwritten signature can (more or less) only be generated by that person, though it can be verified by others. But it would seem as if a number shouldn't be hard to generate, especially if it can be verified. Theoretically, you could generate someone's signature by trying lots of numbers and testing each one until one passed the verification test. But with the size of the numbers used, it would take too much compute time (for instance, several universe lifetimes) to generate the signature that way. So a digital signature has the same property as a handwritten signature, in that it can only be generated by one person. But a digital signature does more than a handwritten signature. Since the digital signature depends on the contents of the message, if someone alters the message the signature will no longer be correct and the tampering will be detected. This will all become clear if you read Chapter 2 Introduction to Cryptography. Cryptography is a major theme in this book, not because cryptography is intrinsically interesting (which it is), but because many of the security features people want in a computer network can best be provided through cryptography. ROADMAP TO THE BOOK After this introductory chapter, there are five main sections in the book: • Part 1

CRYPTOGRAPHY Chapter 2 Introduction to Cryptography is the only part of the cryptography section of the book essential for understanding the rest of the book, since it explains the generic properties of secret key, message digest, and public key algorithms, and how each is used. We've tried our best to make the descriptions of the actual cryptographic algorithms nonthreatening yet thorough, and to give intuition into why they work. It's intended to be readable by anyone, not just graduate students in mathematics. Never once do we use the term lemma. We do hope you read Chapter 3 Secret Key Cryptography, Chapter 4 Modes of Operation, Chapter 5 Hashes and Message Digests, and Chapter 6 Public Key Algorithms which give the details of the popular standards, but it's also OK to skip them and save them for later, or just for reference.

- Part 2 AUTHENTICATION Chapter 7 Overview of Authentication Systems introduces the general issues involved in proving your identity across a network. Chapter 8 Authentication of People deals with the special circumstances when the device proving its identity is a human being. Chapter 9 Security Handshake Pitfalls deals with the details of authentication handshakes. There are many security flaws that keep getting designed into protocols. This chapter attempts to describe variations of authentication handshakes and their relative security and performance strengths. We end the chapter with a checklist of security attacks so that someone designing a protocol can specifically check their protocol for these flaws.
- Part 3 STANDARDS This portion of the book describes the standards: Kerberos versions 4 and 5, certificate and PKI standards, IPsec, and SSL. We hope that our descriptions will be much more readable than the standards themselves. And aside from just describing the standards, we give intuition behind the various choices, and criticisms where they are overly complex or have flaws. We hope that our commentary will make the descriptions more interesting and provide a deeper understanding of the design decisions. Our descriptions are not meant to, and cannot, replace reading the standards themselves, since the standards are subject to change. But we hope that after reading our description, it will be much easier to understand the standards.
- Part 4 ELECTRONIC MAIL Chapter 17 Electronic Mail Security describes the various types of security features one might want, and how they might be provided. Chapter 18 PEM & S/MIME and Chapter 19 PGP (Pretty Good Privacy) describe the specifics of PEM, S/MIME, and PGP.
- Part 5 LEFTOVERS Chapter 20 Firewalls talks about what firewalls are, what problems they solve, and what problems they do not solve. Chapter 21 More Security Systems, describes a variety of security systems, including Novell NetWare (Versions 3 and 4), Lotus Notes, DCE, KryptoKnight/NetSP, Clipper, SNMP, DASS/SPX, Microsoft (LAN Manager and Windows NT), and sabotage-proof routing protocols. We close with Chapter 22 Folklore, which describes the reasoning behind some of the advice you will hear from cryptographers.

WHAT TYPE OF BOOK IS THIS? We believe the reason most computer science is hard to understand is because of jargon and irrelevant details. When people work with something long enough they invent their own language, come up with some meta-architectural framework or other, and forget that the rest of the world doesn't talk or think that way. We intend this book to be reader-friendly. We try to extract the concepts and ignore the meta-architectural framework, since whatever a meta-architectural framework is, it's irrelevant to what something does and how it works. We believe someone who is a relative novice to the field ought to be able to read this book. But readability doesn't mean lack of technical depth. We try to go beyond the information one might find in specifications. The goal is not just to describe exactly how the various standards and de facto standards work, but to explain why they are the way they are, why some protocols designed for similar purposes are different, and the implications of the design decisions. Sometimes engineering tradeoffs were made. Sometimes the designers could have made better choices (they are human after all), in which case we explain how the protocol could have been better. This analysis should make it

easier to understand the current protocols, and aid in design of future protocols. The primary audience for this book is engineers, especially those who might need to evaluate the security of, or add security features to, a distributed system; but the book is also intended to be usable as a textbook, either on the advanced undergraduate or graduate level. Most of the chapters have homework problems at the end. Not all the chapters will be of interest to all readers. In some cases we describe and critique a standard in great detail. These chapters might not be of interest to students or people trying to get a conceptual understanding of the field. But in many cases the standards are written fairly unintelligibly. People who need to understand the standard, perhaps to implement it, or maybe even to use it, need to have a place where it is described in a readable way (and we strive for readability), but also a place in which mistakes in the standard are pointed out as such. It's very difficult to understand why, for instance, two fields are included which both give the same information. Sometimes it is because the designers of the protocol made a mistake. Once something like that is pointed out as a simple mistake, it's much easier to understand the specification. We hope that reading the descriptions in the book will make the specifications more intelligible.

TERMINOLOGY

Computer science is filled with ill-defined terminology used by different authors in conflicting ways, often by the same author in conflicting ways. We apologize in advance for probably being guilty sometimes ourselves. Some people take terminology very seriously, and once they start to use a certain word in a certain way, are extremely offended if the rest of the world does not follow. When I use a word, it means just what I choose it to mean—neither more nor less. — Humpty Dumpty (in *Through the Looking Glass*)

PREFACE xxxi

Some terminology we feel fairly strongly about. We do not use the term hacker to describe the vandals that break into computer systems. These criminals call themselves hackers, and that is how they got the name. But they do not deserve the name. True hackers are master programmers, incorruptibly honest, unmotivated by money, and careful not to harm anyone. The criminals termed “hackers” are not brilliant and accomplished. It is really too bad that they not only steal money, people's time, and worse, but they've also stolen a beautiful word that had been used to describe some remarkable and wonderful people. We instead use words like intruder, bad guy, and impostor. When we need a name for a bad guy, we usually choose Trudy (since it sounds like intruder). We grappled with the terms secret key and public key cryptography. Often in the security literature the terms symmetric and asymmetric are used instead of secret and public. We found the terms symmetric and asymmetric intimidating and sometimes confusing, so opted instead for secret key and public key. We occasionally regretted our decision to avoid the words symmetric and asymmetric when we found ourselves writing things like secret key based interchange keys rather than symmetric interchange keys. We use the term privacy when referring to the desire to keep communication from being seen by anyone other than the intended recipients. Some people in the security community avoid the term privacy because they feel its meaning has been corrupted to mean the right to know, because in some countries there are laws known as privacy laws which state that citizens have the right to see records kept about themselves. Privacy also tends to be used when referring to keeping personal information about people from being collected and misused. The security community also avoids the use of the word secrecy, because secret has special meaning within the military context, and they feel it would be confusing to talk about the secrecy of a message that was not actually labeled top secret or secret. The term most commonly used in the security community for keeping communication from being seen is confidentiality. We find that strange because confidential, like secret, is a security label, and the security community should have scorned use of confidential, too. In the first edition, we chose not to use confidentiality because we felt it had too many syllables, and saw no reason not to use privacy. For the second edition we reconsidered this decision, and

were about to change all use of privacy to confidentiality until one of us pointed out we'd have to change the title of the book to something like Network Security: Confidential Communication in a Non-Confidential World, at which point we decided to stick with privacy. Speaker: Isn't it terrifying that on the Internet we have no privacy? Heckler1: You mean confidentiality. Get your terms straight. Heckler2: Why do security types insist on inventing their own language? Heckler3: It's a denial-of-service attack. —Overheard at recent gathering of security types We often refer to things involved in a conversation by name, for instance, Alice and Bob, whether the things are people or computers. This is a convenient way of making things unambigu- xxxiii

PREFACE ous with relatively few words, since the pronoun she can be used for Alice and he can be used for Bob. It also avoids lengthy inter- (and even intra-) author arguments about whether to use the politically incorrect he, a confusing she, an awkward he/she or (s)he, an ungrammatical they, an impersonal it, or an incredibly awkward rewriting to avoid the problem. We remain slightly worried that people will assume when we've named things with human names that we are referring to people. Assume Alice, Bob, and the rest of the gang may be computers unless we specifically say something like the user Alice, in which case we're talking about a human. With a name like yours, you might be any shape, almost. —Humpty Dumpty to Alice (in *Through the Looking Glass*) Occasionally, one of the three of us authors will want to make a personal comment. In that case we use I or me with a subscript. When it's a comment that we all agree with, or that we managed to slip past me₃ (the rest of us are wimpier), we use the term we. **NOTATION** We use the symbol \oplus (pronounced ex-or) for the bitwise-exclusive-or operation. We use the symbol | for concatenation. We denote secret key encryption with curly brackets preceded by the key with which something was encrypted, as in $K\{\text{message}\}$, which means message is secret key encrypted with K. Public key encryption we denote with curly braces, and the name of the owner of the public key subscripting the close brace, as in $\{\text{message}\}\text{Bob}$. Signing (which means using the private key), we denote with square brackets, with the name of the owner of the key subscripting the close bracket, as in $[\text{message}]\text{Bob}$. **Table of Notation** \oplus bitwise exclusive or (pronounced ex-or) | concatenation (pronounced concatenated with) $K\{\text{message}\}$ message encrypted with secret key K $\{\text{message}\}\text{Bob}$ message encrypted with Bob's public key $[\text{message}]\text{Bob}$ message signed with Bob's private key xxxiii

ACKNOWLEDGMENTS Despite the controversies that crop up around security issues, it has been our experience that people in the security community are generally generous with their wisdom and time. It's always a little scary thanking specific people, for fear we'll leave someone out, but leaving everyone out seems wrong. It's not even the fair thing to do, since some people would be more egregiously wronged by being left out than others. Eric Rescorla and Hilarie Orman have been particularly helpful with answering questions and reviewing chapters for this edition. Other reviewers, and people who have been helpful answering questions, include Tom Wu, Kevin Fu, Marshall Rose, Joe Tardo, Joe Pato, Seth Proctor, Timothy Spiller, Tom Rice, Kristen McIntyre, Gary Winiger, Dan Harkins, Peter Memishian, Jeff Schiller, Burt Kaliski, Tony Lauck, Phil Karn, Ron Rivest, Steve Crocker, Steve Kent, John Linn, Steve Hanna, Jim Bidzos, Dave Jablon, Ted Ts'o, Matthew Barnes, Keith McCloughrie, Jeffrey Case, Kathrin Winkler, Philippe Auphelle, Sig Handelman, Phillip Hallam-Baker, Uri Blumenthal, Serge Vaudenay, and Boyd Roberts. We could not have done Chapter 21 More Security Systems without help from the various companies involved, since for the most part the security systems were previously undocumented. We'd like to thank Al Eldridge from Iris (Lotus Notes), Amir Herzberg and Mark Davis from IBM (KryptoKnight), Walt Tuvell from OSF, and Cliff Van Dyke from Microsoft (LAN Manager and Windows NT security) for explaining their systems to us, doing timely reviews of what we wrote, and being enthusiastic and supportive of the project. Although nearly 67% of us work for compa-nies that have products in this area, the opinions we

offer are ours alone, and not those of our companies. Mary Franz, our editor at Prentice Hall, has been enthusiastic and optimistic and patient with us throughout. She's shown good judgment about when to be helpful, when to keep out of the way, when to nag, and when to just look soulful so we feel guilty enough to meet a deadline. Despite the fact that this book has kept both of his parents busy for a significant part of his life, Ray Perlner has kept us inspired with his wholehearted and unselfish enthusiasm for the project. He's shown genuine interest in the subject matter, offered useful advice during interauthor arguments, helped search for quotes, reviewed part of the book, and particularly liked the subscripted pronouns. If we overdo those, it's just because it's fun to see him giggle. Dawn Perlner has also been a great supporter of the project, and manages to convince a surprising number of her friends, as well as complete strangers, to buy the book. xxxiv ACKNOWLEDGEMENTS And of course we thank you, our reader. We welcome your comments and suggestions. Compliments are always welcome. We hope to update the book periodically, so if there are topics you wish we'd covered or errors you'd like us to correct, let us know. Errata can be found at

<http://www.phptr.com/networksecurity>. Our current email addresses are ckaufman@us.ibm.com, radia@alum.mit.edu, and ms@alum.mit.edu. We wish to thank the following for their permission to use their quotes in this book: • Quote on page 10 from The Hollywood Book of Quotes, Omnibus Press. • Quotes on page 17 and page 25 Copyright © 1994 Newsweek, Inc. All rights reserved. Reprinted by permission. • Quote on page 43 reprinted by permission of Singer Media Corporation. • Quote on page 19 reprinted by permission of Turner Entertainment. • Quote on page 117 courtesy of Donald Knuth. • Quote on page 253 reprinted by permission of The Wall Street Journal, Copyright © 1992 Dow Jones & Company, Inc. 1 1.1

PRIMER ON NETWORKING You have to know something about computer networks to understand computer network security, so we're including this primer. For a more detailed understanding, we recommend PERL99, TANE96, COME00, STEV94, KURO00. Networks today need to be very easy to use and configure. Networks are no longer an expensive educational toy for researchers, but instead are being used by real people. Most sites with networks will not be able to hire a full-time person with networking expertise to start and keep the network running.

1.1.1 OSI Reference Model Somehow, a book about computer networks would seem incomplete without a picture of the OSI (Open Systems Interconnection) Reference Model, so here it is. The OSI Reference Model is useful because it gives some commonly used terminology, though it might mislead you into thinking that there is only one way to construct a network. The reference model was designed by an organization known as the International Standards Organization (ISO). The ISO decided it would be a good idea to standardize computer networking. Since that was too big a task for a single committee, they decided to subdivide the problem among several committees. They somewhat arbitrarily chose seven, each responsible for one layer. The basic idea is that each layer uses the services of the layer below, adds functionality, and provides a service to the layer above. When you start looking at real networks, they seldom neatly fit into the seven-layer model, but for basic understanding of networking, the OSI Reference Model is a good place to start. 1. physical layer. This layer delivers an unstructured stream of bits across a link of some sort. 2. data link layer. This layer delivers a piece of information across a single link. It organizes the physical layer's bits into packets and controls who on a shared link gets each packet. application layer presentation layer session layer transport layer network layer data link layer physical layer Figure 1-1. OSI Reference Model INTRODUCTION 2 INTRODUCTION 1.1.2 3. network layer. This layer computes paths across an interconnected mesh of links and packet switches, and forwards packets over multiple links from source to destination. 4. transport layer. This layer establishes a reliable communication stream between a pair of systems across a network by putting sequence numbers in packets,