

Telecommunications
LAW
in the
INTERNET
AGE

Sharon K. Black

Telecommunications Law in the Internet Age

The Morgan Kaufmann Series in Networking
Series Editor, David Clark, MIT

Telecommunications Law in the Internet Age
Sharon K. Black

Optical Networks: A Practical Perspective, 2e
Rajiv Ramaswami and Kumar N. Sivarajan

Internet QoS: Architectures and Mechanisms
Zheng Wang

TCP/IP Sockets in Java: Practical Guide for Programmers
Michael J. Donahoo and Kenneth L. Calvert

TCP/IP Sockets in C: Practical Guide for Programmers
Kenneth L. Calvert and Michael J. Donahoo

Multicast Communication: Protocols, Programming, and Applications
Ralph Wittmann and Martina Zitterbart

MPLS: Technology and Applications
Bruce Davie and Yakov Rekhter

High-Performance Communication Networks, 2e
Jean Walrand and Pravin Varaiya

Computer Networks: A Systems Approach, 2e
Larry L. Peterson and Bruce S. Davie

Internetworking Multimedia
Jon Crowcroft, Mark Handley, and Ian Wakeman

Understanding Networked Applications: A First Course
David G. Messerschmitt

Integrated Management of Networked Systems: Concepts, Architectures, and their Operational Application
Heinz-Gerd Hegering, Sebastian Abeck, and Bernhard Neumair

Virtual Private Networks: Making the Right Connection
Dennis Fowler

Networked Applications: A Guide to the New Computing Infrastructure
David G. Messerschmitt

Modern Cable Television Technology: Video, Voice, and Data Communications
Walter Ciciora, James Farmer, and David Large

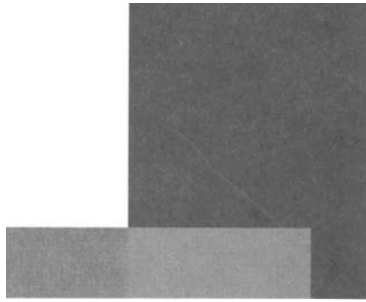
Switching in IP Networks: IP Switching, Tag Switching, and Related Technologies
Bruce S. Davie, Paul Doolan, and Yakov Rekhter

Wide Area Network Design: Concepts and Tools for Optimization
Robert S. Cahn

Practical Computer Network Analysis and Design
James D. McCabe

Frame Relay Applications: Business and Technology Case Studies
James P. Cavanagh

For further information on these books and for a list of forthcoming titles,
please visit our Web site at <http://www.mkp.com>.



Telecommunications Law in the Internet Age

Sharon K. Black, Attorney-at-Law

Law Offices of S. K. Black, Boulder, Colorado



MORGAN KAUFMANN PUBLISHERS

AN IMPRINT OF ACADEMIC PRESS

A Harcourt Science and Technology Company

SAN FRANCISCO SAN DIEGO NEW YORK BOSTON
LONDON SYDNEY TOKYO

Copyright Elsevier 2025

IPR2025-01572
Apple EX1044 Page 4

<i>Editor</i>	Rick Adams
<i>Publishing Services Manager</i>	Scott Norton
<i>Senior Production Editor</i>	Cheri Palmer
<i>Assistant Acquisitions Editor</i>	Karyn Johnson
<i>Project Management</i>	Dusty Friedman, The Book Company
<i>Cover Design</i>	Ross Carron Design
<i>Cover Image</i>	© Corbis Image/PictureQuest
<i>Text Design</i>	Andrew Ogus
<i>Composition</i>	Thompson Type
<i>Copyeditor</i>	Jane Loftus
<i>Proofreader</i>	Debra Gates
<i>Indexer</i>	Bill Meyers
<i>Printer</i>	Edwards Brothers

Designations used by companies to distinguish their products are often claimed as trademarks or registered trademarks. In all instances in which Morgan Kaufmann Publishers is aware of a claim, the product names appear in initial capital or all capital letters. Readers, however, should contact the appropriate companies for more complete information regarding trademarks and registration.

Morgan Kaufmann Publishers
340 Pine Street, Sixth Floor, San Francisco, CA 94104-3205, USA
<http://www.mkp.com>

ACADEMIC PRESS
A Harcourt Science and Technology Company
525 B Street, Suite 1900, San Diego, CA 92101-4495, USA
<http://www.academicpress.com>

Academic Press
Harcourt Place, 32 Jamestown Road, London, NW1 7BY, United Kingdom
<http://www.academicpress.com>

© 2002 by Academic Press
All rights reserved
Printed in the United States of America

06 05 04 03 02 5 4 3 2 1

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, or otherwise—without the prior written permission of the publisher.

Library of Congress Control Number: 2001094370

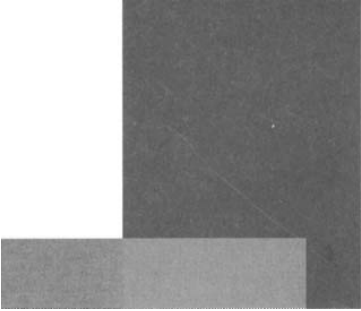
ISBN 1-55860-546-0

This book is printed on acid-free paper.



*This book is dedicated to my family,
Lisa, Craig, Sean, Andrea, Seth, and Isabella.*

This Page Intentionally Left Blank



Contents

Chapter 1

Introduction—The New Telecommunications Environment 1

- 1.1 New Transport Technologies 2
- 1.2 Converged Voice, Data, Video, and Graphics Systems 2
- 1.3 Legal Changes 3
 - 1.3.1 *Breakup of the Bell System* 3
 - 1.3.2 *The Internet* 4
 - 1.3.3 *Changes in State Law* 4
 - 1.3.4 *The Telecommunications Act of 1996* 4
 - 1.3.5 *World Trade Organization Agreement of 1997* 5
- 1.4 International Telecommunications Equipment Markets 5
- 1.5 Technical Standards 6
- 1.6 What Is Communicated? 6
- 1.7 With Whom Are We Communicating? 7
- 1.8 Where Are We Communicating? 7
- 1.9 New Local Access Options 7
- 1.10 Universal Service Fund Support of Internet Connections 8
- 1.11 Structural Changes 8
- Conclusion 9
- Endnotes 9

PART I

THE NEW COMPETITIVE TELECOMMUNICATIONS ENVIRONMENT

Chapter 2

Competition and Regulation—a Continuing Telecommunications Cycle 11

- 2.1 Competition versus Regulation—Seeking a Balance 12
 - 2.1.1 *Rise of Trusts and Anticompetitive Behavior* 12
 - 2.1.2 *Antitrust Law and Regulation* 13
 - 2.1.3 *Impact of Technological Changes* 16
- 2.2 Early Competition in the Communications Industry 17
 - 2.2.1 *Telegraph* 17
 - 2.2.2 *International Telegraph Communications* 18
 - 2.2.3 *Equipment Manufacturing* 18
 - 2.2.4 *Telephone* 19
- 2.3 The Rise of the Bell System Dominance 21
 - 2.3.1 *Bell's Patent Exclusivity and Return on Investment* 21
 - 2.3.2 *AT&T Parent over Bell System and Western Union* 22
 - 2.3.3 *AT&T's Refusal to Interconnect with Competitors* 22

2.4	Regulation of the Communications Industry	23
2.4.1	1912 Antitrust Case: Settled with 1913 Kingsbury Commitment	23
2.4.2	Universal Service	24
2.4.3	1921 The Willis-Graham Act	26
2.4.4	1934 Communications Act	27
2.4.5	1949 Antitrust Case: Settled with 1956 Consent Decree	27
2.4.6	1974 Antitrust Case: Settled with 1982 Modified Final Judgment	28
2.5	Technological Convergence and Renewed Competition	29
2.5.1	Customer Premises Equipment	30
2.5.2	Microwave	31
2.5.3	Undersea Cables	33
2.5.4	Satellites	35
2.5.5	Computers	39
	Conclusion	47
	Endnotes	48

Chapter 3

The Telecommunications Act of 1996 55

3.1	Purpose of the Telecommunications Act of 1996	56
3.1.1	Federal Action	56
3.1.2	States' Action	59
3.2	Structure and Organization of the 1996 Act—47 U.S.C. §§ 151 <i>et seq.</i>	59
3.3	Definitions—Section 3 of the Telecommunications Act of 1996	61
3.3.1	Three-Pronged Definition of Telecommunications	61
3.3.2	Definitions of Carriers	63
3.3.3	Definitions of Equipment	67
3.4	Provisions to Open the Competitive Market	68
3.4.1	Three Ways to Enter the New Competitive Market, 251(c)(2-4)	68
3.4.2	Implementation of the 1996 Act, § 251(d)(1)	70
3.4.3	Process for Writing Interconnection Agreements, § 252	72
3.4.4	Post-Approval Issues	74

3.5	Duties and Obligations of Carriers	75
3.5.1	All Telecommunications Carriers, § 251(a)	76
3.5.2	Duties of Local Exchange Carriers, § 251(b)	79
3.5.3	Duties of Incumbent Local Exchange Carriers, § 251(c)	84
3.5.4	Duties of Bell Operating Companies, § 271	87
3.6	Challenges to the Constitutionality of Section 271 Requirements	92
3.6.1	Bill of Attainder	93
3.6.2	Separation of Powers	94
3.6.3	Equal Protection Clause	94
3.6.4	Bell Operating Companies' Right to Free Speech	95
	Conclusion	95
	Endnotes	96

Chapter 4

Outstanding Issues from the Telecommunications Act of 1996 99

4.1	Local Number Portability	99
4.1.1	Three Types of Number Portability	101
4.1.2	The North American Numbering Plan	102
4.1.3	Pre-1996 Number Portability in the United States	103
4.1.4	Interim Methods	103
4.1.5	Long-Term Database-Dip Methods	105
4.1.6	Number Portability Regulation	106
4.1.7	Ongoing Issues	106
4.2	Universal Service	108
4.2.1	The Early Concept	108
4.2.2	Universal Service in the 1996 Act	108
4.3	Access	112
4.3.1	FCC's 1983 Access Charge Rules	113
4.3.2	Initial Challenge to FCC's Exemption of ISPs—ACTA's Internet Phone Petition to Designate ISPs as Long-Distance Providers	115
4.3.3	Impact of the Telecommunications Act of 1996	116
4.4	Reciprocal Compensation—Payment for Transport and Termination of Communications	117

- 4.4.1 *Initial Reaction of Incumbent Local Exchange Carriers and Competitive Local Exchange Carriers to Reciprocal Compensation* 119
- 4.4.2 *Incumbent Local Exchange Carriers' Reaction to Competitive Local Exchange Carriers' ISP-Minutes-Terminated Strategy* 121
- 4.4.3 *State Regulatory Concerns Regarding Competitive Local Exchange Carriers' ISP Strategy* 130
- 4.4.4 *Challenges to FCC's Authority and Rules Implementing the Telecommunications Act of 1996* 134
- 4.4.5 *February 1999—FCC's Declaratory Ruling* 136

Conclusion 144

Endnotes 145

PART II EMBRACING THE EXPANDED GLOBAL TELECOMMUNICATIONS MARKET

Chapter 5

The World Trade Organization and Its Telecommunications-Related Agreements 151

- 5.1 *Historical International Trade—Goods, Not Services* 152
 - 5.1.1 *International Trade Law* 153
 - 5.1.2 *U.S. Trade Policy* 153
- 5.2 *1948—The General Agreement on Tariffs and Trade* 155
 - 5.2.1 *Structure and Operation of GATT* 155
 - 5.2.2 *1970s and 1980s—Movement to Include Trade in Services in GATT* 157
 - 5.2.3 *September 20, 1986—Opening of the GATT's Uruguay Round* 158
 - 5.2.4 *GATT Principles* 159
 - 5.2.5 *Drafts of the Services Framework* 162
- 5.3 *December 1992—North American Free Trade Agreement NAFTA* 165
 - 5.3.1 *Telecommunications Equipment and Service* 165
 - 5.3.2 *Licensing* 166

- 5.3.3 *Technical Standards* 166
- 5.3.4 *Basic versus Enhanced Telecommunications Services* 166
- 5.3.5 *Antitrust Issue* 167
- 5.3.6 *Intellectual Property Issues* 167
- 5.3.7 *Dispute Resolution* 167

- 5.4 *March 1994—The Global Information Infrastructure (GII) Concept is Introduced* 168
 - 5.5 *April 15, 1994—Uruguay Round Concluded, WTO Created in Marrakesh, Morocco* 168
 - 5.5.1 *Volume 1—The Legal Texts* 169
 - 5.5.2 *WTO Established and Absorbed GATT* 171
 - 5.5.3 *Annex 1A—1994 GATT* 175
 - 5.5.4 *Annex 1B—1994 GATS* 175
 - 5.5.5 *Annex on Article II (Most-Favored Nations) Exceptions* 184
 - 5.5.6 *April 1995—Annex on Telecommunications* 184
 - 5.5.7 *Annex on Negotiations on Basic Telecommunications (NBT)* 185
 - 5.6 *April 24, 1996—Initial Results of the Negotiations on Basic Telecommunications* 188
 - 5.6.1 *Negotiating Group on Basic Communications' Reference Paper to the Council for Trade in Services* 188
 - 5.6.2 *Market Access Offers—Country Commitments to Include Basic Telecommunications* 189
 - 5.6.3 *Agreement to Set Second Deadline for Continued Negotiations on Basic Telecommunications* 190
 - 5.7 *December 1996—Singapore Ministerial Conference* 190
 - 5.8 *February 15, 1997—WTO Agreement on Basic Telecommunications* 191
 - 5.9 *April 15, 1997—Fourth Protocol to GATS Adopted* 191
 - 5.9.1 *November 1997* 192
- Conclusion 192
- Endnotes 193

Chapter 6

Participating in Global Telecommunications Trade: U.S. Import and Export Laws 197

- 6.1 U.S. Trade Laws 199
 - 6.1.1 Chapter 4—Tariff Act of 1930 200
 - 6.1.2 Chapter 12—Trade Act of 1974 201
 - 6.1.3 Chapter 13—Trade Agreements Act of 1979 201
 - 6.1.4 Chapter 17—Negotiation and Implementation of Trade Agreements (*The Omnibus Trade and Competitiveness Act of 1988*) 202
 - 6.1.5 Chapter 19—Telecommunications Trade Act of 1988 203
 - 6.1.6 Chapter 21—North American Free Trade Agreement Implementation Act of 1993 203
 - 6.1.7 Chapter 22—Uruguay Round Trade Agreements 203
- 6.2 U.S. Export Laws 204
 - 6.2.1 Export Administration Act of 1979 (EAA) 204
 - 6.2.2 Arms Export Control Act (AECA) 204
- 6.3 Implementing Agencies 205
 - 6.3.1 U.S. Trade Representative 206
 - 6.3.2 International Trade Commission (ITC) 206
 - 6.3.3 Coordinating Committee for Multilateral Export Control (COCOM) 206
 - 6.3.4 The Defense Technology Security Administration and the Office of Defense Trade Control 207
 - 6.3.5 Department of Commerce 207
- 6.4 What Is Exported? 209
 - 6.4.1 Department of Commerce's Commodity Control List (CCL) 209
 - 6.4.2 COCOM's International Industrial and Munitions Lists 210
 - 6.4.3 Department of Defense's Munitions List 210
 - 6.4.4 Classification of Re-exports 210
 - 6.4.5 Licensing Requirements 211
- 6.5 To Whom Is the Product Exported? 213
 - 6.5.1 Trading with the Enemy Act (TWEA) and the International Emergency Economic Powers Act (IEEPA) 213
 - 6.5.2 Country Lists 214
 - 6.5.3 Table of Denial Orders 214

- 6.5.4 Specially Designated Nationals List 215
- 6.6 How Are Exports Conducted? 215
 - 6.6.1 Anti-Boycott Amendments 215
 - 6.6.2 Ribicoff Amendments to the Tax Reform Act 217
 - 6.6.3 Foreign Corrupt Practices Act (FCPA) 218
- 6.7 Record Retention Requirements 220
- 6.8 Penalties for Violations of Export Laws 221
 - 6.8.1 Criminal Penalties 221
 - 6.8.2 Civil Penalties 222
- 6.9 Drafting International Trade Contracts 223
 - 6.9.1 Government Regulations and Licensing Requirements 223
 - 6.9.2 Use of Incoterms 223
 - 6.9.3 Choice of Law and Jurisdiction—*The United Nations Convention on Contracts for the International Sales of Goods (CISG)* 223
 - 6.9.4 Payment 224
 - 6.9.5 Currency To Be Used 225
 - 6.9.6 Warranties 225
 - 6.9.7 Unforeseeable Force majeure Events 226
 - 6.9.8 Dispute Resolution 226
- 6.10 Establishing an Export Compliance Program 226

Conclusion 228

Endnotes 228

Chapter 7

Licensing to Protect Telecommunications Intellectual Property 233

- 7.1 U.S. Patent Law 235
- 7.2 U.S. Trademark Law 236
- 7.3 U.S. Trade Secret Law 236
- 7.4 U.S. Copyright Law 238
 - 7.4.1 Exceptions to the Rights of Copyright Owners 240
 - 7.4.2 Remedies for Infringement 243
- 7.5 The Legality of Reverse Engineering and Restrictive License Clauses 244
 - 7.5.1 "Only Means" of Access 244

7.5.2 Restrictive Clauses	244
7.5.3 Noncompete Clauses	245
7.5.4 Overreaching Clauses	245
7.5.5 Appropriate License Clauses	246
7.6 The European Software Directive	247
7.6.1 Similarities of European Software Copyright Law to U.S. Copyright Law	247
7.6.2 Differences Between European Software Copyright Law and U.S. Copyright Law	248
7.6.3 Importance of the Similarities and Differences between European Software Law and U.S. Law to Software Developers	249
7.7 “Must Include” Concepts for Software Licenses	250
7.8 Model License	252
Conclusion	254
Endnotes	254

PART III

LEGAL ISSUES WITH ADVANCED TECHNOLOGIES

Chapter 8

Privacy 259

8.1 Introduction	260
8.2 The Evolution of a Legal Right to Privacy	261
8.2.1 Privacy in the U.S. Constitution	262
8.2.2 Invasion of Privacy—Tort Law	262
8.2.3 Supreme Court Interpretations of Constitutional Amendments Recognizing a Right of Privacy	264
8.2.4 Balance of Personal Privacy with Other Considerations	266
8.2.5 Supreme Court Interpretation of Fourth Amendment Regarding Wiretapping	267
8.3 Federal Privacy Laws Protecting Communications in Transit and in Storage	269
8.3.1 Omnibus Crime Control and Safe Streets Act of 1968, Including the Wiretap Act of 1968	270

8.3.2 Electronic Communications Privacy Act (ECPA) of 1986	270
8.3.3 Communications Assistance for Law Enforcement Act of 1994—The Digital Telephony Act	274
8.4 Federal Privacy Laws Protecting Personal Information in Government Databases	275
8.4.1 Federal Records Act of 1950	275
8.4.2 The Privacy Act of 1974	277
8.4.3 The Computer Matching and Privacy Protection Act	277
8.4.4 Freedom of Information Act (FOIA) of 1976	279
8.5 Federal Privacy Laws Protecting Personal Bank and Financial Information	281
8.5.1 Bank Records and Foreign Transactions Act (BRAFTA) of 1970	282
8.5.2 Right to Financial Privacy Act (RFPA) of 1988	284
8.6 Federal Privacy Laws Protecting Private Databases from Searches and Seizures by Government Officials	285
8.6.1 Privacy Protection Act (PPA) of 1980	285
8.6.2 Court Cases Reviewing the Privacy Protection Act	285
8.7 Federal Privacy Laws Prohibiting Illegal Access to Protected Computers	286
8.7.1 Computer Fraud and Abuse Act of 1988	287
8.7.2 National Information Infrastructure Protection Act (NIIPA) of 1996	289
8.8 Federal Privacy Laws Prohibiting Unwanted and Harassing Communications	290
8.8.1 The Telephone Harassment Act of 1968	290
8.8.2 The Telephone Consumer Protection Act (TCPA) of 1991	291
8.9 Federal Privacy Laws Protecting Information about Children	294
8.9.1 Children’s Online Privacy Protection Act (COPPA) of 1998	294
8.9.2 Child Online Protection Act (COPA) of 1998	295
8.9.3 Child Pornography Prevention Act (CPPA) of 1996	296
8.9.4 Protection of Children from Sexual Predators Act (PCSPA) of 1998	296

8.9.5	<i>Children's Internet Protection Act (CIPA) of 1999</i>	296	9.2.1	<i>1930s–1950s: Encryption</i>	335
8.10	<i>State Privacy Laws</i>	297	9.2.2	<i>1960s–1970s: Computers, Digitization, Multiplexing, Packetization and Encryption</i>	337
8.11	<i>Collection, Use, and Dissemination of Personal Information without Permission</i>	297	9.3	<i>Private-Key Cryptosystems</i>	339
8.11.1	<i>Cookies</i>	298	9.3.1	<i>1970 (1977): U.S. Data Encryption Standard (DES)</i>	340
8.11.2	<i>Social Security Numbers—Identity Theft</i>	300	9.3.2	<i>1995 (1999): Triple DES (3DES)</i>	341
8.11.3	<i>Intellectual Property Theft</i>	303	9.3.3	<i>1997 (2001): Advanced Encryption System (AES)</i>	342
8.11.4	<i>Monitoring by Browsers and ISPs</i>	303	9.4	<i>Public-Key: Cryptosystems</i>	342
8.11.5	<i>Purchased Information and Merged Databases</i>	303	9.4.1	<i>Mathematical Link Between Key Pairs</i>	343
8.12	<i>Solutions to Collection and Use of Information without Permission</i>	304	9.4.2	<i>Digital Signatures</i>	347
8.12.1	<i>Proposed Legislation</i>	305	9.4.3	<i>Key Servers</i>	349
8.12.2	<i>Tort Action</i>	306	9.4.4	<i>Session Keys</i>	349
8.12.3	<i>Customer Caution</i>	306	9.4.5	<i>Well-Known Public-Key Cryptosystems</i>	351
8.12.4	<i>Industry Self-Regulation</i>	306	9.5	<i>Comparison of Private-Key and Public-Key Encryption Technologies</i>	352
8.12.5	<i>Software to Detect and Delete Cookies and Spam</i>	309	9.6	<i>Law Enforcement and National Security Concerns with Public Use of Encryption</i>	353
8.12.6	<i>The Individual's Ability to Correct Inaccurate Information</i>	310	9.6.1	<i>U.S. Laws Restricting the Export of Encryption Systems</i>	353
8.12.7	<i>Web Sites Offering Information on Privacy Protection</i>	311	9.6.2	<i>U.S. Laws Restricting Private, Nonmilitary Use of Encryption Systems within the United States</i>	356
8.13	<i>Application of Privacy Law to Modern Technologies and Services</i>	312	9.6.3	<i>Escrowed Encryption Standard (ESS) and the Clipper and Capstone Chips</i>	359
8.13.1	<i>Email and Voicemail Systems</i>	313	9.6.4	<i>Opposition to the EES, Clipper Chip and Encryption Export Restrictions</i>	360
8.13.2	<i>Cordless/Wireless Phones</i>	317	9.6.5	<i>Efforts to Relax Export Restrictions</i>	366
8.13.3	<i>Pagers</i>	318	9.7	<i>International Encryption Policies</i>	367
8.14	<i>International Privacy Concerns</i>	318	9.7.1	<i>The Organization for Economic Cooperation and Development (OECD)</i>	367
8.14.1	<i>European Community's Privacy Directive</i>	319	9.7.2	<i>1996–1998: Wassenaar Arrangement</i>	369
8.14.2	<i>Other Nations</i>	320	9.7.3	<i>United Kingdom</i>	372
Conclusion		320	9.7.4	<i>1997—European Commission Policy Paper on Encryption</i>	373
Endnotes		321	9.7.5	<i>United Nations Commission on International Trade Law (UNCITRAL)</i>	374
Chapter 9			9.8	<i>U.S. Reaction to International Views of Encryption</i>	375
Encryption		327	9.8.1	<i>1996—Proposed Encrypted Communications Privacy Act of 1996 (S. 1587)</i>	375
9.1	<i>Encryption Technology</i>	330	9.8.2	<i>1996—Promotion of Commerce On-Line in the Digital Era (PRO-CODE) Act S. 1726</i>	376
9.1.1	<i>Forms of Encryption</i>	331	9.8.3	<i>1996—National Research Council Report</i>	376
9.1.2	<i>Key Structure</i>	333			
9.2	<i>Early Use of Encryption in the United States</i>	334			

- 9.8.4 1997—*Proposed Security and Freedom through Encryption (SAFE) Act (HR 695)* 376
- 9.8.5 1997—*Secure Public Networks Act (S. 909)* 377
- 9.8.6 1997—*Amended SAFE Act* 377
- 9.9 Court Cases Reviewing the U.S. Encryption Export Restrictions 378
 - 9.9.1 *Bernstein Cases* 378
 - 9.9.2 *Karn Decisions* 381
 - 9.9.3 *Junger Decisions* 382
- 9.10 Changes in 2000 383
- 9.11 State Laws Concerning Encryption, Key Escrow, and Digital Signatures 384
- Conclusion 384
- Endnotes 385

Chapter 10

Cyberlaw: Evolving Legal Issues with the Internet 389

- 10.1 Commerce on the Internet 390
 - 10.1.1 *Uniform Commercial Code (U.C.C.)* 390
 - 10.1.2 *End-User Contracts* 393
 - 10.1.3 *International E-Commerce Efforts* 395
- 10.2 Jurisdiction 396
 - 10.2.1 *Jurisdiction in E-Commerce* 398
 - 10.2.2 *Personal Jurisdiction in the Internet Age* 398
 - 10.2.3 *International Jurisdiction* 399
- 10.3 Taxation 400
 - 10.3.1 1967—*National Bella Hess, Inc. v. Dept. of Revenue* 401
 - 10.3.2 1987—*Proposed Modem Tax* 401
 - 10.3.3 1992—*Quill Corp. v. Heitkamp* 402
 - 10.3.4 1996 to 1997—*International Tax Discussions* 403
 - 10.3.5 1997—*Proposed Internet Tax Freedom Act (ITFA)* 404
 - 10.3.6 1998—*California Internet Tax Freedom Act* 404
 - 10.3.7 1998—*Federal Internet Tax Freedom Act* 406
 - 10.3.8 *National Tax Association Communications and Electronic Commerce Tax Project* 407

- 10.4 Trademark/Domain Names 407
 - 10.4.1 *Trademark Infringement Issues in the Internet Age* 408
 - 10.4.2 *Actions by Companies to Protect Their Trademarks* 409
- 10.5 Copyright 413
 - 10.5.1 *Copyright Act of 1976* 413
 - 10.5.2 *National Commission on New Technological Uses of Copyright Works (CONTU)* 413
 - 10.5.3 1998—*Digital Millennium Copyright Act (DMCA)* 414
 - 10.5.4 *Exclusive Rights* 415
 - 10.5.5 *Impact of Fair Use on Copyright Contracts* 416
- 10.6 Trade Secrets 417
- 10.7 Defamation on the Internet 418
 - 10.7.1 *Morrison & Forester v. Wick, 94 F. Supp.2d 1125 (D. Colo. 2000)* 418
 - 10.7.2 *Lucent Technologies v. Johnson, Civ. No. 00-05668 (C. D. Cal. Sept. 12, 2000)* 419
 - 10.7.3 *Lucent Technologies v. lucentucks.com, 54 U.S.P. Q2d 1653 (E. D. Va. 2000)* 419
- 10.8 Liability of ISPs and Computer System Operators 419
 - 10.8.1 *Publishers* 420
 - 10.8.2 *Distributors* 420
 - 10.8.3 *Common Carriers* 420
 - 10.8.4 *Claims on Web Sites* 421
 - 10.8.5 *Digital Millenium Copyright Act* 421
- 10.9 Obscenity and Violence on the Internet 421
 - 10.9.1 1996—*The Communications Decency Act (CDA)* 422
 - 10.9.2 *Reno v. American Civil Liberties Union (Reno II)* 422
 - 10.9.3 *Child Online Protection Act (COPA)* 423
 - 10.9.4 *American Civil Liberties Union v. Reno (Reno III)* 423
 - 10.9.5 *Child Online Privacy Protection Act (COPPA)* 423
 - 10.9.6 *State Laws* 424
- 10.10 Fraud on the Internet 424
- Conclusion 426
- Endnotes 426

Appendix A	Key Documents and Decisions Concerning Local Number Portability	429	Appendix F	Commitments and Most Favored Nation Exemptions	451
Appendix B	Key Documents and Decisions Concerning Universal Service	431	Appendix G	Chapters within Title 19 of the U. S. Code Customs Duties	463
Appendix C	Key Documents and Decisions Concerning Access and Reciprocal Compensation	433	Appendix H	State Privacy Laws	465
Appendix D	Legal Instruments Embodying the Results of the Uruguay Round	443	Appendix I	Resources to Detect and Delete Cookies	479
Appendix E	Membership of the World Trade Organization	447	Appendix J	State Laws Concerning Encryption, Key Escrow, and Digital Signatures	483
			Index		503

Encryption technologies are the most important technological breakthrough in the last one thousand years. No other technological discovery—from nuclear weapons (I hope) to the Internet—will have a more significant impact on social and political life. Cryptography will change everything.

Lawrence Lessig, Harvard law professor and author of *Code: and Other Laws of Cyberspace*¹

WITH THE INCREASED COLLECTION, USE, SALE, AND EXCHANGE OF private information about individuals, usually without the individual's knowledge or permission, it is clear that technology has introduced privacy concerns that the framers of the U.S. Constitution never dreamed about. As discussed in Chapter 8, current law has not totally addressed these concerns, and very few legal restrictions exist to control them.

Technology, however, also provides a solution to many of these privacy concerns. *Encryption* is the process of writing a message in code or other secret form so that only persons with the *key* can decode or “decrypt” the message to read it. Readily available through low-cost or free computer programs, encryption prevents eavesdroppers or interceptors of a communication, including the government, from reading that communication. This allows nearly anyone to protect email, e-commerce transactions, online banking, contracts, data files, and other electronically transmitted communications or messages stored in unsecured computer databases. Furthermore, modern encryption programs allow users to control their own encryption rather than having to go through a central government agency or clearinghouse. This provides an extra level of privacy that legislation cannot offer.

As use of the Internet increases, people will demand this greater security for their communications, credit card information, and e-commerce transactions.

They will also resist having their “net-surfing” and purchasing habits recorded. Corporations will demand increased privacy for their communications to their branch offices, customers, and suppliers worldwide. Thus, modern forms of communications such as the Internet are driving the need for greater privacy. Since encryption provides a technical solution to privacy concerns, it will profoundly affect every person and corporation existing today and in the future. For this reason, Lawrence Lessig, a Harvard law professor and international authority on cyberlaw, stated in his recent book *Code: and Other Laws of Cyberspace* that encryption technologies are the most important technological breakthrough in the last 1,000 years . . . and will change everything.

However, several critical issues surround the topic of encryption in the United States today. First, while nearly everyone, including the U.S. government, acknowledges the increasing need for individual and corporate privacy in the 21st century, law enforcement and national security agencies, such as the Federal Bureau of Investigation (FBI), Central Intelligence Agency (CIA), and the National Security Administration (NSA), argue that they must be able to intercept and decode encrypted messages in order to fight terrorism, drug trafficking, organized crime, and child pornography. This requires that the government assess the true crime fighting needs of law enforcement and national security agencies and find a balance between those needs and the privacy needs of individuals.

Second, while the U.S. government may be willing to permit the use of encryption in the United States, historically it has severely restricted the export of certain encryption products and technologies, believing that such export threatens our national security. However, strong encryption software programs are readily available worldwide for free or as little as \$5.00. Therefore, many persons in the United States strongly oppose the government’s restrictions on the export of encryption. They point out that the export restrictions do nothing to protect the national security of the United States but, instead, harm the competitiveness of U.S. companies to sell software or to provide the seamless privacy protections required in modern communications and e-commerce transactions. Opponents also state that the restrictions are unconstitutional constraints on the right of free speech and are inconsistent with the approach used by other democratic governments and international organizations with equal national security concerns. Finally, opponents argue that the U.S. government’s definition of “export” is overly broad. The definition includes sending an encrypted email to a relative, friend, colleague, or customer abroad. Even internal memos to corporate branch offices abroad are considered “export.” It can also include clicking into Web sites located outside of the United States if people use encryption in their Web systems. Basically, any encrypted transaction involving a party outside the United States, is considered an “export.”

In seeking a solution to this conflict, the U.S. government has proposed several alternative concepts including (1) “key escrow,” both voluntary and

automatic in hardware such as the Chipper Chip, (2) “key recovery,” providing “back door” access to encrypted messages for the government through both hardware and software options; and (3) legislation limiting the strength of the keys used in encryption. *Key escrow*, is a general name for regulations requiring that encryption users register or “escrow” with the government or a designated third party their “keys” to unlock or decode their encrypted messages, so that the government can, with a court-ordered warrant, read any encrypted message. This is intended to provide strong encryption capabilities to U.S. citizens while still allowing the government to be able to decrypt an encrypted message if it deemed necessary to do so. *Key recovery*, on the other hand, is a general name for the hardware or software capability built into an encryption system that allows the government, “with proper judicial authorization in the form of a court order,” to decrypt an encrypted message without the knowledge of the parties to the communication. Key recovery therefore provides “back-door” access for the government to encrypted communications designed into the basic operations of the system by the system developers at their own expense.

However, public opposition to these proposals has delayed their adoption. In addition, several important court cases have held that encrypting a message is *free speech* protected by the U.S. Constitution, and on January 14, 2000, the government issued new, more relaxed encryption export regulations, but did not remove all of them. These new regulations make it somewhat easier for U.S. companies and individuals to export encryption technology in common products to certain countries, but still require companies to file applications, escrow keys, and provide key-recovery capability to the government before they can export products containing or using encryption.

The purpose of this chapter is to describe briefly how encryption works, the main issues surrounding it, and the major laws governing it. To do this, Section 9.1 explains basic encryption technology, including the importance of “keys” and key strength. Section 9.2 outlines the early use of encryption in the United States and some of the initial legislation securing its use for military and law enforcement. Sections 9.3 and 9.4 describe the two most important encryption technologies available to the public today, private-key and public-key systems, respectively. One important aspect of public-key encryption technology discussed is that of “digital signatures,” which are amazingly secure and thus important to e-commerce and “identity theft” issues. For this reason, recent legislation recognized digital signatures as having the same force as handwritten signatures in contracts and other commercial documents. Section 9.5 compares the private-key and public-key technologies, noting the strengths and weaknesses of each. Section 9.6 expands on the concerns of law enforcement and national security agencies regarding public use of encryption systems and the legislation initiated by law enforcement and the security agencies to control that use. It also discusses public and private opposition to these restrictions and government efforts to relax the restrictions. Section 9.7

outlines the views and approaches of other democratic countries and international organizations concerning encryption. Section 9.8 then describes the United States's reaction to these changes and three key court cases whose decisions have impacted recent legislation and caused some U.S. restrictions on encryption use and export to be relaxed. Since this is such a rapidly changing area of technology, Section 9.9 also provides a list of the current state, federal, and international laws that exist in this area, new laws that have been proposed, and several Web sites that provide additional information and updates.

9.1

ENCRYPTION TECHNOLOGY

Encryption does not prevent someone from intercepting a message, but rather it prevents that person from reading the intercepted message. In many cases, encryption also blocks information about *to whom* the message is sent or *from where* it came.² Encryption is based on the ancient study of cryptology and the resulting practice of cryptography. Such systems have been in use for over 4,000 years, beginning with the written hieroglyphics of ancient Egypt. Governments since the Greeks and Romans have used encryption to protect important military and diplomatic communications, and today, computer-generated mathematical algorithms make encryption available to individuals for free or at very low cost.

In each case, the text of the original message, known as the “plaintext” or “cleartext,” is encoded or enciphered into “codetext” or “ciphertext,” which usually has the appearance of random, unintelligible characters. This unreadable message is called a “cryptogram.” The process of reading the cryptogram requires decoding or deciphering the encrypted message with a key. If the key is unknown, “cryptanalysis” is the art of breaking the code or cipher to discover the key.

Traditionally, the term *code* described any system in which the basic unit of concealment was a word, while the term *cipher* described any system in which the basic unit of concealment was a single letter within a word. However, in Morse Code, letters are the basic unit, which in turn encodes words.

Most individuals have had some experience with cryptography in puzzles or games. Many children have used decoder rings found in boxes of cereal to write notes to their friends. However, before computers, most secure encryption systems were too expensive and complicated to be used by individuals or corporations. Only governments could afford the cost and then only for diplomatic and military, not financial or administrative communications. As computers have evolved, however, this has changed, and strong encryption systems are now readily available for private, nongovernmental use. This is fortunate since the need for highly secure private messages has also increased significantly with the proliferation of computers and the Internet.

9.1.1.1 Forms of Encryption

In the thousands of encryption systems that have existed over the years, all use some form of “substitution,” “transposition,” “concealment,” “device,” or “mathematical” techniques to change the original message.

Substitution

Substitution encryption systems replace the letters of the alphabet with combinations of symbols or signals to encode the message. Two familiar examples of substitution encryption systems are the Morse code, in which dots and dashes substitute for the letters of each word, and the five-row–five-column code used by U.S. prisoners of war (POWs) during the Vietnam War.

In the Vietnam POW system, the English alphabet was grouped into five rows, each containing five columns. Row 1 contained *A, B, C, D,* and *E*; row 2 contained *F, G, H, I,* and *J*; row 3 skipped *K* (represented by *C* to reduce the alphabet to 25 letters), and contained *L, M, N, O, P*. Rows 4 (*Q, R, S, T,* and *U*) and 5 (*V, W, X, Y,* and *Z*) completed the alphabet in sequential fashion. To tap out a message, the prisoners would tap first the row, then the column. For example, *C* would be one tap, followed by three quick taps representing Row 1, third column or position. Similarly, *R* would be four taps, followed by two taps, representing fourth row, second column.

Like the Morse code and the Vietnam POW system, all substitution systems are understandable or interpretable only by those who know the code or have access to a codebook. Other systems may require a decoding device or symbol manipulator.

Transposition

Transposition encryption systems rearrange the position of the letters or elements in the text of the message. For example, each letter of the original message may be replaced by a letter one or more positions to the left or right. Thus, if shifted one letter to the left, the name *IBM* becomes *HAL*. Some students of the movie *2001: A Space Odyssey* suggest that this was the source of the computer’s name in the movie.

Julius Caesar used a simple code in which each letter of the text was replaced by the letter three positions to the right. Thus *CAB* became *FDE*. This system was called the “Caesarian Cipher,” named after the Roman general Cipher (100–44 BC) who is credited with inventing it.³ Other transposition encryption systems also divide the letters into groups and then reverse the letters in each group. If needed, the system then uses extra, or filler letters called “nulls” to complete block groups. For example, if a five-letter group system were used, the message “HELLO THERE” would be *OLLEH EREHT* or more hidden, *OLLEHEREHT*.

Concealment

In 1600, Cardinal Richelieu invented the *grille* or a card with holes in it. He would place the card on a sheet of paper, write his message in the holes and then fill in the rest of the paper to appear as an innocent message. Many other concealment systems exist, including patterns of letters created on a page.

Device

The Spartans, centuries ago, used a *device* encryption system in which communicators would wrap a belt around a stick, write the message along the length of the stick, and then unwind the belt. To read the message, the same size stick was needed to wrap the belt around.

In the United States, Thomas Jefferson invented an early cryptographic device known as the “wheel cipher” around 1795. The wheel cipher contained a stack of wheels loaded onto a central rod or axle. On each wheel, Jefferson wrote the letters of the alphabet in random order. To encode a message, he would shuffle the wheels and then place them on the axle, in random order. The letters of the message would then be aligned along the rotational axis of the axle, one letter per wheel. Any other row of aligned letters could then be used as the ciphertext for transmission. To avoid the very small probability that two readable messages could be spelled by the order of the wheels, the sender would review all combinations on the wheels.

To decrypt the message, the recipient aligned the letters of the ciphertext along the rotational axis and looked for a set of aligned letters that spelled words. Without knowing the order of symbols on the wheels or the order of wheels on the axle, any plaintext of the appropriate length is possible, and thus the system is quite secure for one-time use. Statistical decryption is feasible if the same wheels are used in the same order many times. Thus, the strength of the system is in the random order of the wheels when they are placed on the axle.

Although Jefferson rarely used his device himself, the U.S. Navy used a similar item for nearly 200 years, until the mid-1990s. Today, device systems generally include computerized discs, spun in opposite directions.

Mathematical Algorithms or Source Codes

Modern encryption systems use computers to arrange strings of zeros and ones, also called “bits,” into groups or blocks to create keys. Each key has a preset number of bits. The arrangement of the bits in each key is based on mathematical patterns provided by the encryption algorithm or source code. These algorithms then use the keys to encrypt and decrypt messages.

In their book *Privacy on the Line*, encryption experts Whitfield Diffie and Susan Landau provide an excellent description of the manner in which algorithms use keys to encrypt and decrypt messages. The example they use is this:

If two people were trying to meet on a specific day, time, and location, the information needed to be sent from one to the other would include the year, month, day, hour, minute, avenue, and street in that pre-agreed upon order. Thus, if the meeting were to take place at 3:25 PM on December 30, 1999, on the corner of 1st Avenue and 44th Street, and a two-digit system were agreed upon to represent each piece of information, the resulting message would be:

19 99 12 30 15 25 01 44

Every digit in this message is significant. To encrypt it for secrecy, both persons must also agree on a key that will convert the string of 14 digits into some other string of 14 digits that is understandable by both persons, but not by anyone else. For example, if the key agreed upon by the two people is

64 25 83 09 76 23 55 72

when it is added to the original message, the resulting encrypted message is:

73 14 95 39 81 48 56 16

The above “cryptogram” is what is transmitted to the receiver in whatever manner is possible, including very public, nonsecure methods such as over the telephone, on a postcard, or over the radio. Diffie and Landau point out that, in some cases, the addition produced a number greater than 10. In the third place, for example, the sum is 11. In such cases, the 1 in the 10s place is thrown away, rather than “carried” into the next place as in ordinary arithmetic.

To decrypt the message when received, the intended recipient simply subtracts the agreed-upon key, without “borrowing,” to learn the actual message. Since the key was chosen at random, even if the message were intercepted in route, the interceptor could see that a series of numbers or information had been transmitted, but could not determine the key or whether the actual information was numbers or letters. Therefore, the interceptor could not decrypt the message. If the key were used a second time, however, the interceptor could use information about the first message, to determine the key. Thus it is important to use a different key each time a critical message is transmitted.

This mathematical algorithm type of encryption system is readily generated by computers and yet works well for transmitting important information, such as a credit card number, even in the midst of other less-critical information, such as the items purchased on the Internet. The remaining issue is, however: How does the intended recipient learn the key? The next several sections explain this, but *public-key* and *private-key encryption systems* complete the process in very different ways.

9.1.2 Key Structure

As noted, if the receiver has the correct key, he or she can “decrypt” any message encrypted with that key. If the receiver does not have the correct key,

however, that person has three options: (1) steal the key, (2) analyze the code to determine the algorithm used to create the key, or (3) use a “brute-force attack” in which all possible keys are tried, one at a time, until the correct key is found. In either of the two last options, the more bits a key contains, the more secure it is considered to be. This is because with Option 2, longer keys require more time and effort to analyze, while with Option 3, keys require more time to break the code using a brute-force attack. Thus, the strength of an encryption scheme increases with its “key length.”⁴

For example, if a key contains only two bits, four possible key combinations exist: 00, 01, 10, and 11. If a third bit is added to the key, eight possible key combinations result: 000, 001, 010, 100, 011, 101, 110 and 111. Thus, key combinations grow exponentially as each bit is added. For this reason, the following increase in possible key combinations results as increasingly more bits are added to the key.

Key Length	Possible Number of Key Combinations
2-bit key	4
3-bit key	8
8-bit key	256
56-bit key	72 quadrillion
128-bit key	4.7 billion trillion ⁵

In the same fashion, the time required to break the code with a brute-force attack, or by trying all key combinations until the correct one is found, also increases exponentially. Usually, the process requires a network of computers and an average of trying about 50% of the possible keys. It is also impacted by changes in technology. For example, in 1986, it was estimated that a fast computer would take 2,283 years to try all possible keys in a 56-bit key, the then-adopted IBM standard called the U.S. Data Encryption Standard (DES). However, advances in computer power and speed have decreased the time required to find a key using a brute-force attack to under five hours.⁶

9.2

EARLY USE OF ENCRYPTION IN THE UNITED STATES

Encryption systems in the United States historically have been the domain of government and military systems. Systems such as Thomas Jefferson’s wheel system, shift systems, and the Morse code served the government well, so long as the keys were changed frequently and the key or code was not intercepted while being communicated to the intended recipient of the message.

This concern became a special problem with radio. During the early 1900s, radio became an increasingly popular broadcast medium but was not secure. Thus, during World War I, communicating sensitive information by radio required encryption. The United States realized the need for broad-based en-

encryption systems, but in a precomputer era, such systems tended to be slow and costly. Their security also depended on unusual keys with complex key handoffs, usually coordinated by a centralized authority.

9.2.1 1930s–1950s: Encryption

Encryption remained the domain of military and diplomatic use through the Depression in the 1930s, World War II in the 1940s, and the Cold War in the 1950s. Its focus was national security, followed by law enforcement and protection of technological advances such as nuclear power and airline traffic safety. During World War II, the function of intelligence, including communications intelligence, was placed under military command.⁷ However, this caused its development and oversight to be quite disjointed and uncoordinated.

Central Intelligence Act of 1947

To correct this, Congress passed the Central Intelligence Act of 1947, creating the Central Intelligence Agency (CIA). The new position of *Director of Central Intelligence* was tasked with coordinating the efforts of the entire U.S. intelligence community.

Wiretapping

As discussed in Chapter 8, Section 8.2.5, wiretapping was a common practice for law enforcement who monitored some domestic and all international calls from 1876–1967. It did not require a court order until two cases, *Katz v. U.S.*⁸ and *Berger v. New York*,⁹ were decided in 1967. Even then, however, a court order was not required when issues of national security or wiretaps of a foreign government were involved.

Shannon's "Communications Theory of Secrecy"

In 1948, Claude Shannon, an electrical engineering professor at MIT, published an article in the *Bell System Technical Journal* entitled "The Communications Theory of Secrecy Systems."¹⁰ Shannon was one of the first modern cryptographers to apply advanced mathematical techniques to the study of cryptography. Although the use of frequency analysis for solving substitution encryption began many years earlier, Shannon's work demonstrated several important features about the statistical nature of language that made the solution to nearly all previous codes very straightforward. Perhaps the most important result of Shannon's famous paper is the development of a measure of cryptographic strength called the *unicity distance*.

The *unicity distance* is a number that indicates the amount or quantity of an encrypted message that is required in order to decrypt that message. It is a

function of the length of the key used to encrypt the message and the statistical nature of the language in which the original message was written. Given enough time, it is guaranteed that any encrypted message can be broken if the unicity distance is 1. For example, any time the length of all messages sent under a particular key in English exceeds 2.6 times the length of that key, the key and the original messages eventually can be determined. Encryption systems with an infinite length random key have a unicity distance that is infinite. While unbreakable, they are also impractical. However, Shannon found that a message created with an alphabetic substitution encryption system (1) with a random key, (2) with a length greater than or equal to the length of the message, and (3) used only one-time, cannot be decrypted from the ciphertext alone.

Shannon also introduced the concept of “workload,” which is the difficulty in decrypting a message given the availability of enough ciphertext to theoretically break a code. He showed that an alternative to increasing the unicity distance is the use of systems that increase the workload required to decrypt the message. Two important concepts provided by Shannon in his paper are the *diffusion* and *confusion* properties of encryption. These form the basis for many modern cryptosystems because they tend to increase the workload of cryptanalysis.

Diffusion is the dissipation of the statistical structure behind the language being transmitted. For example, making a different symbol for each English word makes statistical occurrence for many words difficult to detect in the short run, and increases the quantity of data needed to decrypt messages. This difficulty occurs because meaningful words are rarely repeated, and common words such as “the,” “and,” “or,” are frequently repeated. The random use of obscure synonyms for frequently repeated words tends to dissipate the ability to decipher them. Strange sentence structures have a similar effect on the cryptanalysis process.

Confusion is the obscuring of the relationship between the original message, the key, and the encrypted message. For example, if any bit of the key has a 50% chance of affecting any bit in the encrypted message, statistical attacks on the key require solving a large number of simultaneous equations.

Extensions to Shannon’s basic theories include the derivation of an “index of coincidence” that allows approximations of key length to be determined purely from statistical data,¹¹ the development of semiautomated techniques for attacking cryptosystems, and the concept of using computational complexity for assessing the quality of cryptosystems.¹²

National Security Agency

In 1952, responding to increasing Cold War concerns, President Truman created the National Security Agency (NSA). The unexpected result was that the National Security Agency took over all work in cryptography in the United States, successfully suppressing it in other agencies of government. As a re-

sult, the use of encryption in the other agencies froze or diminished, even for nuclear command and air traffic control systems. This did not change for over a decade, until ordered to change by President Kennedy in the 1960s.

Abuses of Power

During this era, the government's control of encryption was meant to benefit all Americans through increased national security. However, the control also led to serious abuses. For example, although census information was publicized as confidential, during World War II it, and other government-held information, was used to wiretap and locate Japanese-Americans to be sent to internment camps. During the McCarthy era, Civil Rights movement, and Vietnam protests, many illegal wiretaps were placed on numerous citizens' communications, not just on those of political activists. In 1968, court orders were required for wiretaps, but these were easy to obtain, and when they could not readily be obtained, the FBI and others frequently ignored this requirement and wiretapped many law-abiding citizens, political leaders, Supreme Court judges, members of the U.S. Congress, and *all* international calls. As many readers may recall, illegal wiretaps against the Democratic National Committee, ordered by the White House, ignited the Watergate scandal.

9.2.2 1960s–1970s: Computers, Digitization, Multiplexing, Packetization, and Encryption

During this era of frequent wiretapping, individuals and companies made no practical use of encryption, even though analog communications were not very secure. It wasn't until the 1960s and 1970s, with the development of computers, that several important changes occurred in communications technology, including the *digitization of communications, multiplexing, packetization, and affordable encryption*.

Digitization of communications improved the security of communications because, when communications are digitized, the communication is converted to 1s and 0s, divided up into small groups called “bytes,” and then transmitted over whatever circuit or route is best for that transmission. When someone tries to wiretap a digitized conversation, they hear only static.

When *multiplexed* onto shared resources, such as T-1, T-3, and higher circuits, portions of each digitized communication are mixed with digitized portions of hundreds of other communications and transmitted over the same communication line. This makes it even more difficult to wiretap single digitized communication.

By the time technology evolved to *packet* communications, hundreds of thousands of communications were first digitized, divided into “packets” of information, and then multiplexed together before being transmitted over thousands of

circuits. When the packets reached the receiving end, they were placed in their proper sequence and delivered to the listener. Thus, *packetization* further enhanced the security of communications by disassembling messages and permitting their transmission over different paths, further complicating wiretaps.

With computers also came affordable *encryption*, opening possibilities for its use by individuals and companies. Computers drove the cost of encryption technology to a low enough level to be affordable for private, nongovernmental use. Second, people became excited about the revolutionary power and speed that computers brought to encryption, providing the complexity required for truly secure encryption systems. Third, computers eliminated the need for centralized control of encryption, enabling “end-to-end” user control. These three benefits brought about by computers touched off tremendous private research and development of encryption systems and created an explosion in technology that continues today.

1965—Brooks Act

In 1965, recognizing the potential of computers and their increasing importance in commerce, Congress passed the Brooks Act of 1965. Sponsored by Representative Jack Brooks of Texas, the uncontested law assigned responsibility to the U.S. Department of Commerce’s National Bureau of Standards (NBS) to make recommendations to the president concerning standards for both civilian and government computers under a uniform federal automatic data-processing standard (FADPS). Given this new range of responsibilities, Congress also changed the name of the National Bureau of Standards to the National Institute of Standards and Technology (NIST).

1967—International Covenant on Human Rights

However, along with the increasing use and commercial benefits of computers came increased concerns about privacy. In 1967, two years after the Brooks Act, the international community recognized the growing use and impact of computers on human rights and renewed Article 12 of the 1948 Universal Declaration of Human Rights, which stated

*No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.*¹³

1967—Publications on Encryption Ignite Public Interest

Also in 1967, David Kahn, a journalist, published a history of cryptography entitled *The Codebreakers*.¹⁴ Years later, in 1982, James Bamford published a history of the National Security Agency (NSA) entitled *The Puzzle Palace*.¹⁵ Both works ignited tremendous public interest in cryptography, especially

among academics, as a means of providing the needed privacy and increased security required with modern communications.

As part of this new interest in encryption, the academic community developed two main approaches to computerized encryption in the early 1970s: private-key and public-key cryptosystems. They are also known as “symmetric” and “asymmetric” systems respectively, or one-key and two-key systems, not to be confused with one-bit and two-bit key systems. Details of these systems are described in the following two sections of this chapter. The U.S. government, on the other hand, was less excited about this new civilian interest in encryption and threatened the academic community with *prior restraint* in order to prevent the publication of additional information on new encryption concepts and systems.

9.3

PRIVATE-KEY CRYPTOSYSTEMS

Private-key encryption systems are the most familiar encryption systems to people because they include the “James Bond” type of cryptosystems in which both the sender and receiver know the same code so they can exchange secret messages. Other private-key systems include the Navaho “code-talkers” of World War II. The primary risk with private-key systems is when third parties learn the code and thus compromise the secrecy of the messages.

To send a message through a computerized private-key encryption system, the sender (1) writes the message as normal, (2) encrypts it using an encryption system previously agreed upon with the recipient, and (3) sends it to the recipient. To decrypt it, the recipient must have the *same* key or code. For this reason, private-key systems are also known as “single-key” or “symmetric” systems.

To respond, the recipient uses a different, randomly generated key to protect the security of the keys, communicates it to the sender, drafts the response, encrypts it, and sends the encrypted response to the sender. When the sender receives the response, he or she decrypts it with the same key.

This requirement that both the sender and recipient must have the same key leads to several limitations. First, the sender and receiver must either know each other before they can communicate or they must have some method of establishing a secure “key hand-off.” Second, private keys cannot be changed without the recipient’s knowledge. Third, the secrecy of the key must be preserved so that unauthorized eavesdroppers or interceptors cannot learn the key and read the message. Thus, the security of private-key systems is more dependent on the security of the key than on the complexity of the encryption system. These limitations make private-key systems less desirable in the Internet Age since (1) parties, who often do not know one another, communicate, but perhaps only once; (2) many users want to change their

keys frequently; and (3) the Internet is an open medium. Thus, the communicators have little opportunity to agree upon a key and need to have a separate key for each communication.

Nevertheless, the main encryption system in the United States for 21 years, from January 1977 through December 1998, was a computerized private-key system called the U.S. Data Encryption Standard (DES). In January 1999, the DES was replaced by a more complex private-key system known as the Triple DES (3DES), and in 2001, Triple DES is being replaced by an Advanced Encryption System (AES). All three systems are described below.

9.3.1 1970 (1977): U.S. Data Encryption Standard (DES)

In 1970, as computers were becoming increasingly used, an engineering team at IBM, led by Horst Feistel, developed a private-key encryption system that became the U.S. Data Encryption Standard (DES). The DES is a “shift-register” or “block-cipher” system that uses the fact that most modern communications systems divide each 64 bits of digitized information in a message into eight blocks of eight bits each. These blocks are called “bytes” or “octets.” It then scrambles the eight bits in each block using a random selection encryption key or pattern. Third, the DES performs a complex mathematical operation on the first four of the eight blocks and uses the results to alter the remaining four blocks.¹⁶ To avoid a possible situation where a block could contain all zeros, the DES uses only seven of the eight blocks, or 56 bits of each 64 bits of data, for the encryption scheme and thus is called a 56-bit key.

Amazingly, this 56-bit key process results in 70 quadrillion possible key combinations for each message. For this reason, any message encrypted by the DES was considered, for many years, to be secure from a successful brute-force attack. As such, the DES provided a highly reliable encryption system for both businesses and individuals. However, it was still breakable by the government if a security threat warranted the effort required to do so. In 1971, one year after the DES was developed, two Israeli scientists developed a way to break the DES under certain limited situations.¹⁷ However, the scientists did not widely distribute their information.

The security of the DES led the U.S. government, in 1974 to select it as the winner of a request for proposals (RFP) for a U.S. encryption standard issued by the National Bureau of Standards in 1973.¹⁸ Discussion about the request for proposal began in the early 1970s, as various federal agencies increasingly used computers and digital communications. The National Security Agency and the National Bureau of Standards recognized that federal government agencies needed standardized cryptography to safeguard their records. This was further emphasized in 1974 when the Privacy Act of 1974 was enacted. However, the National Security Agency was unwilling to develop the needed encryption system for fear that such activity would reveal too much about its capabilities and encryption philosophies. It believed that wide availability of

the National Security Agency's products could compromise other national security efforts.¹⁹

While selected in 1974, it wasn't until three years later, on January 15, 1977, that the U.S. government adopted the DES as the official Federal Information Processing Standard (FIPS) to protect unclassified computer data in the U.S.²⁰ To ensure that the standard kept pace with technical growth and change, the government required that the National Institute of Standards and Technology (NIST) reaffirm the DES's designation as the official U.S. encryption standard every five years. It was reaffirmed for the last time on December 30, 1993, and remained the standard through December 1998.²¹ In its 21 years as the U.S. standard, from January 1977 through December 1998, DES also became the primary international encryption system used by banks and other commercial groups for electronic funds transfer.

During those 21 years, however, computers also became faster and more powerful, reducing the time required to successfully break a DES code by a brute-force attack. This was widely recognized, to the point that even the movie *Sneakers*, released in 1992 by Universal Studios, depicted the potential impact of a fictional computer capable of breaking any encrypted information in the world.

In January 1995, the National Institute of Standards and Technology announced that the 56-bit DES would no longer be sufficient to protect the security of encrypted messages after its December 1998 end date. Instead, NIST recommended that, effective January 1999, the DES be replaced by Triple DES (3DES) as the U.S. encryption standard. The Triple DES code is three times harder to break than the original DES.

As if to underscore the need for a more powerful system, on June 19, 1997, 14,000 computer users took part in a brute-force attack on the DES code. The group tried 18 quadrillion keys before it broke the code but it required only a few weeks. Exactly one year later, on June 18, 1998, a group of Silicon Valley computer workers, using faster computers, cracked the 56-bit DES code in only 56 hours. Nineteen months later, on January 19, 2000, a group of computer users cut this time in half, requiring only 22 hours and 15 minutes to break the 56-bit DES code.

9.3.2 1995 (1999): Triple DES (3DES)

On January 15, 1999, following the recommendation made four years earlier in 1995 by the National Institute of Standards and Technology, Triple DES replaced DES as the new U.S. encryption standard. Triple DES encodes a message using DES, but does it three times in sequence, each time with a different key. It is, therefore, three times harder to break than the original DES. In the four years between January 1995 and January 1999, the banking industry had already converted to the more secure Triple DES, so it had actually become the de facto standard before it was named the official new standard.

9.3.3 1997 (2001): Advanced Encryption System (AES)

However, the continually increasing speed of computers and users' ability to crack the DES code convinced the NIST that Triple DES would only be a temporary solution and on January 2, 1997, even before Triple DES was in place as the U.S. encryption standard, NIST announced plans for an advanced encryption system (AES). Later that same year, on September 12, 1997, the NIST issued a formal RFP for designs for a more secure encryption algorithm. The RFP stated that the selected proposal must be for a private-key, block-cipher system using a minimum 128-bit key, with upward capability to 192-bit and 256-bit keys. It must also be publicly disclosed, available worldwide, and distributed royalty-free. AES is expected to be completed by the summer of 2001 and to become the new federal standard, replacing Triple DES, after that time.

9.4

PUBLIC-KEY CRYPTOSYSTEMS

Also during the 1970s, while private-key DES was becoming the U.S. encryption standard, a second approach to cryptography, public-key encryption, was developed by three men in California. During the academic year, 1974-75, Whitfield Diffie and Martin Hellman, from Stanford University, and Ralph Merkle, from the University of California at Berkeley, developed a two-key encryption system that they called "public-key cryptography."²² One key is a "public-key," which the owner may print on business cards, use in emails, place in public directories, or advertise on billboards. The second key is a "private-key," known only to the key owner. Hence, public-key systems are also called "two-key" or "asymmetric" encryption systems.

There are two ways to send a public-key encrypted message. Users choose one or the other depending on the type of communication desired. First, if the message is being sent to a specific individual, and the sender wants to ensure that only the intended recipient can read the message, the sender would use method one. For example, a customer sending credit card information over the Internet to a company from whom the customer is purchasing items would use this method. Since the company's address and other information are public, they need not be encrypted. However, numerous customers may wish to send separate, individually encrypted messages to the company. For this reason, method one is commonly called "many-to-one encryption." Senders of some email messages, personal health, insurance, banking information and tax filings would also use method one. The focus is that only the sender's side of the message requires encryption. The recipient's side of the message need not be encrypted.

On the other hand, if the message is potentially sent to numerous public recipients, but the sender wants to ensure that only he or she and no one else would be the recognized sender, the sender would use method two. For example, this would be used by a person wishing to send a digital signature on a contract over the Internet to one or more recipients with whom the sender is

conducting business. Since the sender's address and other information must be encrypted in order to verify for potentially numerous recipients, method two is commonly called "one-to-many encryption." Senders of digital signatures, orders, personal email messages, and order confirmations would use this method. Again, the focus is that the sender's side of the message requires encryption, but the recipient's side of the message need not be encrypted. Both methods one and two require that both parties have encryption technology and are in contrast to the one-to-one aspect of private-key cryptography and traditional person-to-person communications.

Method One—Many-to-One Encryption

To send a public-key encrypted message using method one, a user (1) creates the message in normal text, (2) encrypts it *using the intended recipient's public key*, and (3) sends the encrypted message to the intended recipient over any network, including the public switched telephone system (PSTN) or the Internet. When the intended recipient receives the message, that recipient uses his or her corresponding private key to decrypt the message.

To respond to the sender, the recipient (1) drafts a response, (2) encrypts it using the sender's public key (received with the message as part of the sender's ID), and (3) sends the encrypted response to the sender. When the sender receives the response, he or she decrypts it with his or her own private key.

Method Two—One-to-Many Encryption

Method two requires an extra step. With method two, a user (1) creates the message in normal text, (2) *encrypts it using his or her own private key*, (3) then encrypts it a second time with the recipient's public key, and (4) sends the encrypted message to the intended recipient over any network. When the intended recipient receives the message, that recipient uses his or her own private key to decrypt the message and then uses the sender's public key to verify that the message is actually from the person claiming to be sending it.

To respond to the sender, the recipient (1) drafts a response, (2) encrypts it using the sender's public key received with the message as part of the sender's ID, and (3) sends the encrypted response to the sender. When the sender receives the response, he or she decrypts it with his or her private key.

With either method, public-key encryption messages are always sent to a user's public key and decrypted by that user's corresponding private key. Stated another way, a user's private key unlocks any messages sent to his or her public key.

9.4.1 Mathematical Link Between Key Pairs

Public-key cryptography works because each public/private key pair is unique and linked to each other through a complex mathematical process. The

complexity of the mathematical process ensures that a person's private key cannot be linked to two public keys at the same time, discovered from its corresponding public key, or copied, forged, or replaced. The following sections explain how this works.

Hash—Error Checking

The mathematical process that links each public/private key pair creates a single large number called a “hash.” The primary purpose of the hash is to check for errors and it can be generated in several ways, including those used in the *checksum* and *cyclic redundancy check (CRC)* error-checking algorithms.

In the checksum system, the sending computer counts or sums the number of bits in each packet as they leave the sending computer's domain. This summing of the bits creates a single number called the *check digit*. In encryption, this single number is called the hash. The check digit/hash is then attached to the “tail” or “trailer” of the packet, and is sent to the receiving computer with each packet.

As the receiving computer receives each packet, it uses the same algorithm to count the incoming bits. At the end of the packet, if the receiving computer's count of the bits in each packet agrees with the check digit/hash, the receiving computer knows that the transmission was received correctly. If not, the receiving computer asks the sending computer to resend the packet. Since the flow of the check digit/hash is only from the sending computer to the receiving computer and does not work in the reverse, it is called a one-way function.

The cyclic redundancy check (CRC) approach is different only in that the check digit/hash is generated by dividing all of the serialized bits in a packet by a predetermined binary number. The resulting single number is then sent with each packet to the receiving computer, which checks the “remainder” to confirm that the information in the communications was received correctly. It is still a one-way function, but the CRC algorithm is less secure than the checksum algorithm because several combinations of numbers can result in the same remainder and therefore produce an identical hash. This does not occur with the checksum algorithm because only one number is possible when the bits are summed. Therefore, the CRC algorithm is not used for secure communications, but does work well for link-level, bit-oriented communications.

While the primary purpose of the hash is to check for errors, it also provides several additional important benefits in encryption. Some of these are described below.

Security of Link Between Public and Private Keys

First, the one-way function of the hash process prevents a private key from being linked to two public keys at the same time. If such a link occurs, the hash will not “add up,” and the receiving computer will detect the mismatch immediately upon receipt. Thus, with public-key encryption systems, it is

mathematically infeasible for two private keys to be linked to the same public key. In the same manner, the hash produces a “fingerprint” that inextricably links one key to the other.

Decryption with Private Key

Second, the hash means that a message encrypted with a person’s public key can only be decrypted by that key’s corresponding private key. Since the two keys are mathematically linked within the encryption program, only the owner of the public key can break the code or decrypt a message sent to his or her public key. No one else, not even the person who encrypted and sent the message, can decrypt the message. Any unintended wiretapper, eavesdropper, or recipient, including governments, can see that a message exists on the network, addressed to a specific public key, but cannot read the encrypted source or content of the message.

No Discovery of Private Key through Public Key

Third, since the hashing algorithm is a one-way function, the hash cannot be analyzed or reversed to obtain the encryption key. Thus, knowing a person’s public key does not help to determine that person’s corresponding private key or discover the link between the two keys.

Encrypted Messages Cannot Be Duplicated, Forged, or Replaced

Fourth, if either the hash or the text of the message is changed in any way, the hash will not “add up” when it arrives at the receiving computer, and the change will be detected immediately. In addition, with the mismatch, the message cannot be decoded. Thus, it is mathematically infeasible for someone to copy, forge, or substitute a message encrypted with a public-key encryption, checksum system. Any attempt to do so will not produce an identical hash.

Message Digests

Fifth, when a message is encrypted, the calculation of the hash also automatically produces an encrypted, abbreviated version of the message, called a “message digest.”²³ The message digest is unique to each message and thus provides an exclusive “message ID” for that message that is then attached to the front of each encrypted message. Typically, a message digest uses a 128-bit encryption scheme, so it is highly resistant to brute-force attacks and thus “cryptographically strong.” The one-way function of the hash further ensures that it is computationally infeasible for anyone to decrypt the message digest in order to obtain the original message or to duplicate the message.

Key-IDs

Sixth, in the encryption process, the hash produces an identifier of each key used to encrypt a message. This “key ID” is an abbreviation of the full key used to encrypt the message and usually contains the least significant 64-bits of the

actual key. Like the message digest, the key ID, is attached to the front of each encrypted message as part of a “key certificate,” but usually is further abbreviated to half of its 64-bits, displaying only its lower 32 bits.

Key Certificates

Seventh, each key ID is part of a key certificate and is stored on a “key ring” With the message digest, a key certificate is attached to the front of each encrypted message. However, the key certificates and key rings for public-key systems differ from those of private-key encryption systems in the following ways.

“Private-key certificates” contain (1) the key owner’s name or user ID, (2) a private-key ID, (3) the actual private-key material, and (4) a unique encrypted password to protect the private key in case it is stolen. An individual’s private key is intended to remain private and, therefore, can only be accessed through the encrypted password.

“Public-key certificates” contain (1) the key owner’s name or user ID, (2) a public-key ID, (3) the actual public-key material, and (4) a time stamp of when the public/private-key pair was generated. An individual’s public key can be accessed through either the public-key ID or the user ID. Both are useful because many users have multiple keys and thus the same *user ID*, but no two keys are identical and therefore never have the same *key ID*.

Key Rings

Eighth, the principal method of storing and managing public and private keys are known as key rings. Rather than keep individual keys in separate key files, most encryption systems collect them on key rings to facilitate the automatic lookup of keys either by *key ID* or *user ID*. A key ring may contain one or more key certificates, but public- and private-key certificates are never combined on the same key ring. Instead, public-key rings contain only public-key certificates, and private-key rings contain only private-key certificates. Each user keeps his or her own pair of private-key and public-key rings. Additionally, each public key is temporarily stored in a separate file while in transit to a requester/recipient, who will then add it to his/her key ring.

Receipt Process—Use of Key IDs and Key Rings

Ninth, when an encrypted message is received, the key ID of the key used to encrypt the message appears in the prefixed key certificate. The recipient’s encryption software uses the key ID to find the correct private-key required to decrypt the message.

Private key: When a private-key encrypted message is received, the recipient’s software uses the private-key ID in the prefixed key certificate to retrieve the full private key from the recipient’s private-key ring. The full private key is then used to decrypt the message.

Public-key: When a public-key encrypted message is received, the recipient’s software uses the key ID of the recipient’s public key used to send the

message and provided in the prefixed key certificate, to retrieve the public key's corresponding private key from the recipient's private-key ring. The recipient's private key is then used to decrypt the message.

Validation of Sender's Identity—Digital Signature

Tenth, since both the sender's user ID and the key ID of the key used to encrypt the message appear in the key certificate attached to the front of each encrypted message, when an encrypted message is received, the recipient's software compares the sender's user ID with the sender's public-key ID on the receiver's public-key ring. If the two do not match, the mismatch immediately alerts the recipient that an imposter sent the message.

In this manner, the hash "authenticates" that the message is truly from the person who says he or she is sending it. It thus (1) validates the identity of the actual sender, (2) provides a critical part of security verification used in "firewalling," (3) prevents forgery, and (4) ensures that the response reaches the correct party. This verification is called an "electronic" or "digital signature." As an additional benefit, digital signatures also confirm that no one has tampered with or read the message en route, assuring its integrity and security.²⁴

9.4.2 Digital Signatures

Sending Process—Creation of a Digital Signature

Since a digital signature is created when a sender uses his or her private key to encrypt a message, it is, therefore, an integral part of the encryption process. As such, encryption provides, at no additional cost, nonforgible electronic signatures that are far more secure, reliable, accurate, and verifiable than a handwritten signature. For this reason, they prevent confusion and fraud in the Internet Age and provide the security required by persons doing business in a non-face-to-face manner. As such, digital signatures will be an increasingly important technology in the new Internet Age. They provide the means for any intended recipient to receive a highly secure, identifiable private message that cannot be altered or decrypted by others. Without this digital verification, e-commerce and advanced uses of communication could not proceed to its fullest potential.

1991/1993—U.S. Digital Signature Algorithm (DSA)

Since the National Institute of Standards and Technology (NIST) was given responsibility for computers and related systems in the Brooks Act of 1965, it reviewed encryption and digital signature issues for the United States in the 1970s and 1980s, even before people realized the importance of digital signatures to commerce and other official communications. However, it wasn't until a quarter of a century later, in August 1991, that NIST announced its selection

of the United States's digital signature standard, called the digital signature algorithm (DSA). The DSA, developed by an employee of the National Security Agency (NSA) was made available free to users with no royalties charged, but it was not broadly embraced because of its close connection to NSA.

1993—Digital Signature Standard (DSS)

As a result, two years later, in June 1993, NIST announced a second, more refined standard known as the digital signature standard (DSS). NIST first issued its Notice of Approval for the DSS on May 19, 1994.²⁵ When it received no negative comments, it proceeded with its recommendation to the White House and U.S. Congress. Both approved the DSS as the U.S. standard in 1994 and reconfirmed it four years later, on December 9 1998.²⁶ It continues to be the standard used for digital used for digital signature technology in the United States today.

1999—Millennium Digital Commerce Act (MDCA)

Based on this standard, the next year, in 1999, Senator Spencer Abraham (R, Michigan) sponsored the Millennium Digital Commerce Act (MDCA) to “ensure that individuals and organizations in different states are held to their agreements and obligations even if their respective state have different rules concerning electronically signed documents.” The proposed MDCA sought to (1) prohibit individual state laws from restricting the legality of digital contracts simply because they are in electronic form, (2) establish guidelines for international use of electronic signatures that would remove obstacles to electronic transactions, and (3) allow the market to determine the type of authentication technology used in international commerce.

2000—Electronic Signatures in Global and National Commerce Act (E-SIGN Commerce Act), June 30, 2000

Springboarding off the support generated by the proposed Millennium Digital Commerce Act, the U.S. Congress passed the Electronics Signatures in Global and National Commerce Act (E-SIGN Commerce Act) of 2000, also known as the Digital Signature Act (DSA), enacted on June 30, 2000. The DSA affirmed the legal validity of digital signatures for e-commerce transactions, contracts, and court documents. For this reason, it is an enormously important law in the new Internet Age. The two major reasons Congress passed the Digital Signature Act were: digital signatures are superior to handwritten signatures, in that they cannot be forged or later denied, and numerous commerce and trade groups, plus many judicial courts petitioned in strong support of them. This new law has generated numerous activities that are best tracked through sources such as the Digital Signatures: A Practitioners Checklist found at <http://www.macleoddixon.com/04public/Articles/digsig.pdf>.

9.4.3 Key Servers

As the effectiveness and popularity of public-key systems have increased, a recipient's public key must be known in order to use it. When public-key systems were first developed, if a recipient's public key was unknown, it was difficult to find. Today, however, public keys are as easy to locate as someone's telephone number. Many companies also offer public-key information with their employees phone numbers. Public directories, or "key servers," act as white pages or information databases, providing easy-to-use, readily available, up-to-date listings of public keys. Acknowledging that not everyone wants his or her phone number or public key published, key servers require registration of each public key by the key owner. In the future, key servers are likely to be an increasingly significant part of the National Information Infrastructure (NII), especially since public keys are required to verify digital signatures. Generally, key servers fall into two basic categories: certification and "web-of-trust" systems.

Certification

Certification key servers involve a central body or certification authority with whom parties register their public keys. The central body then uses its private key to "sign" or "certify" each registered party's public key for anyone seeking confirmation that a public key is truly owned by a particular party. The U.S. Post Office has proposed that it serve as such authority for the United States in the future.

Web of Trust

In contrast, a *web-of-trust* key server involves no central authority. Instead, users upload their public keys to a key server at any time. To verify that a specific individual is the true owner of a public key, the inquirer asks other people to "certify" the key ownership by uploading authentications "signed" by their private keys.

9.4.4 Session Keys

A second issue with public-key encryption systems is that the encryption and decryption processes take longer, require more resources, and thus are slower than with one-key systems, such as DES. For this reason, in the 1970s and early 1980s, one-key systems were used for longer messages and real-time applications, while two-key systems were more useful for shorter messages and stored information.

Today, with high-speed computers, this time and resource difference is less noticeable, but still a factor. To solve this speed problem while retaining

the advantages of public-key systems, “session keys” are used. Each session key is unique and used only for one communication or session. Two of the most popular types of session keys are “hybrid systems” and “key exchanges.” The strengths and weaknesses of both are discussed below.

Diffie-Hellman Key Exchange

When a recipient’s public key is not known and not available in a key server, or when the two parties wish to establish a session key in public, rather than in private, the parties may use a “key exchange.” In 1976, a year after the original public-key concept was developed, two of the developers, Diffie and Hellman, published a paper in *IEEE Transactions* entitled “New Directions in Cryptography,” in which they described a partial solution to these problems existing with the use of public-key cryptosystems.²⁷ With the Diffie-Hellman Key Exchange, for example, the following procedure is followed.

1. Parties A and B first send each other numbers (N_1 and N_2) to establish a session key.
2. In the session, Parties A and B then agree on a number (b) to serve as the basis for their calculations. This number does not have to be kept secret.
3. With the calculation number, parties agree on a large prime number, which will serve as their “modulus m ” or base for arithmetic operations. Normally, we operate in “base ten,” while in binary we calculate in “base two.”
4. To add to their “base number,” the parties A and B select two secret large random numbers (A and B).
5. Party A then sends the number she calculates as $[(b \times A) \text{ modulus } m]$ to Party B.
6. Party B reciprocates with $[(b \times B) \text{ modulus } m]$.
7. Finally, both parties can then compute $[b \times AB]$, which becomes their secret session key for subsequent encryption of their information.

While this sounds complicated, it is easy to calculate, especially with computers, and yet very difficult to break. It works well for real-time communication, but imposes long delays as the parties exchange the six or more messages to generate a session key.

The Diffie-Hellman Key Exchange also provided an additional feature, the reality of ephemeral keys that changed the basic power relationships in cryptography because they allow two parties to create a secret key in a very public “conversation,” without the use of any centralized resources. Before public-key cryptography, encryption always required centralized facilities to manufacture and distribute equipment and keys—consistent with the military’s top-down structure. After public-key encryption systems became available, businesses could communicate readily with each other even if the parties did not know each other or had never done business before.

Hybrid Systems

Hybrid session key systems are similar to the Diffie-Hellman systems except that instead of going through the multiple steps to develop a session key the following occurs.

1. Party A simply generates a session key, encrypts it with Party B's public key, and sends the encrypted message to Party B.
2. Party B then decrypts the message with his or her private key, inputs the session key into his or her single-key software or telephone, and begins the conversation or data transfer in the faster temporary, single-key mode.
3. The actual process of selecting the temporary, random session key is invisible to the users because it occurs in the mathematical algorithm contained in the encryption software each uses.

This more simplified process retains the ability for two parties to communicate in a secure manner over a nonsecure communications link such as the public phone system, wireless communications, or the Internet. For this reason, public-key systems have become the preferred encryption systems for email and e-commerce communications. The most popular systems include the RSA, Pretty Good Privacy (PGP), and Hewlett-Packard's VeriSecure. Each is described below.

9.4.5 Well-Known Public-Key Cryptosystems

RSA

In 1977, one year after Diffie and Hellman's paper was published in *IEEE Transactions*, three young faculty members from MIT, Ronald Rivest, Adi Shamir, and Leonard Adelman, began a company called the RSA Data Security, Inc. in Redwood City, California. They developed a popular two-key system called the RSA system. Like the name of their company, their software product's name came from the first initial of each developer's last name.

The RSA system uses two very large prime numbers to create the public-private-key pairs. The two prime numbers are then multiplied by each other, creating a number that is over 200 digits long. Nearly 22 years later, on January 6, 1999, RSA Data Security, Inc. established an Australian subsidiary through which it distributes its encryption products without violating the then-existing U.S. 56-bit limit on exported encryption systems. That U.S. limit has recently been increased to 128-bits, but it is still less than the RSA's capability.

Pretty Good Privacy

All encryption systems developed in the 1970s and 1980s used 56-bit keys. However, in the early 1990s, Philip Zimmerman, a computer programmer in

Boulder, Colorado, designed a public-key encryption program that conformed to the DES algorithm, but used a variable key-bit length starting at 128-bit key encryption and moving up from there. Each user may select the key length he or she desires.²⁸ Zimmerman named his new program the Pretty Good Privacy (PGP) encryption system and shared it with friends. The program was eventually loaded onto an Internet bulletin board.

While Zimmerman never sold PGP, it is now available worldwide from the Internet and has become the de facto standard for Internet email. For this reason, it is called the “encryption program of the people.” Governments worldwide, however, oppose it because no government or law enforcement agency, including the U.S. government and the U.S. National Security Agency, can break the code.²⁹ In part, this is because of its variable key-bit length, but mainly because all public-key technology is so hard to break. The PGP encryption system is also based on a web-of-trust validation system, so it is completely independent of centralized control.

Hewlett-Packard’s VeriSecure

Hewlett-Packard also developed a public-key encryption system known as VeriSecure, which received the U.S. government’s approval to export to customers in five countries. However, the Center for Democracy and Technology opposes VeriSecure because of the extent of government access built into its design.

9.5

COMPARISON OF PRIVATE-KEY AND PUBLIC-KEY ENCRYPTION TECHNOLOGIES

Both private-key and public-key encryption systems were developed in academia in the early 1970s and provide very secure modern communications over public networks. Both use computers and many of the same technical concepts and approaches including (1) a mathematical process that generates each key, (2) an error checking scheme that also generates a hash, (3) message digests, (4) key IDs, (5) key certificates, and (6) key rings. However, the manner in which the two encryption systems do this differs significantly. The similarities and differences, advantages and disadvantages, of each are compared in Table 9.1 on pages 354 and 355.

Given today’s technological environment, encryption provides a very effective, efficient, and affordable means of retaining privacy in communications and protecting users against electronic theft, fraud, and forgery. As such, it meets the privacy needs of modern communicators, whether over the Internet, satellite, optic fiber, wireless, or other paths of modern communications.