

CRYPTOGRAPHY'S
ROLE
IN
SECURING THE
INFORMATION
SOCIETY

Kenneth W. Dam and Herbert S. Lin, *Editors*

Committee to Study National Cryptography Policy

Computer Science and Telecommunications Board

Commission on Physical Sciences, Mathematics, and Applications

National Research Council

NATIONAL ACADEMY PRESS
Washington, D.C. 1996

Contents

EXECUTIVE SUMMARY	1
A ROAD MAP THROUGH THIS REPORT	15

PART I—FRAMING THE POLICY ISSUES

1	GROWING VULNERABILITY IN THE INFORMATION AGE	19
1.1	The Technology Context of the Information Age, 19	
1.2	Transition to an Information Society—Increasing Interconnections and Interdependence, 22	
1.3	Coping with Information Vulnerability, 27	
1.4	The Business and Economic Perspective, 30	
1.4.1	Protecting Important Business Information, 30	
1.4.2	Ensuring the Nation’s Ability to Exploit Global Markets, 38	
1.5	Individual and Personal Interests in Privacy, 40	
1.5.1	Privacy in an Information Economy, 41	
1.5.2	Privacy for Citizens, 44	
1.6	Special Needs of Government, 46	
1.7	Recap, 48	

2	CRYPTOGRAPHY: ROLES, MARKET, AND INFRASTRUCTURE	51
2.1	Cryptography in Context, 51	
2.2	What Is Cryptography and What Can It Do?, 52	
2.3	How Cryptography Fits into the Big Security Picture, 57	
2.3.1	Factors Inhibiting Access to Information, 58	
2.3.2	Factors Facilitating Access to Information, 60	
2.4	The Market for Cryptography, 65	
2.4.1	The Demand Side of the Cryptography Market, 66	
2.4.2	The Supply Side of the Cryptography Market, 72	
2.5	Infrastructure for Widespread Use of Cryptography, 74	
2.5.1	Key Management Infrastructure, 74	
2.5.2	Certificate Infrastructures, 75	
2.6	Recap, 77	
3	NEEDS FOR ACCESS TO ENCRYPTED INFORMATION	79
3.1	Terminology, 79	
3.2	Law Enforcement: Investigation and Prosecution, 81	
3.2.1	The Value of Access to Information for Law Enforcement, 81	
3.2.2	The Legal Framework Governing Surveillance, 84	
3.2.3	The Nature of the Surveillance Needs of Law Enforcement, 88	
3.2.4	The Impact of Cryptography and New Media on Law Enforcement (Stored and Communicated Data), 90	
3.3	National Security and Signals Intelligence, 94	
3.3.1	The Value of Signals Intelligence, 95	
3.3.2	The Impact of Cryptography on Signals Intelligence, 101	
3.4	Similarities in and Differences Between Foreign Policy/National Security and Law Enforcement Needs for Communications Monitoring, 102	
3.4.1	Similarities, 102	
3.4.2	Differences, 104	
3.5	Business and Individual Needs for Exceptional Access to Protected Information, 104	
3.6	Other Types of Exceptional Access to Protected Information, 108	
3.7	Recap, 109	

PART II—POLICY INSTRUMENTS

- | | | |
|-------|---|-----|
| 4 | EXPORT CONTROLS | 113 |
| 4.1 | Brief Description of Current Export Controls, 113 | |
| 4.1.1 | The Rationale for Export Controls, 113 | |
| 4.1.2 | General Description, 114 | |
| 4.1.3 | Discussion of Current Licensing Practices, 122 | |
| 4.2 | Effectiveness of Export Controls on Cryptography, 127 | |
| 4.3 | The Impact of Export Controls on U.S. Information Technology Vendors, 134 | |
| 4.3.1 | De Facto Restrictions on the Domestic Availability of Cryptography, 134 | |
| 4.3.2 | Regulatory Uncertainty Related to Export Controls, 138 | |
| 4.3.3 | The Size of the Affected Market for Cryptography, 145 | |
| 4.3.4 | Inhibiting Vendor Responses to User Needs, 152 | |
| 4.4 | The Impact of Export Controls on U.S. Economic and National Security Interests, 153 | |
| 4.4.1 | Direct Economic Harm to U.S. Businesses, 153 | |
| 4.4.2 | Damage to U.S. Leadership in Information Technology, 155 | |
| 4.5 | The Mismatch Between the Perceptions of Government/ National Security and Those of Vendors, 157 | |
| 4.6 | Export of Technical Data, 159 | |
| 4.7 | Foreign Policy Considerations, 162 | |
| 4.8 | Technology-Policy Mismatches, 163 | |
| 4.9 | Recap, 165 | |
| 5 | ESCROWED ENCRYPTION AND RELATED ISSUES | 167 |
| 5.1 | What Is Escrowed Encryption?, 167 | |
| 5.2 | Administration Initiatives Supporting Escrowed Encryption, 169 | |
| 5.2.1 | The Clipper Initiative and the Escrowed Encryption Standard, 170 | |
| 5.2.2 | The Capstone/Fortezza Initiative, 176 | |
| 5.2.3 | The Relaxation of Export Controls on Software Products Using “Properly Escrowed” 64-bit Encryption, 177 | |
| 5.2.4 | Other Federal Initiatives in Escrowed Encryption, 179 | |
| 5.3 | Other Approaches to Escrowed Encryption, 179 | |

- 5.4 The Impact of Escrowed Encryption on Information Security, 181
 - 5.5 The Impact of Escrowed Encryption on Law Enforcement, 184
 - 5.5.1 Balance of Crime Enabled vs. Crime Prosecuted, 184
 - 5.5.2 Impact on Law Enforcement Access to Information, 185
 - 5.6 Mandatory vs. Voluntary Use of Escrowed Encryption, 187
 - 5.7 Process Through Which Policy on Escrowed Encryption Was Developed, 188
 - 5.8 Affiliation and Number of Escrow Agents, 189
 - 5.9 Responsibilities and Obligations of Escrow Agents and Users of Escrowed Encryption, 193
 - 5.9.1 Partitioning Escrowed Information, 193
 - 5.9.2 Operational Responsibilities of Escrow Agents, 194
 - 5.9.3 Liabilities of Escrow Agents, 197
 - 5.10 The Role of Secrecy in Ensuring Product Security, 201
 - 5.10.1 Algorithm Secrecy, 201
 - 5.10.2 Product Design and Implementation Secrecy, 204
 - 5.11 The Hardware/Software Choice in Product Implementation, 208
 - 5.12 Responsibility for Generation of Unit Keys, 211
 - 5.13 Issues Related to the Administration Proposal to Relax Export Controls on 64-bit Escrowed Encryption in Software, 213
 - 5.13.1 The Definition of "Proper Escrowing," 213
 - 5.13.2 The Proposed Limitation of Key Lengths to 64 Bits or Less, 214
 - 5.14 Recap, 215
- 6 OTHER DIMENSIONS OF NATIONAL CRYPTOGRAPHY POLICY 216
- 6.1 The Communications Assistance for Law Enforcement Act, 216
 - 6.1.1 Brief Description of and Stated Rationale for the CALEA, 217
 - 6.1.2 Reducing Resource Requirements for Wiretaps, 218
 - 6.1.3 Obtaining Access to Digital Streams in the Future, 220

- 6.1.4 The CALEA Exemption of Information Service Providers and Distinctions Between Voice and Data Services, 221
- 6.2 Other Levers Used in National Cryptography Policy, 221
 - 6.2.1 Federal Information Processing Standards, 222
 - 6.2.2 The Government Procurement Process, 224
 - 6.2.3 Implementation of Policy: Fear, Uncertainty, Doubt, Delay, Complexity, 225
 - 6.2.4 R&D Funding, 227
 - 6.2.5 Patents and Intellectual Property, 228
 - 6.2.6 Formal and Informal Arrangements with Various Other Governments and Organizations, 231
 - 6.2.7 Certification and Evaluation, 232
 - 6.2.8 Nonstatutory Influence, 234
 - 6.2.9 Interagency Agreements Within the Executive Branch, 235
- 6.3 Organization of the Federal Government with Respect to Information Security, 237
 - 6.3.1 Role of National Security vis-à-vis Civilian Information Infrastructures, 237
 - 6.3.2 Other Government Entities with Influence on Information Security, 241
- 6.4 International Dimensions of Cryptography Policy, 243
- 6.5 Recap, 244

PART III—POLICY OPTIONS, FINDINGS, AND RECOMMENDATIONS

- 7 POLICY OPTIONS FOR THE FUTURE 249
 - 7.1 Export Control Options for Cryptography, 249
 - 7.1.1 Dimensions of Choice for Controlling the Export of Cryptography, 249
 - 7.1.2 Complete Elimination of Export Controls on Cryptography, 251
 - 7.1.3 Transfer of All Cryptography Products to the Commerce Control List, 254
 - 7.1.4 End-use Certification, 256
 - 7.1.5 Nation-by-Nation Relaxation of Controls and Harmonization of U.S. Export Control Policy on Cryptography with Export/Import Policies of Other Nations, 256
 - 7.1.6 Liberal Export for Strong Cryptography with Weak Defaults, 257

7.1.7	Liberal Export for Cryptographic Applications Programming Interfaces, 259	
7.1.8	Liberal Export for Escrowable Products with Encryption Capabilities, 262	
7.1.9	Alternatives to Government Certification of Escrow Agents Abroad, 263	
7.1.10	Use of Differential Work Factors in Cryptography, 264	
7.1.11	Separation of Cryptography from Other Items on the U.S. Munitions List, 264	
7.2	Alternatives for Providing Government Exceptional Access to Encrypted Data, 265	
7.2.1	A Prohibition on the Use and Sale of Cryptography Lacking Features for Exceptional Access, 265	
7.2.2	Criminalization of the Use of Cryptography in the Commission of a Crime, 273	
7.2.3	Technical Nonescrow Approaches for Obtaining Access to Information, 274	
7.2.4	Network-based Encryption, 278	
7.2.5	Distinguishing Between Encrypted Voice and Data Communications Services for Exceptional Access, 281	
7.2.6	A Centralized Decryption Facility for Government Exceptional Access, 284	
7.3	Looming Issues, 286	
7.3.1	The Adequacy of Various Levels of Encryption Against High-Quality Attack, 286	
7.3.2	Organizing the U.S. Government for Better Information Security on a National Basis, 289	
7.4	Recap, 292	
8	SYNTHESIS, FINDINGS, AND RECOMMENDATIONS	293
8.1	Synthesis and Findings, 293	
8.1.1	The Problem of Information Vulnerability, 293	
8.1.2	Cryptographic Solutions to Information Vulnerabilities, 296	
8.1.3	The Policy Dilemma Posed by Cryptography, 297	
8.1.4	National Cryptography Policy for the Information Age, 298	
8.2	Recommendations, 303	
8.3	Additional Work Needed, 338	
8.4	Conclusion, 339	

APPENDIXES

A	CONTRIBUTORS TO THE NRC PROJECT ON NATIONAL CRYPTOGRAPHY POLICY	343
	A.1 Committee Members, 343	
	A.2 Additional Contributors to the Project, 349	
B	GLOSSARY	353
C	A BRIEF PRIMER ON CRYPTOGRAPHY	364
	C.1 A Very Short History of Cryptography, 364	
	C.2 Capabilities Enabled by Cryptography, 365	
	C.2.1 Ensuring the Integrity of Data, 365	
	C.2.2 Authentication of Users, 367	
	C.2.3 Nonrepudiation, 370	
	C.2.4 Preservation of Confidentiality, 371	
	C.3 Basic Constructs of Cryptography, 374	
	C.4 Attacks on Cryptographic Systems, 378	
	C.5 Elements of Cryptographic Security, 383	
	C.6 Expected Lifetimes of Cryptographic Systems, 384	
	C.6.1 Background, 385	
	C.6.2 Asymmetric Cryptographic Systems, 385	
	C.6.3 Conventional Cryptographic Systems, 388	
	C.6.4 Timing Attacks, 390	
	C.6.5 Skipjack/Clipper/EES, 391	
	C.6.6 A Warning, 391	
	C.6.7 Quantum and DNA Computing, 392	
	C.6.8 Elliptic Curve Cryptographic Systems, 394	
	C.6.9 Quantum Cryptography, 394	
D	AN OVERVIEW OF ELECTRONIC SURVEILLANCE: HISTORY AND CURRENT STATUS	396
	D.1 The Legal Framework for Domestic Law Enforcement Surveillance, 396	
	D.1.1 The General Prohibition on Electronic Surveillance, 396	
	D.1.2 Title III of the Omnibus Crime Control and Safe Streets Act of 1968 and the Electronic Communications Privacy Act of 1986, 396	
	D.1.3 The Foreign Intelligence Surveillance Act, 403	
	D.2 Historical Overview of Electronic Surveillance, 410	

- N.2 Executive Orders, 573
 - N.2.1 Executive Order 12333 (U.S. Intelligence Activities), 573
 - N.2.2 Executive Order 12958 (Classified National Security Information), 589
 - N.2.3 Executive Order 12472 (Assignment of National Security and Emergency Preparedness Telecommunications Functions), 612
 - N.2.4 National Security Directive 42 (National Policy for the Security of National Security Telecommunications and Information Systems), 620
- N.3 Memorandums of Understanding (MOU) and Agreement (MOA), 627
 - N.3.1 National Security Agency/National Institute of Standards and Technology MOU, 627
 - N.3.2 National Security Agency/Federal Bureau of Investigation MOU, 630
 - N.3.3 National Security Agency/Advanced Research Projects Agency/Defense Information Systems Agency MOA, 632
- N.4 Regulations, 636
 - N.4.1 International Traffic in Arms Regulations (22 CFR, Excerpts from Parts 120-123, 125, and 126), 636
 - N.4.2 Export Administration Regulations, 655