

CONTENTS

CHAPTER 1

OVERVIEW 1

- 1.1 Attacks, Services, and Mechanisms 4
- 1.2 Security Attacks 7
- 1.3 Security Services 10
- 1.4 A Model for Internetwork Security 12
- 1.5 Outline of the Book 14
- 1.6 Recommended Reading 18

PART I

INTERNETWORK SECURITY PRINCIPLES

CHAPTER 2

CONVENTIONAL ENCRYPTION 21

- 2.1 Conventional Encryption Model 22
- 2.2 Classical Encryption Techniques 27
- 2.3 The Data Encryption Standard (DES) 42
- 2.4 Triple DES 64
- 2.5 Recommended Reading 69
- 2.6 Problems 70

CHAPTER 3

CONFIDENTIALITY USING CONVENTIONAL ENCRYPTION 76

- 3.1 Placement of Encryption Function 77
- 3.2 Traffic Confidentiality 86
- 3.3 Key Distribution 87
- 3.4 Random Number Generation 96
- 3.5 Recommended Reading 103
- 3.6 Problems 103

CHAPTER 4

PUBLIC-KEY CRYPTOLOGY 107

- 4.1 Principles of Public-Key Cryptosystems 109
- 4.2 The RSA Algorithm 121

4.3	Key Management	129
4.4	Recommended Reading	136
4.5	Problems	137
APPENDIX 4A: Introduction to Number Theory		141
APPENDIX 4B: The Complexity of Algorithms		153

CHAPTER 5

AUTHENTICATION AND DIGITAL SIGNATURES 157

5.1	Authentication Requirements	158
5.2	Authentication Functions	159
5.3	Cryptographic Checksums	171
5.4	Hash Functions	174
5.5	Digital Signatures	184
5.6	Authentication Protocols	188
5.7	Recommended Reading	197
5.8	Problems	198
APPENDIX 5A: Mathematical Basis of Birthday Attack		201

CHAPTER 6

INTRUDERS, VIRUSES, AND WORMS 207

6.1	Intruders	208
6.2	Viruses	238
6.3	Worms	250
6.4	Trusted Systems	255
6.5	Recommended Reading	262
6.6	Problems	263

PART II

INTERNETWORK SECURITY PRACTICE

CHAPTER 7

CRYPTOGRAPHIC ALGORITHMS 267

7.1	The MD5 Message Digest Algorithm	268
7.2	The Secure Hash Algorithm (SHA)	276
7.3	International Data Encryption Algorithm (IDEA)	282
7.4	SKIPJACK	293
7.5	LUC Public-Key Encryption	300
7.6	Problems	309
APPENDIX 7A: Mathematical Details of the LUC Algorithm		311

*CHAPTER 8***AUTHENTICATION AND KEY EXCHANGE** 314

- 8.1 Kerberos 315
- 8.2 X.509 Directory Authentication Service 333
- 8.3 Diffie-Hellman Key Exchange 340
- 8.4 Digital Signature Standard (DSS) 343
- 8.5 Problems 346
- APPENDIX 8A: Kerberos Encryption Techniques 349
- APPENDIX 8B: Discrete Logarithms 352
- APPENDIX 8C: Proof of the DSS Algorithm 357

*CHAPTER 9***ELECTRONIC MAIL SECURITY** 360

- 9.1 Pretty Good Privacy (PGP) 361
- 9.2 Privacy Enhanced Mail (PEM) 383
- 9.3 Problems 403
- APPENDIX 9A: Data Compression Using ZIP 404
- APPENDIX 9B: Radix-64 Conversion 407
- APPENDIX 9C: PGP Random Number Generation 408

*CHAPTER 10***NETWORK MANAGEMENT SECURITY** 412

- 10.1 Basic Concepts of SNMP 413
 - 10.2 SNMPv1 Community Facility 421
 - 10.3 SNMPv2 Security Facility 424
 - 10.4 Problems 441
- Glossary 443
- Standards Cited in This Book 447
- References 449
- Index 457