

Contents

Preface	ix
Chapter 1 Security Threats, Services, and Mechanisms	1
1.1 Introduction	1
1.1.1 The Security Policy	2
1.1.2 Risk Analysis and Management	4
1.1.3 Summary	6
1.2 Deliberate Threats to Information	6
1.3 Services	7
1.4 Security Mechanisms	9
1.4.1 Encryption	9
1.4.2 Integrity Checks	10
1.4.3 Uniqueness Mechanisms	12
1.5 Security Standards	13
1.6 Summary	16
References	16
Chapter 2 Security Procedures	17
2.1 Attacks To Be Thwarted	17
2.1.1 Statistical Analysis	17
2.1.2 Known Plaintext Attack	18
2.1.3 Chosen Cyphertext Attack	18
2.1.4 Searching the Key Space	18
2.1.5 Breaking the Algorithm	18
2.1.6 Stealing the Key	19
2.1.7 Introducing a False Key	19
2.1.8 Modifying Cyphertext	19
2.1.9 Modifying Plaintext	19
2.2 Encryption Procedures	20

2.3	Authentication Procedures	24
2.3.1	Secure Access Management	27
2.3.2	Personal Identification Procedures	31
2.3.3	Chipcards for Access Control	35
2.3.4	The Secure Session	38
2.3.5	Anonymity	41
2.4	OSI Layers and Networks	43
	References	46
Chapter 3	Security Management	47
3.1	Scope of Security Management	47
3.2	Key Management	48
3.2.1	Key Generation	48
3.2.2	Certification and Notarisation of Keys	51
3.2.3	Distribution of Keys	55
3.2.4	Withdrawal of Keys	59
3.3	PIN Management	60
3.4	Authorization	61
3.5	System Security Management	63
3.6	Security Service Management	66
	References	68
Chapter 4	Algorithms	69
4.1	Traditional Cypher Algorithms	69
4.2	The Data Encryption Algorithm	77
4.3	Asymmetric Algorithms	82
4.3.1	DL Authentication	86
4.3.2	The RSA Algorithm	86
4.3.3	Fiat-Shamir (FS) Signatures	90
4.3.4	Trapdoor Knapsack Schemes	92
4.3.5	Making Asymmetric Cyphers From Symmetric Ones	95
4.4	Stream Cyphers	98
4.5	Some Other Useful Algorithms	104
4.5.1	Hashing	104
4.5.2	Random Numbers	110
4.5.3	The Euclidean Algorithm	113
4.6	Conclusion	115
	References	115
Chapter 5	OSI and Security	117
5.1	The OSI/RM and Security	117
5.2	Security and X.400 MHS	122
5.2.1	Origin Authentication	127
5.2.2	Proof and Nonrepudiation of Submission and Delivery	127

5.2.3	Secure Access Management	129
5.2.4	Integrity/Confidentiality	130
5.2.5	General Message Security Services	132
5.2.6	Registration Security Services	132
5.2.7	A Different Approach—PEM	133
5.3	EDI Security	134
5.3.1	X.435 and Security	134
5.3.2	The ANSI X12 Secure EDI Approach	138
5.3.3	Security and EDIFACT	142
5.4	The X.500 Directory	144
5.5	Conclusion	147
	References	148
Chapter 6	Applications, Systems, Products, and Architectures	149
6.1	Some Banking and Financial Applications	149
6.1.1	ISO 8730	150
6.1.2	SWIFT	151
6.1.3	ETEBAC 5	152
6.1.4	ATMs and Debit and Credit Cards	154
6.2	Security Products	155
6.2.1	Communication Encryptors	155
6.2.2	File Security Products	158
6.2.3	Products for User Identification	159
6.2.4	Products for Intersystem Access Control	162
6.2.5	Security Management Products	163
6.2.6	Some Other Relevant Products	165
6.2.7	A Typical Security Product for a PC	166
6.3	Security Architectures	166
6.3.1	Kerberos	167
6.3.2	SESAME	169
6.3.3	Comparison of Architectures	173
6.3.4	Other Security Architectures	174
	References	175
Chapter 7	Conclusion	177
7.1	Voice and Video Networks	177
7.2	Security of Mobile- and Radio-Based Systems	179
7.3	Some Other Application Areas for Security	181
	References	182
Appendix A	The Open Systems Interconnection Reference Model (OSI/RM) and Security	185
	References	189
Appendix B	Shannon's Theory of Secrecy Systems	191

B.1	Perfect Secrecy	191
B.2	The Unicity Key Length and Unicity Distance	193
References		194
Appendix C	Maximum Length Sequences	195
C.1	Linear Feedback Shift Registers (LFBSR)	196
C.2	Another Form for LFBSRs	198
C.3	De Bruijn Sequences	199
C.4	Statistical Properties of MLSs	203
C.5	Synthesizing Sequences—The Massey Algorithm	204
References		206
Appendix D	Euler's Totient Function	207
References		213
Appendix E	Finding Large Prime Numbers	215
E.1	Testing Primality	216
E.2	Finding Primes for RSA	220
References		221
Appendix F	Factorising Large Integers	223
F.1	Fermat Factorisation	223
F.2	Pollard's Monte Carlo Method	224
References		226
Appendix G	The CCITT X.400 (1988) Message Handling Systems Recommendations	227
Appendix H	Information Technology Security Evaluation Criteria	229
H.1	Assuring Effectiveness	230
H.2	Assuring Correctness	231
H.2.1	Construction	231
H.2.2	Operation	232
Selected Bibliography		233
Index		237