

1	Basic Concepts and Historical Overview	1
1.1	Introduction	1
1.1.1	Encryption	1
1.1.2	Algorithms and Keys	2
1.1.3	Strong Cryptosystems Design Principles	4
1.1.4	Computational Complexity of Algorithms	5
1.2	Simple Stream Ciphers	10
1.2.1	Caesar Cipher	10
1.2.2	XOR Encryption (Vernam Cipher)	11
1.3	Simple Block Ciphers	13
1.3.1	Permutations	13
1.3.2	Transpositions	13
1.3.3	Example of a Simple Transposition Cipher	14
1.3.4	Example of a Substitution Block Cipher	17
1.3.5	Example of a Product Cipher	17
1.3.6	Generalized Substitutions—Bigrams	18
1.3.7	Polyalphabetic Substitutions	20
1.3.8	Vigenère Cipher	20
1.4	Wheel Cipher and Rotor Machines	21
1.4.1	Wheel Cipher	21
1.4.2	Rotor Machines	22
1.5	Enigma	23
1.5.1	History of the Enigma	24
1.5.2	Construction of the Enigma	26
1.5.3	Enigma Operation	29
1.5.4	Breaking the Enigma Cipher	31

2	Mathematical Foundations of Cryptography	37
2.1	Basic Concepts in the Theory of Algebraic Structures	37
2.1.1	Groups	38
2.1.2	Rings and Fields	40
2.1.3	Finite Fields	44
2.1.4	Polynomial Ring	45
2.1.5	Applications of Galois Fields	49
2.2	Elements of Number Theory	50
2.2.1	Divisibility	50
2.2.2	Prime Numbers and Their Properties	52
2.2.3	Euler's Function	55
2.2.4	Modular Congruences	55
2.2.5	Simple Modular Equations	57
2.2.6	Euler's Theorem	59
2.3	Sieve of Eratosthenes, Euclidean Algorithms	59
2.3.1	Sieve of Eratosthenes	59
2.3.2	Euclidean Algorithm	60
2.3.3	Extended Euclidean Algorithm	64
2.4	Tests for Primality	67
2.4.1	Fermat's Test	67
2.4.2	Fermat's Primality Test	68
2.4.3	Miller-Rabin Test	69
2.4.4	Algorithm AKS	70
2.5	Computationally Hard Problems in Number Theory	71
2.5.1	Factorization	72
2.5.2	Discrete Logarithm Problem	75
3	Foundations of Symmetric Cryptography	77
3.1	Idea of Symmetric Cryptography	77
3.1.1	The Feistel Network	78
3.2	The DES Algorithm	79
3.2.1	S-Boxes	79
3.2.2	Description of the DES Algorithm	80
3.2.3	Breaking DES	85
3.3	Extensions of the DES Algorithm	86
3.3.1	Triple DES	86
3.3.2	DESX	87
3.4	Modes of Operation of the DES Algorithm	87
3.4.1	Electronic Codebook Mode of Operation	87
3.4.2	Cipher Block-Chaining Mode of Operation	87
3.4.3	Cipher Feedback Mode of Operation	89
3.5	The IDEA Algorithm	90
3.6	RC Algorithms	92
3.6.1	RC4 Algorithm	92
3.6.2	RC5 Algorithm	94
3.6.3	RC5-Breaking Project	96
3.6.4	RC6 Algorithm	99

3.7	AES—The Successor to DES	100
3.7.1	Mathematical Foundations of AES	100
3.7.2	Description of the Algorithm	108
3.7.3	Key Expansion	111
3.7.4	Encryption Algorithm	113
3.7.5	Decryption Algorithm	114
3.8	Generalizations and Refinements of DES, IDEA and AES	117
3.8.1	Algorithms DES-768, IDEA-832, AES-1408, AES-1664, and AES-1920	117
3.8.2	Generalized DES and AES Ciphers	118
4	Foundations of Asymmetric Cryptography	119
4.1	Idea of Asymmetric Cryptography	119
4.2	The Diffie-Hellman Algorithm	120
4.3	The ElGamal Algorithm	121
4.4	The RSA Algorithm	123
4.4.1	Key Generation	123
4.4.2	Encryption and Decryption	124
5	An Electronic Signature and Hash Functions	127
5.1	Digital Signature Algorithms	127
5.1.1	A Digital Signature	128
5.1.2	The RSA Signature	129
5.1.3	The ElGamal Signature	130
5.1.4	DSA Signature	131
5.2	Cryptographic Hash Functions	132
5.2.1	Classification of Hash Functions	134
5.2.2	Birthday Paradox and Brute Force	135
5.2.3	MD5 Algorithm	136
5.2.4	SHA-1 Algorithm	140
5.2.5	Keccak/SHA-3	142
6	PGP Systems and TrueCrypt	147
6.1	PGP System	147
6.1.1	The Idea and the History of PGP	147
6.1.2	PGP Algorithms	149
6.1.3	The Use of PGP	152
6.1.4	Web of Trust and Key Certification	161
6.2	FireGPG and Enigmail	162
6.3	TrueCrypt	164
6.3.1	Formating the TrueCrypt Volume	165
6.3.2	Encrypting a Partition	169
6.3.3	Forming a Hidden Volume	170
6.3.4	Work with Hidden Volumes	171
6.3.5	The Usage of Keyfiles	171
6.3.6	Summary	172

7	Public Key Infrastructure	175
7.1	Public Key Infrastructure and Its Services	175
7.2	Modern Web Threats	175
7.3	Trusted Third Party, Certification Process	176
7.4	PKI	180
7.5	Certificates, Keys and Management	183
7.5.1	Generating and Installing the Certificates	183
7.5.2	Configuration of Certificate	184
7.5.3	Cancellation of Certificates	190
8	Cryptographic Protocols	193
8.1	Examples of Cryptographic Protocols	194
8.2	Reliability	195
8.2.1	The Needham-Schroeder Protocol	196
8.3	Needham-Schroeder Symmetric Key Protocol	199
8.4	Timestamps	201
8.5	Key Exchange Public-Key Protocol	202
8.6	Kerberos System	203
8.6.1	Description of Kerberos Components	204
8.6.2	Example of Application of Kerberos	206
8.7	Verification of Correctness of Cryptographic Protocols	207
8.7.1	Axiomatic (Deductive) Method	208
8.7.2	Model Checking	209
8.7.3	Inductive Method	209
8.7.4	Results	210
8.7.5	Summary	211
9	Cryptographic Applications for Network Security	213
9.1	Application of Cryptography to Internet Mail Systems Security	213
9.1.1	PEM	213
9.1.2	S/MIME	214
9.1.3	MOSS	216
9.2	Security of Document Interchange	216
9.2.1	EDI	217
9.2.2	OpenEDI	217
9.2.3	OBI	218
9.2.4	Swift, Edifact	218
9.2.5	EDI in Practice	219
9.3	Computer Network Security—SSH and SSL Protocols	220
9.3.1	Introduction	220
9.3.2	Idea of the SSH Protocol	221
9.3.3	Using the SSH Protocol	224
9.3.4	Construction of SSL Protocol	225
9.3.5	The Use of SSL in Practice	227
9.4	Wireless Network Security	229
9.4.1	WEP Protocol	229
9.4.2	WPA Protocol and Its Modifications	230
	References	233
	Index	237