

Contents

<i>Preface</i>	v
1. Introduction	1
Problems and Exercises	6
2. Public Key Cryptosystems	7
2.1 Prehistory and Main Ideas	7
2.2 The First Public Key System — Diffie–Hellman Key Agreement	12
2.3 The Elements of Number Theory	15
2.4 Shamir Cipher	22
2.5 ElGamal Encryption	24
2.6 RSA Encryption and Trapdoor Functions	27
Problems and Exercises	30
Themes for Labs	32
3. Solving Discrete Logarithm Problem	33
3.1 Problem Setting	33
3.2 The Baby-step Giant-step Algorithm	35
3.3 Index Calculus Algorithm	37
Problems and Exercises	42
Themes for Labs	42
4. Digital Signatures	43
4.1 RSA Digital Signature	43
4.2 ElGamal Digital Signature	46

4.3	Digital Signature Standards	49
	Problems and Exercises	52
	Themes for Labs	53
5.	Cryptographic Protocols	55
5.1	Mental Poker	55
5.2	Zero Knowledge Proofs	59
5.2.1	Graph Colouring Problem	60
5.2.2	Hamiltonian Cycle Problem	63
5.3	Digital Cash	70
5.4	Mutual Identification with Key Establishment	76
	Problems and Exercises	81
	Themes for Labs	82
6.	Elliptic Curve Cryptosystems	83
6.1	Introduction	83
6.2	Mathematical Foundations	84
6.3	Choosing Curve Parameters	91
6.4	Constructing Cryptosystems	93
6.4.1	Elliptic Curve ElGamal Encryption	94
6.4.2	Elliptic Curve Digital Signature Algorithm	95
6.5	Efficient Implementation of Operations	95
6.6	Counting Points on Elliptic Curve	102
6.7	Using Standard Curves	110
	Problems and Exercises	112
	Themes for Labs	113
7.	Theoretical Security of Cryptosystems	115
7.1	Introduction	115
7.2	Theory of Perfect Secrecy	116
7.3	Vernam Cipher	118
7.4	Elements of Information Theory	119
7.5	Unicity Distance for Secret Key Cipher	125
7.6	Ideal Cryptosystems	130
	Problems and Exercises	136
8.	Modern Secret Key Ciphers	137
8.1	Introduction	137

8.2	Block Ciphers	140
8.2.1	The GOST 28147-89 Block Cipher	141
8.2.2	The RC5 and RC6 Ciphers	144
8.2.3	The Rijndael (AES) Cipher	148
8.3	Main Modes of Operation of Block Ciphers	158
8.3.1	ECB Mode	159
8.3.2	CBC Mode	159
8.4	Stream Ciphers	160
8.4.1	The OFB Block Cipher Mode	162
8.4.2	The CTR Block Cipher Mode	163
8.4.3	The RC4 Algorithm	163
8.5	Cryptographic Hash Functions	165
9.	Random Numbers in Cryptography	169
9.1	Introduction	169
9.2	Refining Physical Random Number Generators	170
9.3	Pseudo-Random Number Generators	173
9.4	Statistical Tests for Random and Pseudo-Random Number Generators	175
9.5	Statistical Attack to Block Ciphers	178
	<i>Answers to Problems and Exercises</i>	185
	<i>Bibliography</i>	189
	<i>Author Index</i>	193
	<i>Subject Index</i>	195