

## Contents

Preface *xviii*

<b>1</b>	<b>Introduction to Computer Security</b>	<b>1</b>
1.1	Introduction	1
1.1.1	Why Do Attacks Occur?	1
1.1.2	Are Security Attacks Avoidable?	2
1.1.3	What Should Be Protected in Cyberspace?	2
1.1.4	Security vs Safety	3
1.1.5	Cybersecurity vs IT Security	3
1.2	Security Terms and Definitions	4
1.2.1	Assets and Attackers	4
1.2.2	Vulnerabilities, Threats, and Risks	5
1.3	Security Services	6
1.3.1	Confidentiality and Privacy	6
1.3.2	Integrity	6
1.3.3	Availability	7
1.3.4	Authentication and Authenticity	7
1.3.5	Non-repudiation and Accountability	8
1.3.6	Authorization	8
1.4	Attacks	8
1.4.1	Taxonomy of Attacks	8
1.4.1.1	Attacks According to Their Origin	9
1.4.1.2	Passive vs Active Attacks	9
1.4.1.3	Attacks According to Their Objectives	10
1.4.2	Taxonomy of Attackers	12
1.4.3	Malware Taxonomy	13
1.4.3.1	Virus	14
1.4.3.2	Worm	14
1.4.3.3	Trojan	14
1.4.3.4	Ransomware	14
1.4.3.5	Spyware and Adware	14
1.4.3.6	Botnet	15
1.4.3.7	Keylogger, Screen Scraper, and Web Shell	15
1.4.3.8	Exploit, Logic Bomb, Backdoor, and Rootkit	15
1.4.4	Daily Awareness to IT Security	15
1.5	Countermeasures/Defenses	16
1.5.1	Very Old Roots of Countermeasures	16
1.5.2	Methods for Defense	16

1.5.2.1	Prevention/Detection/Reaction Methods	16
1.5.2.2	Level of Automation of Defense Methods	17
1.5.2.3	Design Orientations of Defense Methods	17
1.5.3	Overview of Security Countermeasures	18
1.5.3.1	Organizational Measures	18
1.5.3.2	Technical Countermeasures	19
1.5.4	Security Penetration Testing Tools	19
1.6	Overview of Defense Systems	20
1.6.1	Firewalls	20
1.6.2	Proxy Overview	21
1.6.3	Intrusion Detection Systems	22
1.6.4	Intrusion Protection Systems	24
1.6.4.1	Performance Requirements Regarding IDSs and IPSs	24
1.6.5	Honeypots	24
1.6.6	Network Address Translation	25
1.6.7	Virtual Private Networks	25
1.6.8	Layered-Security Architecture	26
1.7	Introduction to Privacy Protection	26
1.7.1	Overview of Privacy Issues	26
1.7.2	Introduction to the GDPR Directive	27
1.7.2.1	Personal Data and Acts of Processing	28
1.7.2.2	Principles of Data Protection	28
1.8	Concluding Remarks	29
1.9	Exercises and Solutions	29
1.9.1	List of Exercises	29
1.9.2	Solutions to Exercises	30
	Notes	31
	References	31
<b>2</b>	<b>Introduction to Cryptography</b>	33
2.1	Definitions of Basic Terms	33
2.1.1	Cryptography, Cryptanalysis, and Cryptology	33
2.1.2	Brief History of Cryptography	34
2.1.3	Basic Terms Related to Encryption Systems	36
2.1.4	Symmetric and Asymmetric Cryptographic Systems	37
2.1.4.1	Symmetric Cryptosystems	37
2.1.4.2	Asymmetric Cryptosystems	37
2.1.4.3	Symmetric vs Asymmetric Cryptosystems and Their Combination	37
2.1.4.4	Trapdoor Functions	38
2.2	Cryptographic Primitives	39
2.2.1	Encryption	40
2.2.2	Hash Functions and Data Integrity	40
2.2.3	Message Authentication Codes	40
2.2.4	Digital Signature	41
2.2.5	Digital Certificates and Non-Repudiation	42
2.2.6	Shared-Secret Generation	42
2.2.7	Pseudorandom Number Generation	43
2.3	Fundamental Properties of Cryptographic Algorithms	43
2.3.1	Should Cryptographic Algorithms Be Secret or Not?	43
2.3.2	Models of Security Proof	43
2.3.2.1	Computational Infeasibility	43
2.3.2.2	Provable Security	43
2.3.3	Perfect Secrecy	44

2.3.4	Security Strength of Cryptographic Algorithms	45
2.4	Attacks Against Cryptographic Algorithms	45
2.4.1	What Is Cryptanalysis?	45
2.4.2	Categorization of Cryptanalysis Attacks	46
2.4.2.1	First Categorization of Cryptanalysis Attacks	46
2.4.2.2	Second Categorization of Cryptanalysis Attacks	47
2.4.3	Attacks on Implementations of Cryptographic Algorithms	49
2.4.3.1	Side-Channel Attacks	49
2.4.3.2	Fault-Injection Attacks	50
2.4.4	Practicality of Cryptanalysis Attacks	50
2.5	Steganography	51
2.5.1	Examples of Secret Hiding Without Using Computer	51
2.5.2	Examples of Secret Hiding Using Computer	51
2.6	Exercises and Problems	52
2.6.1	List of Exercises and Problems	52
2.6.2	Solutions to Exercises and Problems	53
	Notes	57
	References	57

### **3 Mathematical Basics and Computation Algorithms for Cryptography 59**

3.1	Number Theory Notations, Definitions, and Theorems	59
3.1.1	Basic Terms and Facts of Number Theory	60
3.1.2	Sets	61
3.1.3	Modulo Operator and Equivalence Class	61
3.1.4	Basic Properties of Modular Arithmetic	62
3.1.5	$\mathbb{Z}_n$ : Integers Modulo n	62
3.1.6	Multiplicative Inverse	62
3.1.7	Modular Square Roots	63
3.1.8	List of Exercises and Problems	65
3.2	Basic Algebraic Structures	66
3.2.1	Groups and Rings and Their Properties	66
3.2.2	Fields	69
3.2.3	Extension Fields $F_{p^n}$	71
3.2.4	Extension Fields	75
3.2.5	List of Exercises and Problems	79
3.3	Computation Algorithms	80
3.3.1	Euclidean and Extended Euclidean Algorithms	80
3.3.1.1	Euclidean Algorithm	80
3.3.1.2	Extended Euclidean Algorithm	80
3.3.1.3	Finding Multiplicative Inverse	81
3.3.2	Modular Exponentiation: Square-and-Multiply	81
3.3.3	Fast Modular Multiplication and Montgomery's Multiplication	82
3.3.3.1	Single-precision Montgomery Multiplication Algorithm	83
3.3.3.2	Multi-precision Montgomery Multiplication Algorithm	84
3.3.4	Chinese Remainder Theorem and Gauss's Algorithm	86
3.3.5	Finding Modular Square Roots	87
3.3.5.1	Tonelli-Shanks Algorithm for Finding Modular Square Roots of Primes	87
3.3.5.2	Finding Square Roots of Multiple Primes	88
3.3.6	Test of Irreducibility	89
3.3.6.1	Naïve Approach	89
3.3.6.2	Efficient Approach (Rabin's Test of Irreducibility)	90
3.3.7	List of Exercises and Problems	91

3.4	Birthday Paradox and Its Generalization	92
3.5	Solutions to Exercises and Problems	93
	Notes	115
	References	116
<b>4</b>	<b>Symmetric Ciphering: Historical Ciphers</b>	<b>117</b>
4.1	Definitions	117
4.2	Caesar's Cipher	117
4.3	Affine Ciphers	118
4.4	Vigenere's Cipher	120
4.5	Enigma Machine	122
4.5.1	Principle of Secure Communication Using Enigma	123
4.5.2	Rotors and Reflector	123
4.5.3	Plug Board	124
4.5.4	Machine Setting	124
4.5.5	Encryption and Decryption Procedures	124
4.5.6	Enigma Decryption Correctness	126
4.5.7	Complexity Analysis	128
4.5.8	Breaking Enigma Code	129
4.5.8.1	Weaknesses, Practices, and Other Features that had been Exploited	129
4.5.8.2	Crib-based Attack	130
4.5.8.3	Improvement of Settings Identification Process	132
4.6	One-time Pad	133
4.7	Exercises and Problems	133
4.7.1	List of Exercises and Problems	133
4.7.2	Solutions to Exercises and Problems	135
	Notes	141
	References	141
<b>5</b>	<b>Hash Functions, Message Authentication Codes, and Digital Signature</b>	<b>142</b>
5.1	Hash Functions	142
5.1.1	Properties of Hash Functions	142
5.1.2	Generic Attacks Against Hash Functions	143
5.1.3	Overall Operation Principle of Hashing Algorithms	144
5.1.3.1	Merkle-Damgård Construction	145
5.1.3.2	Vulnerability to Length Extension Attack	145
5.2	Secure Hash Algorithms (SHA)	146
5.2.1	SHA-1 and SHA-2 Algorithms	146
5.2.1.1	SHA-1 Algorithm	147
5.2.1.2	SHA-256 Algorithm	148
5.2.1.3	SHA-224 Algorithm	150
5.2.1.4	SHA-512 Algorithm	150
5.2.1.5	SHA-384, SHA-512/224, and SHA-512/256 Algorithms	151
5.2.1.6	SHA-1 Security	152
5.2.2	SHA-3 Functions	152
5.2.2.1	Keccak-p Permutation	152
5.2.2.2	Sponge Construction	155
5.2.2.3	SHA-3 Functions	157
5.3	Message Authentication Codes	157
5.3.1	Objectives and Properties of MACs	157
5.3.2	Hash Function-based MACs	158
5.3.2.1	HMAC	158

5.3.2.2	KMAC	160
5.3.2.3	Generic Attacks Against Hash Function-based MAC Algorithms	161
5.3.3	Block Cipher-based MACs	161
5.4	Digital Signature	161
5.4.1	Digital Signature in Public Key World	161
5.4.2	Attacks Against Digital Signature Schemes	162
5.5	Concluding Remarks	163
5.6	Problems	163
5.6.1	List of Problems	163
5.6.2	Solutions to Problems	165
	Notes	171
	References	171

## **6 Stream Ciphers** 173

6.1	Stream Ciphers	173
6.1.1	Principles of Stream Ciphers	173
6.1.2	Synchronous vs Self-synchronized Keystream Generators	174
6.1.2.1	Synchronous Stream Ciphers	175
6.1.2.2	Self-synchronized Stream Ciphers	175
6.1.3	How to Generate Random Keystream Bits?	177
6.1.4	Linear-Feedback Shift Registers (LFSRs)	177
6.1.4.1	LFSR Principle and Properties	177
6.1.4.2	Feedback Polynomial of LFSRs	180
6.1.5	LFSRs for Building Stream Ciphers	181
6.2	Examples of Standard Keystream Generators	182
6.2.1	A5/1 Keystream Generator	183
6.2.2	E0 Keystream Generator	183
6.2.3	SNOW 3G Keystream Generator	184
6.2.3.1	Formal Description of SNOW 3G	184
6.2.3.2	Algorithmic Description of SNOW 3G	186
6.2.4	ZUC Keystream Generator	188
6.2.4.1	Principle of ZUC Keystream Generator	188
6.2.4.2	ZUC Algorithm	188
6.2.5	ChaCha20 Stream Cipher	191
6.2.5.1	ChaCha20 State	191
6.2.5.2	ChaCha20 Quarter Round	191
6.2.5.3	ChaCha20 Keystream Block Generation	191
6.2.5.4	Plaintext Encryption and Decryption Using ChaCha20	192
6.2.6	RC4 Stream Cipher	193
6.2.6.1	RC4 Key-scheduling Algorithm	193
6.2.6.2	Keystream Generation Phase	193
6.2.7	Lightweight Cryptography Stream Ciphers	194
6.2.7.1	Trivium Stream Cipher	194
6.2.7.2	Enocoro Stream Cipher	195
6.3	Exercises and Problems	197
6.3.1	List of Exercises and Problem	197
6.3.2	Solutions to Exercises and Problems	199
	Notes	205
	References	206

<b>7</b>	<b>Block Ciphers: Basics, TDEA, and AES</b>	207
7.1	Construction Principles for Block Cipher Design	207
7.1.1	Confusion and Diffusion Properties	208
7.1.1.1	Substitution Boxes	208
7.1.1.2	Permutation	208
7.1.1.3	Key Expansion	208
7.1.2	Feistel Structure	209
7.2	Triple Data Encryption Algorithm (TDEA)	211
7.2.1	Data Encryption Algorithm (DEA)	211
7.2.1.1	DEA Encryption and Decryption	211
7.2.1.2	Initial Permutation and Its Inverse	213
7.2.1.3	Function $f$	213
7.2.2	TDEA Construction and Usage	216
7.2.2.1	Bundle and DEA Keys	216
7.2.2.2	TDEA Encryption and Decryption	217
7.2.2.3	Key Schedule Function KS	218
7.2.3	Security Issues	220
7.2.3.1	Complexity of Attacks Against DES	220
7.2.3.2	TDEA Security Limit	220
7.2.3.3	Meet-in-the-Middle Attack Against Double DES and TDEA	220
7.3	Advanced Encryption System (AES)	222
7.3.1	Distinctive Features of AES	222
7.3.2	Data Representation in AES	222
7.3.3	Overall Structure of AES	223
7.3.4	AES Transformation Description	224
7.3.4.1	SubBytes and InvSubBytes Transformations	224
7.3.4.2	ShiftRows and InvShiftRows Transformations	226
7.3.4.3	MixColumns and InvMixColumns Transformations	227
7.3.4.4	AddRoundKey Transformation	227
7.3.5	Key Expansion	227
7.3.6	Mathematical Description of AES	229
7.3.6.1	Data Representation and Operations on Data	229
7.3.6.2	SubBytes and InvSubBytes Transformations	232
7.3.6.3	ShiftRows and InvShiftRows Transformations	233
7.3.6.4	MixColumns and InvMixColumns Transformations	233
7.3.6.5	AddRoundKey Transformation	234
7.3.7	Security of AES	234
7.4	Exercises and Problems	235
7.4.1	List of Exercises and Problems	235
7.4.2	Solutions to Exercises and Problems	236
	Notes	245
	References	246
<b>8</b>	<b>Block Cipher Modes of Operation for Confidentiality</b>	247
8.1	Introduction	247
8.1.1	Definitions	247
8.1.2	Overview of Standard Modes of Operation	248
8.1.3	Notations and Common Basic Functions	248
8.1.4	Common Aspects of Modes for Confidentiality	249
8.1.4.1	Plaintext Length and Padding	249
8.1.4.2	Initialization Vector	249
8.2	ECB Mode of Operation	249
8.3	CBC Modes of Operation	250

8.3.1	Basic CBC Mode	250
8.3.2	CBC Variants (CS1, CS2, CS3)	251
8.3.2.1	CBC-CS1 Mode	251
8.3.2.2	CBC-CS2 and CBC-CS3 Modes	252
8.4	OFB Mode of Operation	253
8.5	CTR Mode of Operation	253
8.6	CFB Mode of Operation	255
8.7	Format-Preserving Encryption Modes of Operation	256
8.7.1	Common Aspects to FPE Modes	256
8.7.2	Encryption and Decryption in FF1 and FF3-1 Modes	258
8.7.3	FF1 Mode	259
8.7.4	FF3-1 Mode	262
8.8	XTS-AES Mode of Operation	264
8.8.1	Overview of XTS-AES	264
8.8.2	Encryption and Decryption Algorithms	265
8.8.3	Some Strengths and Weaknesses of XTS-AES	268
8.9	Comparison of Design Features of Modes for Confidentiality	269
8.10	Security of Modes of Operation for Confidentiality	269
8.10.1	Vulnerability to Block Repetitions and Replay	270
8.10.2	Vulnerability to Predictable IV or Tweak	271
8.10.3	Vulnerability to IV/Tweak that Is Not a Nonce	271
8.10.4	Vulnerability to Birthday Attacks	272
8.10.5	Vulnerability to Bit-Flipping Attacks	272
8.11	Exercises and Problems	273
8.11.1	List of Exercises and Problems	273
8.11.2	Solutions to Exercises and Problems	274
	Notes	279
	References	280
<b>9</b>	<b>Block Cipher Modes of Operation for Authentication and Confidentiality</b>	<b>281</b>
9.1	Introduction	281
9.2	Block Cipher Modes of Operation for Confidentiality and Authentication	282
9.2.1	Authenticated Encryption and AEAD Algorithms	282
9.2.1.1	Approaches to Data Authentication	282
9.2.1.2	Authenticated Encryption with Associated Data Algorithms	283
9.2.1.3	Limits of Authenticated-Decryption Modes	283
9.2.2	CMAC Mode of Operation	284
9.2.3	CCM Mode of Operation	285
9.2.3.1	MAC Generation and Encryption	285
9.2.3.2	MAC Verification and Decryption	287
9.2.3.3	Information Formatting Function	287
9.2.3.4	Counter Formatting Function	288
9.2.4	GCM and GMAC Modes of Operation	289
9.2.4.1	GCTR Encryption Mode	289
9.2.4.2	Hash Function of GCM	290
9.2.4.3	Authenticated Encryption with GCM	290
9.2.4.4	Authenticated Decryption with GCM	291
9.2.4.5	GMAC Mode	292
9.2.4.6	Forbidden Attack Against GCM with Repeated IV	293
9.2.5	AES-GCM-SIV Mode	294
9.2.5.1	What Does Nonce Misuse-resistance Mean?	294
9.2.5.2	Overview of AES-GCM-SIV Mode	294

9.2.5.3	Key Derivation and Hash Functions	295
9.2.5.4	Authenticated Encryption with AES-GCM-SIV	295
9.2.5.5	Authenticated Decryption with AES-GCM-SIV	297
9.2.6	Poly1305	298
9.2.6.1	Poly1305-AES	298
9.2.6.2	ChaCha20-Poly1305 AEAD	299
9.2.7	Key Wrapping Modes	300
9.2.7.1	KW and KWP Modes of Operation	301
9.2.7.2	TKW Mode of Operation	305
9.2.7.3	Security of Key Wrapping Modes	305
9.2.8	Security of Authenticated-Encryption Modes	305
9.2.8.1	Block Repetitions and Replay	305
9.2.8.2	Chosen-Ciphertext Attacks	306
9.2.8.3	Birthday Attacks	306
9.2.8.4	Bit-flipping Attacks	306
9.2.8.5	Nonce Misuse	306
9.3	Exercises and Problems	306
9.3.1	List of Exercises and Problems	306
9.3.2	Solutions to Exercises and Problems	308
	Notes	312
	References	313
<b>10</b>	<b>Introduction to Security Analysis of Block Ciphers</b>	<b>314</b>
10.1	Pseudorandom Functions and Permutations	314
10.1.1	Definitions of Random and Pseudorandom Functions and Permutations	315
10.1.2	Indistinguishability and Security of PRFs	316
10.1.2.1	Indistinguishability and Security of PRPs	317
10.1.2.2	PRF/PRP Switching Lemma	319
10.2	Security of TDEA and AES	320
10.2.1	Security Against Key Recovery Attack	321
10.2.2	Birthday Attack Against Block Ciphers	322
10.3	Security Analysis Modes of Operation of BC for Confidentiality	322
10.3.1	Left-or-Right Indistinguishability	323
10.3.2	Some Bounds of Security of Block Cipher Modes of Operation	324
10.4	Security Analysis of Authenticity-only Schemes	326
10.4.1	Generic Models for Security Analysis of Authenticity Schemes	326
10.4.1.1	Game for Tag Forgery Analysis	326
10.4.1.2	Game for MAC Indistinguishability	327
10.4.2	Some Security Bounds for MAC Schemes	328
10.4.2.1	Security Bounds for CMAC	328
10.4.2.2	Security Bounds for HMAC	328
10.5	Generic Models for Security Analysis of Authenticated-Encryption Modes	329
10.5.1	Generic Modeling of Security of AEAD Modes	329
10.5.2	Some Security Bounds for CCM, GCM, and AES-GCM-SIV	330
10.5.2.1	Bounds for CCM	330
10.5.2.2	Bounds for GCM	330
10.5.2.3	Some Bounds for AES-GCM-SIV Security	331
10.6	Problems and Solutions	332
10.6.1	List of Problems	332
10.6.2	Solutions to Problems	333
	Notes	336
	References	336

**11 Introduction to Cryptanalysis Attacks on Symmetric Ciphers 338**

- 11.1 Memory-Time Trade-off Attacks 339
  - 11.1.1 Hellman's Table-based Attacks 339
  - 11.1.2 Offline Precomputation 339
  - 11.1.3 Key Search 340
  - 11.1.4 Rainbow Chains 343
- 11.2 Linear Cryptanalysis 347
  - 11.2.1 Bias and Piling-up Lemma 348
  - 11.2.2 Constructing Linear Approximation Expressions 349
    - 11.2.2.1 Finding Linear Approximations Associated with an s-box 349
    - 11.2.2.2 Measuring Quality of Linear Approximations 351
    - 11.2.2.3 Finding Linear Expressions Associated with an s-box and a Key 352
    - 11.2.2.4 Finding Linear Expressions Associated with Two s-boxes and a Key 352
    - 11.2.2.5 Finding Linear Expressions Associated with a Full Cipher 353
  - 11.2.3 General Methodology for Performing Linear Cryptanalysis 356
  - 11.2.3.1 Algorithm 1: Deduction of a Bit-information about Cipher Key 356
  - 11.2.3.2 Algorithm 2: Recovery of the Last-round Key 359
- 11.3 Differential Cryptanalysis 360
  - 11.3.1 Difference Distribution Table 361
    - 11.3.1.1 Difference Distribution Table: Construction and Properties 361
    - 11.3.1.2 Difference-Propagation Probability 363
    - 11.3.1.3 Effect of Round Key Addition 363
  - 11.3.2 Differential Attack Design 363
    - 11.3.2.1 First step: Selection of an Overall Difference-Propagation Probability 363
    - 11.3.2.2 Second Step: Selection of Chosen Plaintexts 366
    - 11.3.2.3 Third Step: Recovery of some Bits of the Last-round Key 366
- 11.4 Algebraic Cryptanalysis 366
- 11.5 Cube Attack 368
  - 11.5.1 Main Idea of Cube Attack 368
  - 11.5.2 Polynomial Representation 368
  - 11.5.3 Cube Attack Mounting 369
    - 11.5.3.1 Preprocessing Phase 369
    - 11.5.3.2 Key Recovery Phase 370
  - 11.6 Other Attacks Against Stream Ciphers 372
    - 11.6.1 Divide-and-Conquer Attack 372
    - 11.6.2 Correlation Attack 373
  - 11.7 Problems and Solutions 374
    - 11.7.1 List of Problems 374
    - 11.7.2 Solutions to Problems 375
      - Notes 379
      - References 380

**12 Public-Key Cryptosystems 381**

- 12.1 Introduction to Public-Key Cryptosystems 381
- 12.1.1 Attacks Against Public-Key Cryptosystems 382
  - 12.1.1.1 Attacks Against Encryption Schemes 383
  - 12.1.1.2 Attacks Against Digital Signature Schemes 383
- 12.2 RSA Cryptosystem 383
  - 12.2.1 RSA Encryption and Decryption 384
  - 12.2.2 Implementation Issues 385
    - 12.2.2.1 Fast Modular Exponentiation Methods 385
    - 12.2.2.2 Chinese Remainder Theorem-based RSA Decryption 385

12.2.2.3	Why $e = 65537$ Is Often Used in RSA Cryptosystems?	387
12.2.3	Proof of Correctness of RSA	387
12.2.4	RSA Security	388
12.2.5	Optimal Asymmetric Encryption Padding (OAEP)	389
12.2.6	RSA Signature	391
12.2.6.1	RSA Signature Generation	392
12.2.6.2	RSA Signature Verification	392
12.2.6.3	Probabilistic Signature Scheme (PSS)	392
12.3	Finite Field-based Cryptography	394
12.3.1	Discrete Logarithm Problem	394
12.3.1.1	What Is the Discrete Logarithm Problem?	394
12.3.1.2	Attacks Against DLP	394
12.3.2	Diffie-Hellman Key Exchange	395
12.3.3	Menezes-Qu-Vanstone Key-exchange Protocol	396
12.3.4	ElGamal Cryptosystem	396
12.3.4.1	ElGamal Encryption	396
12.3.4.2	ElGamal Signature	398
12.3.4.3	ElGamal Digital Signature Security and Potential Attacks	399
12.4	Digital Signature Algorithm (DSA)	400
12.4.1	DSA Domain Parameters	400
12.4.2	DSA-Keys Generation	400
12.4.3	DSA Signature Generation	400
12.4.4	DSA Signature Verification	400
12.4.5	Advantages of DSA over ElGamal Signature Scheme	401
12.5	Exercises and Problems	401
12.5.1	List of Exercises and Problems	401
12.5.2	Solutions to Exercises and Problems	405
	Notes	422
	References	423
<b>13</b>	<b>Public-Key Cryptosystems: Elliptic Curve Cryptography</b>	424
13.1	Introduction	424
13.1.1	What Is Elliptic Curve Cryptography?	424
13.1.2	What Is an Elliptic Curve?	425
13.1.3	Order and Point Set of an Elliptic Curve	426
13.2	Elliptic Curve Cryptography over Prime Field $F_p$	426
13.2.1	Definition of Elliptic Curves over Prime Fields: $E(F_p)$	426
13.2.2	Operations on Elliptic Curves	427
13.2.3	Generator and Cofactor of EC	429
13.2.4	Montgomery and Edwards Curves	430
13.2.4.1	Operations on Edwards EC Points	431
13.2.4.2	Operations on Montgomery EC Points	431
13.3	Elliptic Curve Cryptography over Extension Fields	431
13.3.1	Definition of EC over Extension Fields	432
13.3.1.1	Operations on Points of Curve $E(F_{2^m})$	433
13.3.1.2	Fast Scalar Multiplication	434
13.3.2	Set and Number of Points of an EC	435
13.3.2.1	Finding the Set of Points on an EC	435
13.3.2.2	Finding the Exact Number of Points on an EC	435
13.4	Security of EC Cryptosystems	436
13.5	Elliptic Curve-based Algorithms	437
13.5.1	Security Strength Levels of EC Algorithms	437
13.5.2	Domain Parameters	437

13.5.3	EC Diffie–Hellman (ECDH) Key-Agreement Protocol	437
13.5.3.1	Small-Subgroup Attack Against ECDH	439
13.5.4	EC Menezes–Qu–Vanstone (ECMQV) Key-Agreement Protocol	440
13.5.5	Elliptic-Curve Digital-Signature Algorithm (ECDSA)	441
13.5.5.1	Setup Process	441
13.5.5.2	ECDSA Signature Generation	441
13.5.5.3	ECDSA Signature Verification	441
13.5.5.4	Correctness of ECDSA Algorithm	442
13.5.6	Edwards Curve Digital Signature Algorithm (EdDSA)	443
13.5.6.1	EdDSA Key Pair Generation	443
13.5.6.2	EdDSA Signature Generation	444
13.5.6.3	EdDSA Signature Verification	444
13.5.6.4	Comment on EdDSA Signature Verification Procedure	445
13.5.7	Elliptic Curve Encryption Algorithms	446
13.5.7.1	ECIES Framework	446
13.5.7.2	ElGamal Encryption Using EC Cryptography	448
13.6	Exercises and Problems	451
13.6.1	List of Exercises and Problems	451
13.6.2	Solutions to Exercises and Problems	453
	Notes	463
	References	463

<b>14</b>	<b>Key Management</b>	465
14.1	Key-Management-related Notions	465
14.1.1	Types, Security Strengths, and Cryptoperiod of Keys	465
14.1.1.1	Key Types	465
14.1.1.2	Security Strengths	466
14.1.1.3	Cryptoperiod	467
14.1.2	Key-Management Phases and Functions	468
14.2	Key-Generation Schemes	469
14.2.1	Key Generation for Symmetric-Key Systems	469
14.2.1.1	Key Generation Using DRBGs	470
14.2.1.2	Key Derived from a Password	470
14.2.1.3	Key-Generation by Key-Derivation Methods	471
14.2.1.4	Key Generated by Combining Multiple Other Keys and Data	474
14.2.1.5	Key-Derivation Functions	474
14.2.2	Key Generation for Asymmetric-Key Cryptosystems	476
14.2.2.1	RSA Key-Pair Generation	477
14.2.2.2	Key-Pair Generation for DH and MQV	478
14.2.2.3	ECC Key-Pair Generation	480
14.3	Key-Establishment Schemes	482
14.3.1	Overall View of Key-Establishment Schemes	482
14.3.2	Key-Establishment Using a Key Distribution Center	484
14.3.3	Key-Establishment Using Public-Key-based Schemes	486
14.3.3.1	Common Mechanisms and Functions	486
14.3.3.2	Key-Establishment Schemes Using RSA	487
14.3.3.3	DLC-based Key-Agreement Schemes	492
14.4.1	List of Problems	501
14.4.2	Solutions to Problems	503
	Notes	506
	References	507

<b>15</b>	<b>Digital Certificate, Public-Key Infrastructure, TLS, and Kerberos</b>	<b>509</b>
15.1	Digital Certificate: Notion and X.509 Format	509
15.1.1	Types of Digital Certificates	510
15.1.1.1	TLS (Transport Layer Security) Certificates	510
15.1.1.2	Code (or Software) Signing Certificates	510
15.1.1.3	Client Certificates	510
15.1.2	X.509 Standard Format	510
15.2	Public-Key Infrastructure	511
15.2.1	Components of a PKI	512
15.2.2	Certificate Authority Hierarchy	512
15.2.3	Registration of a Public-Key and Certificate Acquisition	514
15.2.4	Chain of Trust and Trust Models	515
15.2.5	Validation of Certificates and Trust Paths	516
15.2.6	Digital-Certificate Revocation	516
15.3	Transport Layer Security (TLS 1.3)	517
15.3.1	TLS Certificates	517
15.3.2	TLS 1.3 Protocols	518
15.3.2.1	Handshake Protocol	518
15.3.2.2	Record Protocol	520
15.3.2.3	Alert Protocol	520
15.4	Kerberos	521
15.4.1	Kerberos Principles	521
15.4.2	Message Formats and Authentication Steps of Kerberos	523
15.4.2.1	Ticket and Authenticator Formats	523
15.4.2.2	Protocol Actions and Message Description	523
15.4.3	Advantages, Limits, and Security of Kerberos	526
15.5	Exercises and Problems	527
15.5.1	List of Exercises and Problems	527
15.5.2	Solutions to Exercises and Problems	528
	Notes	529
	References	530
<b>16</b>	<b>Generation of Pseudorandom and Prime Numbers for Cryptographic Applications</b>	<b>531</b>
16.1	Introduction to Pseudorandom Number Generation	531
16.1.1	Basic Notions and Definitions	531
16.1.2	Entropy	532
16.1.2.1	Source of Entropy	532
16.1.2.2	Entropy from a Statistical Point of View	533
16.1.3	Some Popular PRNGs (not to use in Cryptography)	535
16.1.3.1	Middle-Square Algorithm	535
16.1.3.2	Linear Congruential Generator	536
16.1.3.3	Mersenne Twister PRNG	536
16.1.4	PRNGs for Cryptography: Notions and Design Principles	536
16.1.4.1	Properties of PRNGs for Cryptography	536
16.1.4.2	General Guidelines for the Design of PRBGs for Cryptography	537
16.2	Pseudorandom Bit Generators Recommended for Cryptography	541
16.2.1	Common Mechanisms and Processes	541
16.2.1.1	Security Strength	541
16.2.1.2	Instantiating a DRBG	541
16.2.1.3	Reseeding a DRBG	541
16.2.1.4	Internal State of a DRBG	542

16.2.1.5	Description Format of DRBG Functions	542
16.2.2	Hash-based DRBGs	542
16.2.3	HMAC-based DRBGs	544
16.2.4	Block Cipher-based DRBGs	546
16.3	Prime Number Generation	549
16.3.1	Basics and Facts about Primes	550
16.3.1.1	Definition of Some Prime Categories of Interest for Cryptography	550
16.3.1.2	Distribution of Prime Numbers	550
16.3.2	Methods for Primality Testing	551
16.3.2.1	Deterministic Methods for Primality Testing	551
16.3.2.2	Probabilistic Methods for Primality Testing	552
16.3.3	Generation of Probably-Prime Pair	554
16.3.3.1	Generation of Probably-Prime Pair for DH and MQV	555
16.3.3.2	Generation of Probably-Prime Pair for RSA	555
16.3.4	Generation of Provable Primes	556
16.3.4.1	Shawe-Taylor Algorithm	556
16.3.4.2	Generation of Provable-Prime Pair for DH and MQV	558
16.3.4.3	Generation of Provable-Prime Pair for RSA	559
16.4	Exercises and Problems	561
16.4.1	List of Exercises and Problems	561
16.4.2	Solutions to Exercises and Problems	562
	Notes	565
	References	565

**Appendix: Multiple Choice Questions and Answers** 566

**Index** 580