
Contents

Preface	ix
CHAPTER 1 ■ Symmetric Cryptography	1
1.1 DEFINITIONS	2
1.2 CONFIDENTIALITY AGAINST EAVESDROPPERS	2
1.3 INTEGRITY	19
1.4 CONFIDENTIALITY AND INTEGRITY	22
1.5 THE KEY DISTRIBUTION PROBLEM	23
CHAPTER 2 ■ Key Exchange and Diffie-Hellman	25
2.1 THE DIFFIE-HELLMAN PROTOCOL	26
2.2 DISCRETE LOGARITHMS	29
2.3 PRIMALITY TESTING	44
2.4 FINITE FIELDS	49
2.5 ELLIPTIC CURVES	58
2.6 ACTIVE ATTACKS	71
CHAPTER 3 ■ Public Key Encryption	73
3.1 DEFINITIONS	74
3.2 SCHEMES BASED ON DIFFIE-HELLMAN	75
3.3 RSA	79
3.4 FACTORING INTEGERS	87
3.5 LATTICES	96
3.6 LATTICE-BASED CRYPTOSYSTEMS	104
3.7 LATTICE ALGORITHMS	109
3.8 THE PUBLIC KEY INFRASTRUCTURE PROBLEM	115

CHAPTER 4 ■ Digital Signatures	117
4.1 DEFINITIONS	118
4.2 HASH FUNCTIONS	118
4.3 RSA SIGNATURES	123
4.4 SCHNORR SIGNATURES	126
4.5 HASH-BASED SIGNATURES	130
4.6 SECURING DIFFIE-HELLMAN	134
4.7 THE PUBLIC KEY INFRASTRUCTURE PROBLEM	135
CHAPTER 5 ■ Factoring Using Quantum Computers	137
5.1 BACKGROUND	137
5.2 QUANTUM COMPUTATION	142
5.3 FACTORING USING A QUANTUM COMPUTER	145
CHAPTER 6 ■ Computational Problems	147
6.1 DEFINITIONS	147
6.2 STATISTICAL DISTANCE	151
6.3 DIFFIE-HELLMAN	153
6.4 RSA	154
6.5 LATTICE PROBLEMS	155
CHAPTER 7 ■ Symmetric Cryptography	159
7.1 DEFINING SECURITY	160
7.2 CONFIDENTIALITY AND UNDERLYING PRIMITIVES	187
7.3 MESSAGE AUTHENTICATION CODES	194
7.4 CHANNELS	201
7.5 HASH FUNCTIONS	206
7.6 IDEAL MODELS	209

CHAPTER 8 ■ Public Key Encryption 213

8.1	DEFINING SECURITY	213
8.2	KEY ENCAPSULATION MECHANISMS	235
8.3	HOMOMORPHIC ENCRYPTION	251
8.4	COMMITMENT SCHEMES	259
8.5	CRYPTOGRAPHIC VOTING	265

CHAPTER 9 ■ Digital Signatures 277

9.1	DEFINING SECURITY	277
9.2	HASH AND SIGN PARADIGM	292
9.3	IDENTIFICATION SCHEMES	310
9.4	MESSAGING	328

CHAPTER 10 ■ Key Exchange 331

10.1	KEY EXCHANGE PROTOCOLS	331
10.2	DEFINING SECURITY	337
10.3	KEY EXCHANGE FROM KEY ENCAPSULATION	367
10.4	SINGLE-MESSAGE KEY EXCHANGE	372
10.5	SINGLE-SIDED AUTHENTICATION	373
10.6	CONTINUOUS KEY EXCHANGE	375

CHAPTER 11 ■ Arguments 379

11.1	ARGUMENTS	380
11.2	NON-INTERACTIVE ARGUMENTS	398
11.3	USING HVZK	402
11.4	FURTHER USEFUL ARGUMENTS	409

CHAPTER 12 ■ Multi-party Computation 429

12.1	SECRET SHARING	430
12.2	MULTI-PARTY COMPUTATION	444
12.3	DISTRIBUTED DECRYPTION	453

CHAPTER 13 ■ Messaging Protocols	459
13.1 MESSAGING PROTOCOLS	460
13.2 DEFINING SECURITY	467
13.3 INVASIVE ADVERSARIES	482
13.4 SOMEWHAT ANONYMOUS MESSAGING	486
CHAPTER 14 ■ Cryptographic Voting	489
14.1 DEFINITIONS	490
14.2 HOW TO USE A VOTING SCHEME	502
14.3 CAST AS INTENDED	509
14.4 COERCION RESISTANCE	514
Index	525