
CONTENTS

LIST OF FIGURES	xviii
-----------------	-------

LIST OF TABLES	xxii
----------------	------

PREFACE	xxiii
---------	-------

I INTRODUCTION	1
----------------	---

1 BEGINNING WITH A SIMPLE COMMUNICATION GAME...	3
---	---

1.1 A Communication Game	4
--------------------------	---

1.1.1 Our First Application of Cryptography	4
---	---

1.1.2 An Initial Hint on the Foundation of Cryptography	6
---	---

1.1.3 Security: More Than a Bless from Mathematical Properties	6
--	---

1.1.4 Modern Role of Cryptography: Ensuring Fair Play of Games	7
--	---

1.2 Criteria for Desirable Cryptographic Systems/Protocols	8
--	---

1.2.1 Stringency of Protection Tuned to Application Needs	9
---	---

1.2.2 Confidence in Security Based on Established “Pedigree”	10
--	----

1.2.3 Efficiency	11
------------------	----

1.2.4 Use of Practical and Available Primitives and Services	12
--	----

1.2.5 Explicitness	14
--------------------	----

1.2.6 Openness	17
----------------	----

1.3 Chapter Summary	18
---------------------	----

2	WRESTLING BETWEEN SAFEGUARD AND ATTACK	20
2.1	Encryption	21
2.2	Vulnerable Environment (the Dolev-Yao Threat Model)	23
2.3	Authentication Servers	24
2.4	Security Properties for Authenticated Key Establishment	26
2.5	Protocols for Authenticated Key Establishment Using Encryption	27
2.5.1	Protocols Serving Message Confidentiality	27
2.5.2	Attack, Fix, Attack, Fix, ...	29
2.5.3	Protocol With Message Authentication	34
2.5.4	Protocol With Challenge-Response	38
2.5.5	Protocol With Entity Authentication	40
2.5.6	Protocol Using Public-key Cryptosystems	42
2.6	Chapter Summary	48
II	MATHEMATICAL FOUNDATIONS	49
	STANDARD NOTATION	51
3	PROBABILITY	53
3.1	Basic Concept of Probability	54
3.2	Properties	55
3.3	Basic Calculation	55
3.3.1	Addition Rules	55
3.3.2	Multiplication Rules	56
3.3.3	The Law of Total Probability	57
3.4	Random Variables and Their Probability Distributions	58
3.4.1	Uniform Distribution	59
3.4.2	Binomial Distribution	60
3.5	The Birthday Paradox	61
3.6	Information Theory	63
3.6.1	Properties of Entropy	64
3.7	Redundancy in Natural Languages	65
3.8	Chapter Summary	66

4	COMPUTATIONAL COMPLEXITY	68
4.1	Introduction	68
4.2	Turing Machines	69
4.3	Polynomial-Time	71
4.4	Polynomial-Time Computational Problems	73
4.5	Algorithms and Computational Complexity Expressions	75
4.5.1	Greatest Common Divisor	76
4.5.2	Extended Euclid's Algorithm	77
4.5.3	Time Complexity of Euclid's Algorithms	78
4.5.4	Two Expressions for Computational Complexity	80
4.5.5	Modular Arithmetic	81
4.5.6	Modular Exponentiation	84
4.6	Probabilistic Polynomial-Time	86
4.6.1	Subclass "Always Fast and Always Correct"	88
4.6.2	Subclass "Always Fast and Probably Correct"	90
4.6.3	Subclass "Probably Fast and Always Correct"	92
4.6.4	Subclass "Probably Fast and Probably Correct"	95
4.7	Efficient Algorithms	99
4.8	Nondeterministic Polynomial-Time	101
4.8.1	Nondeterministic Polynomial-time Complete	105
4.9	Non-Polynomial Bounds	106
4.10	Polynomial-time Indistinguishability	108
4.11	Theory of Computational Complexity and Modern Cryptography	110
4.11.1	A Necessary Condition	111
4.11.2	Not a Sufficient Condition	112
4.12	Chapter Summary	113
5	ALGEBRAIC FOUNDATIONS	115
5.1	Groups	115
5.1.1	Lagrange's Theorem	118
5.1.2	Order of Group Element	120
5.1.3	Cyclic Groups	121
5.1.4	The Multiplicative Group \mathbb{Z}_N^*	124

5.2	Rings and Fields	125
5.3	Structure of Finite Fields	128
5.3.1	Finite Fields of Prime Numbers of Elements	128
5.3.2	Finite Fields Modulo Irreducible Polynomials	130
5.3.3	Finite Fields Constructed Using Polynomial Basis	135
5.3.4	Primitive Roots	139
5.3.5	Field Construction Using Normal Basis	140
5.4	Chapter Summary	144
6	NUMBER THEORY	145
6.1	Congruences and Residue Classes	145
6.1.1	Congruent Properties for Arithmetic in \mathbb{Z}_n	147
6.1.2	Solving Linear Congruence in \mathbb{Z}_n	147
6.1.3	The Chinese Remainder Theorem	149
6.2	The Euler's Phi Function	154
6.3	The Theorems of Fermat, Euler and Lagrange	155
6.4	Quadratic Residues	156
6.4.1	Quadratic Residuosity	157
6.4.2	Legendre-Jacobi Symbols	159
6.5	Computing Square Roots Modulo an Integer	162
6.6	Blum Integers	168
6.7	Chapter Summary	170
III	BASIC CRYPTOGRAPHIC TECHNIQUES	171
7	ENCRYPTION — SYMMETRIC TECHNIQUES	173
7.1	Introduction	173
7.1.1	Chapter Outline	175
7.2	Substitution Ciphers	176
7.2.1	Simple Substitution Ciphers	176
7.2.2	Polyalphabetic Ciphers	178
7.3	The Vernam Cipher and the One-Time Pad	179
7.4	Classical Ciphers: Usefulness and Security	180

7.5	The Data Encryption Standard (DES)	183
7.5.1	A Description of the DES	184
7.5.2	The Kernel Functionality of the DES: Random and Non-linear Distribution of Message	186
7.5.3	The Security of the DES	187
7.6	The Advanced Encryption Standard (AES)	188
7.6.1	An Overview of the Rijndael Cipher	189
7.6.2	The Internal Functions of the Rijndael Cipher	190
7.6.3	Summary of the Roles of the Rijndael Internal Functions	194
7.6.4	Fast and Secure Implementation	194
7.6.5	Positive Impact of the AES on Applied Cryptography	195
7.7	Confidentiality Modes of Operation	196
7.7.1	The Electronic Codebook Mode (ECB)	197
7.7.2	The Cipher Block Chaining Mode (CBC)	198
7.7.3	The Cipher Feedback Mode (CFB)	199
7.7.4	The Output Feedback Mode (OFB)	200
7.7.5	The Counter Mode (CTR)	201
7.8	Key Channel Establishment for Symmetric Cryptosystems	202
7.9	Chapter Summary	203
8	ENCRYPTION — ASYMMETRIC TECHNIQUES	204
8.1	Introduction	204
8.1.1	Insecurity of Textbook Encryption Algorithms	206
8.1.2	Chapter Outline	207
8.2	The Diffie-Hellman Key Exchange Protocol	207
8.2.1	The Man-in-the-Middle Attack	209
8.2.2	The Diffie-Hellman Problem and the Discrete Logarithm Problem	211
8.2.3	The Importance of Arbitrary Instances in Intractability Assumptions	214
8.3	The RSA Cryptosystem (Textbook Version)	215
8.3.1	Cryptanalysis Against Public-key Cryptosystems	217
8.3.2	Insecurity of the Textbook RSA	219

8.3.3	The Integer Factorization Problem	223
8.4	The Rabin Cryptosystem (Textbook Version)	225
8.4.1	Insecurity of the Textbook Rabin	227
8.5	The ElGamal Cryptosystem (Textbook Version)	229
8.5.1	Insecurity of the Textbook ElGamal	231
8.6	Need for Stronger Security Notions for Public-key Cryptosystems	233
8.7	Combination of Asymmetric and Symmetric Cryptography	234
8.8	Bit Security of the Basic Public-key Cryptographic Functions	236
8.8.1	The RSA Bit	236
8.8.2	The Rabin Bit and the Strength of the Blum-Blum-Shub Pseudo Random Bits Generator	240
8.8.3	The ElGamal Bit	241
8.8.4	The Discrete Logarithm Bit	241
8.9	Key Channel Establishment for Public-key Cryptosystems	244
8.10	Chapter Summary	245
9	DATA INTEGRITY TECHNIQUES	246
9.1	Introduction	246
9.1.1	Chapter Outline	248
9.2	Symmetric Techniques	248
9.2.1	Cryptographic Hash Functions	248
9.2.2	MAC Based on a Keyed Hash Function	252
9.2.3	MAC Based on a Block Cipher Encryption Algorithm	253
9.3	Asymmetric Techniques I: Digital Signatures	254
9.3.1	Textbook Security Notion for Digital Signatures	255
9.3.2	The RSA Signature (Textbook Version)	257
9.3.3	Informal Security Argument for RSA Signature	257
9.3.4	The Rabin Signature (Textbook Version)	259
9.3.5	A Paradoxical Security Basis for Signing in Rabin	259
9.3.6	The ElGamal Signature	261
9.3.7	Informal Security Argument for ElGamal Signature	261
9.3.8	Signature Schemes in the ElGamal Signature Family	264
9.3.9	Formal Security Proof for Digital Signature Schemes	268

9.4 Asymmetric Techniques II: Data Integrity Without Source Identification	269
9.5 Chapter Summary	272

IV Authentication 273

10 AUTHENTICATION PROTOCOLS — PRINCIPLES	275
10.1 Introduction	275
10.1.1 Chapter Outline	276
10.2 Authentication and Refined Notions	277
10.2.1 Data-Origin Authentication	277
10.2.2 Entity Authentication	279
10.2.3 Authenticated Key Establishment	280
10.2.4 Attacks on Authentication Protocols	280
10.3 Convention	281
10.4 Basic Authentication Techniques	283
10.4.1 Message Freshness and Principal Liveness	283
10.4.2 Mutual Authentication	291
10.4.3 Authentication Involving Trusted Third Party	293
10.5 Password-based Authentication Techniques	297
10.5.1 Needham's Password Protocol	297
10.5.2 A One-time Password Scheme (and a Flawed Modification)	299
10.5.3 Add Your Own Salt: Encrypted Key Exchange (EKE)	301
10.6 Authenticated Key Exchange Based on Asymmetric Cryptography	304
10.6.1 The Station-to-station Protocol	305
10.6.2 A Flaw in a Simplified STS Protocol	308
10.6.3 A Minor Flaw of the STS Protocol	310
10.7 Typical Attacks on Authentication Protocols	313
10.7.1 Message Replay Attack	314
10.7.2 Man-in-the-Middle Attack	315
10.7.3 Parallel Session Attack	316
10.7.4 Reflection Attack	319
10.7.5 Interleaving Attack	321

10.7.6	Attack due to Type Flaw	322
10.7.7	Attack due to Name Omission	323
10.7.8	Attack due to Misuse of Cryptographic Services	324
10.8	A Brief Literature Note	328
10.9	Chapter Summary	329
11	AUTHENTICATION PROTOCOLS FOR THE REAL WORLD	330
11.1	Introduction	330
11.1.1	Chapter Outline	331
11.2	Authentication Protocols for Internet Security	332
11.2.1	Communications at the Internet Protocol Layer	332
11.2.2	Internet Protocol Security (IPSec)	333
11.2.3	The Internet Key Exchange (IKE) Protocol	335
11.2.4	A Plausible Deniability Feature in IKE	341
11.2.5	Critiques on IPSec and IKE	343
11.3	The Secure Shell (SSH) Remote Login Protocol	344
11.3.1	The SSH Architecture	344
11.3.2	The SSH Transport Layer Protocol	345
11.3.3	The SSH Strategy	349
11.3.4	A Caveat	349
11.4	The Kerberos Protocol and its Realization in Windows 2000	349
11.4.1	A Single-sign-on Architecture	351
11.4.2	The Kerberos Exchanges	353
11.4.3	Caveats	355
11.5	SSL and TLS	356
11.5.1	TLS Architecture Overview	356
11.5.2	TLS Handshake Protocol	357
11.5.3	A Typical Run of the TLS Handshake Protocol	360
11.6	Chapter Summary	361
12	AUTHENTICATION FRAMEWORK FOR PUBLIC-KEY CRYPTOGRAPHY	362
12.1	Introduction	362

12.1.1 Chapter Outline	363
12.2 Directory-Based Authentication Framework	363
12.2.1 Certificate Issuance	365
12.2.2 Certificate Revocation	365
12.2.3 Examples of Public-key Authentication Framework	366
12.3 Non-Directory Based Authentication Framework	367
12.3.1 Shamir's ID-Based Signature Scheme	369
12.3.2 What Exactly does ID-based Cryptography Offer?	372
12.3.3 Self-certified Public Keys	373
12.3.4 ID-Based Encryption from Pairings on Elliptic Curves	375
12.3.5 Non-interaction Property: Authentication Without Key Channel	384
12.3.6 Two Open Questions for Identity-based Public-key Cryptography	384
12.4 Chapter Summary	385

V FORMALISM APPROACHES TO SECURITY ESTABLISHMENT **386**

13 FORMAL AND FIT-FOR-APPLICATION SECURITY DEFINITIONS FOR PUBLIC-KEY CRYPTOSYSTEMS	388
13.1 Introduction	388
13.1.1 Chapter Outline	390
13.2 A Formal Treatment for Security	390
13.3 Semantic Security — the Debut of Provable Security	394
13.3.1 The SRA Mental Poker Protocol	395
13.3.2 A Security Analysis Based on “Textbook Security”	396
13.3.3 Probabilistic Encryption of Goldwasser and Micali	398
13.3.4 The Security of the GM Cryptosystem	401
13.3.5 A Semantically Secure Version of the ElGamal Cryptosystem	402
13.3.6 Semantically Secure Cryptosystems Based on Rabin Bits	405
13.4 Inadequacy of Semantic Security	406
13.5 Beyond Semantic Security	408

13.5.1 Security Against Chosen Ciphertext Attack	409
13.5.2 Security Against Adaptive Chosen-ciphertext Attack	413
13.5.3 Non-Malleable Cryptography	416
13.5.4 Relations Between Indistinguishability and Non-Malleability	419
13.6 Chapter Summary	424
14 PROVABLY SECURE AND PRACTICALLY EFFICIENT PUBLIC-KEY CRYPTOSYSTEMS	425
14.1 Introduction	425
14.1.1 Chapter Outline	426
14.2 The Optimal Asymmetric Encryption Padding (OAEP)	427
14.2.1 Random Oracle Model for Security Proof	429
14.2.2 RSA-OAEP	431
14.2.3 A Twist in the Security Proof for RSA-OAEP	431
14.2.4 Tightness of “Reduction to Contradiction” for RSA-OAEP	443
14.2.5 A Critique on the Random Oracle Model	444
14.3 The Cramer-Shoup Public-key Cryptosystem	445
14.3.1 Provable Security Under Standard Intractability Assumptions	445
14.3.2 The Cramer-Shoup Scheme	446
14.3.3 Proof of Security	449
14.4 An Overview of Provably Secure Hybrid Cryptosystems	458
14.5 Literature Notes on Practical and Provably Secure Public-key Cryptosystems	460
14.6 Chapter Summary	462
15 PROVABLE SECURITY FOR DIGITAL SIGNATURES	464
15.1 Introduction	464
15.1.1 Chapter Outline	464
15.2 Strong Notion of Security for Digital Signatures	464
15.3 Practical and Provably Secure Signature Schemes	464
15.3.1 Unforgeability argued under a random oracle model	464
15.4 Signcryption	465
15.5 Two Birds One Stone (TBOS)	466
15.5.1 Abstract TBOS	466

15.5.2	RSA-TBOS	467
15.6	Security Notions for Signcryption Schemes	468
15.6.1	IND-CCA2 for Signcryption Schemes	468
15.6.2	Unforgeability of Signcryption Schemes	470
15.7	IND-CCA2 Security of TBOS	471
15.7.1	The Underlying Hard Problem	471
15.7.2	IND-CCA2 Security of Abstract TBOS	472
15.7.3	IND-CCA2 Security of RSA-TBOS	474
15.8	Unforgeability of RSA-TBOS	477
15.9	Conclusion	478
15.10	Chapter Summary	480
16	FORMAL METHODS FOR AUTHENTICATION PROTOCOLS ANALYSIS	481
16.1	Introduction	481
16.1.1	Chapter Outline	482
16.2	Toward Formal Specification of Authentication Protocols	483
16.2.1	Imprecision of Encryption-decryption Approach for Authentication	483
16.2.2	A Refined Specification for Authentication Protocols	488
16.2.3	Examples of Refined Specification for Authentication Protocols	489
16.3	A Computational View of Correct Protocols — the Bellare-Rogaway Model	494
16.3.1	Formal Modelling of the Behavior of Principals	495
16.3.2	The Goal of Mutual Authentication: Matching Conversations	497
16.3.3	Protocol <i>MAP1</i> and its Proof of Security	499
16.3.4	Further Work in Computational Model for Protocols Correctness	501
16.3.5	Discussion	501
16.4	A Symbolic Manipulation View of Correct Protocols	502
16.4.1	Theorem Proving	502
16.4.2	A Logic of Authentication	504
16.5	Formal Analysis Techniques: Finite-State System Approach	506

16.5.1	Model Checking	507
16.5.2	The NRL Protocol Analyzer	509
16.5.3	The CSP Approach	512
16.6	Reconciling Two Views of Formal Reasoning about Security	518
16.7	Chapter Summary	518
VI	Cryptographic Protocols	520
17	ZERO-KNOWLEDGE PROTOCOLS	521
17.1	Introduction	522
17.1.1	Chapter Outline	522
17.2	Zero-knowledge Identification Protocols	522
17.3	Zero-Knowledge-ness	522
17.3.1	Simulatability	522
17.3.2	Statistical Zero-knowledge: Proof by Unbounded Prover	522
17.3.3	Computational Zero-knowledge: Argument by Bounded Prover	522
17.3.4	Honest-verifier Zero-knowledge	522
17.4	Non-interactive Zero-Knowledge Protocols	522
17.4.1	Non-interaction based on Mutually Trusted Randomness	522
17.4.2	Non-interaction based on Fiat-Shamir Heuristic	522
17.5	Mafia Attack	522
17.5.1	Designation of Verifiers	522
17.6	Chapter Summary	522
18	APPLICATIONS OF ZERO-KNOWLEDGE PROTOCOLS	523
18.1	Introduction	523
18.1.1	Chapter Outline	523
18.2	Zero-knowledge Proof of Logical Expression	523
18.3	Zero-knowledge Proof of Secret Sharing	523
18.4	Zero-knowledge Proof of Structure	523
18.5	Zero-knowledge Proof of Primality	523
18.6	Electronic Voting	523
18.7	Chapter Summary	523

19 ANONYMITY	524
19.1 Introduction	524
19.1.1 Chapter Outline	524
19.2 Anonymous Cryptographic Credentials	524
19.2.1 Chaum's Blind Signature	524
19.2.2 Cut-and-choose Paradigm and Electronic Cash	524
19.2.3 Okamoto's Blind Signature	524
19.2.4 Brand's Blind Signature	524
19.3 Deniable Cryptographic Credentials	524
19.3.1 Zero-knowledge Undeniable Signatures	524
19.3.2 Designated Verifier Proofs	524
19.3.3 Ring Signatures	524
19.3.4 Spy's Problem and its Application in IPSec	524
19.4 Extortion Prevention: Responsible Anonymity and Deniability	524
19.5 Chapter Summary	524
 20 CRYPTOGRAPHIC PROTOCOLS FOR ELECTRONIC COM- MERCE	 525
20.1 Introduction	525
20.1.1 Chapter Outline	525
20.2 Secure Electronic Transactions (SET)	525
20.3 Protocols for Micro-payments	525
20.3.1 PayWord and MicroMint	525
20.3.2 Aggregation of Small Payments via Gambling	525
20.4 Fair Exchange	525
20.5 Chapter Summary	525
 BIBLIOGRAPHY	 526