

Contents

1	Introduction to Cryptography	1
1.1	Introduction to Cryptography	1
1.2	The Players in the Game	2
1.3	Ciphertext Only Attack: An Example	4
1.4	Exercises	7
2	Introduction to Probability	9
2.1	Introduction to Probability	9
2.1.1	Abstract Probability Spaces	11
2.2	Conditional Probability	14
2.3	Collision Theorems	15
2.4	Random Variables	19
2.5	2-Dimensional Random Variables	22
2.6	Bernoulli's Theorem	25
2.7	Exercises	26
3	Information Theory and Entropy	29
3.1	Entropy	29
3.1.1	Entropy and Randomness: Jensen's Inequality	31
3.2	Entropy of Plaintext English	35
3.2.1	ASCII Encoding	39
3.3	Joint and Conditional Entropy	40
3.4	Unicity Distance	44
3.5	Exercises	50
4	Introduction to Complexity Theory	53
4.1	Basics of Complexity Theory	53
4.2	Polynomial Time Algorithms	54
4.3	Non-polynomial Time Algorithms	58
4.4	Complexity Classes P, PP, BPP	61
4.4.1	Probabilistic Polynomial Time	62
4.4.2	An Example	66

4.5	Probabilistic Algorithms for Functions	68
4.6	Exercises	69
5	Algebraic Foundations: Groups	73
5.1	Introduction to Groups	73
5.2	Examples of Infinite Groups	75
5.3	Examples of Finite Groups	77
5.3.1	The Symmetric Group on n Letters	77
5.3.2	The Group of Residues Modulo n	81
5.4	Direct Product of Groups	84
5.5	Subgroups	85
5.6	Homomorphisms of Groups	87
5.7	Group Structure	88
5.7.1	Some Number Theory	92
5.8	Exercises	97
6	Algebraic Foundations: Rings and Fields	101
6.1	Introduction to Rings and Fields	101
6.1.1	Polynomials in $F[x]$	104
6.2	The Group of Units of $\mathbb{Z}_n$	106
6.2.1	A Formula for Euler's Function	109
6.3	$U(\mathbb{Z}_p)$ Is Cyclic	110
6.4	Exponentiation in $\mathbb{Z}_n$	111
6.4.1	Quadratic Residues	112
6.5	Exercises	116
7	Advanced Topics in Algebra	117
7.1	Quotient Rings and Ring Homomorphisms	117
7.1.1	Quotient Rings	117
7.1.2	Ring Homomorphisms	123
7.2	Simple Algebraic Extensions	126
7.2.1	Algebraic Closure	128
7.3	Finite Fields	128
7.4	Invertible Matrices over $\mathbb{Z}_{pq}$	134
7.5	Exercises	136
8	Symmetric Key Cryptography	139
8.1	Simple Substitution Cryptosystems	140
8.1.1	Unicity Distance of the Simple Substitution Cryptosystem	142
8.2	The Affine Cipher	143
8.2.1	Unicity Distance of the Affine Cipher	145
8.3	The Hill 2×2 Cipher	145
8.3.1	Unicity Distance of the Hill 2×2 Cipher	148
8.4	Cryptanalysis of the Simple Substitution Cryptosystem	149
8.5	Polyalphabetic Cryptosystems	155
8.5.1	The Vigenère Cipher	156

8.5.2	Unicity Distance of the Vigenère Cipher	157
8.5.3	Cryptanalysis of the Vigenère Cipher	157
8.5.4	The Vernam Cipher	160
8.5.5	Unicity Distance of the Vernam Cipher	162
8.6	Stream Ciphers	163
8.7	Block Ciphers	164
8.7.1	Iterated Block Ciphers.....	165
8.8	Exercises	168
9	Public Key Cryptography	173
9.1	Introduction to Public Key Cryptography	173
9.1.1	Negligible Functions	174
9.1.2	One-Way Trapdoor Functions.....	175
9.2	The RSA Public Key Cryptosystem	177
9.3	Security of RSA	180
9.3.1	Pollard $p - 1$	181
9.3.2	Pollard ρ	183
9.3.3	Difference of Two Squares	187
9.4	The ElGamal Public Key Cryptosystem	193
9.5	Hybrid Ciphers	196
9.6	Symmetric vs. Public Key Cryptography	197
9.7	Exercises	199
10	Digital Signature Schemes	203
10.1	Introduction to Digital Signature Schemes.....	203
10.2	The RSA Digital Signature Scheme	205
10.3	Signature with Privacy	207
10.4	Security of Digital Signature Schemes	208
10.5	Hash Functions and DSS.....	209
10.5.1	The Discrete Log Family	210
10.5.2	The MD-4 Family	212
10.5.3	Hash-Then-Sign DSS.....	214
10.6	Exercises	215
11	Key Generation	217
11.1	Linearly Recursive Sequences	217
11.2	The Shrinking Generator Sequence	226
11.3	Linear Complexity	231
11.4	Pseudorandom Bit Generators	235
11.4.1	Hard-Core Predicates	237
11.4.2	Hard-Core Predicates and the DLA.....	238
11.4.3	The Blum–Micali Bit Generator	242
11.4.4	The Quadratic Residue Assumption	245
11.4.5	The Blum–Blum–Shub Bit Generator	247
11.5	Exercises	251

- 12 Key Distribution 255
 - 12.1 The Diffie–Hellman Key Exchange Protocol 255
 - 12.2 The Discrete Logarithm Problem 256
 - 12.2.1 The General DLP 258
 - 12.2.2 Index Calculus 262
 - 12.2.3 Efficiency of Index Calculus 265
 - 12.2.4 The Man-in-the-Middle Attack 267
 - 12.3 Exercises 268
- 13 Elliptic Curves in Cryptography 271
 - 13.1 The Equation $y^2 = x^3 + ax + b$ 271
 - 13.2 Elliptic Curves 276
 - 13.3 Singular Curves 278
 - 13.4 The Elliptic Curve Group 279
 - 13.4.1 Structure of $E(K)$ 285
 - 13.5 The Elliptic Curve Key Exchange Protocol 287
 - 13.5.1 Comparing ECKEP and DHKEP 289
 - 13.5.2 What Elliptic Curves to Avoid 290
 - 13.5.3 Examples of Good Curves 292
 - 13.6 Exercises 296
- 14 Singular Curves 297
 - 14.1 The Group $E_{ns}(K)$ 297
 - 14.2 The DLP in $E_{ns}(K)$ 301
 - 14.3 The Group $G_c(K)$ 303
 - 14.4 $E_{ns}(K) \cong G_c(K)$ 306
 - 14.5 Exercises 309
- References 311
- Index 315