# Contents


**1 Prerequisites and Notation** ..... 1
1.1 Sets ..... 1
1.2 Products of Sets ..... 4
1.3 Relations ..... 5
1.4 Functions ..... 8
1.5 Binary Operations ..... 9
1.6 Cryptography ..... 10
1.6.1 Encryption Mechanisms ..... 11
1.6.2 Confusion and Diffusion ..... 11
1.6.3 Symmetric and Asymmetric Encryption ..... 12
1.7 Notational Conventions ..... 13
1.7.1 Floor and Ceiling ..... 13
1.7.2 Fractional Part ..... 13
1.7.3 Exclusive Or ..... 14
1.7.4 Matrix Multiplication ..... 14

**2 Basic Properties of the Integers** ..... 17
2.1 Divisibility ..... 17
2.2 Ideals and Greatest Common Divisors ..... 19
2.3 The Euclidean Algorithm ..... 23
2.3.1 Stein's gcd Algorithm ..... 27
2.4 Congruences ..... 28
2.5 Fermat's Factoring Method ..... 31
2.6 Solving Linear Congruences ..... 33
2.7 The Chinese Remainder Theorem ..... 36
2.8 Some Number-Theoretic Functions ..... 38
2.8.1 Multiplicative Functions ..... 38
2.8.2 The Möbius Function ..... 41
2.8.3 Euler's $\phi$-Function ..... 42
2.8.4 The Case $n = p \cdot q$ ..... 44

**3 Groups, Rings and Ideals** ..... 45
3.1 Groups ..... 45
3.2 Subgroups ..... 49
3.3 The Lattice of Subgroups ..... 51
3.4 Cosets ..... 52
3.5 Cyclic Groups ..... 55
3.6 Fermat's Little Theorem ..... 57
3.7 Primality Testing ..... 58
3.7.1 Miller's Test ..... 59
3.7.2 The Miller–Rabin Primality Test ..... 60
3.8 Rings and Ideals ..... 61

**4 Applications to Public Key Cryptography** ..... 67
4.1 Public Key Encryption: The RSA Mechanism ..... 67
4.1.1 RSA ..... 68
4.1.2 Breaking RSA ..... 70
4.1.3 Using the Chinese Remainder Theorem ..... 72
4.1.4 Public Key Infrastructures ..... 73
4.2 The Discrete Logarithm Problem (DLP) ..... 74
4.2.1 Statement of the Problem ..... 74
4.2.2 Exhaustive Search ..... 75
4.2.3 Shanks' Method ..... 76
4.2.4 Pollard's Rho Method ..... 76
4.3 Diffie–Hellman Key Establishment ..... 77
4.4 Other Applications of the DLP ..... 79
4.4.1 ElGamal Encryption ..... 79
4.4.2 The ElGamal Digital Signature Scheme ..... 80
4.4.3 The Digital Signature Algorithm ..... 81
4.4.4 A Zero Knowledge Proof ..... 82
4.4.5 What Groups to Use? ..... 83

**5 Fields** ..... 85
5.1 Rings "Without" Ideals ..... 85
5.2 Vector Spaces ..... 88
5.3 Rings of Polynomials ..... 90
5.3.1 Definitions ..... 90
5.3.2 The Euclidean Algorithm Again ..... 92
5.3.3 The "Remainder Theorem" ..... 93
5.3.4 Irreducible Polynomials ..... 95
5.4 Ring Homomorphisms ..... 96
5.5 The Chinese Remainder Theorem Again ..... 99
5.6 Construction of Finite Fields ..... 99

**6 Properties of Finite Fields** ..... 105
6.1 The Minimal Polynomial of an Element ..... 105

6.2 More on the Structure of Finite Fields ..... 109
6.3 Solving Quadratic Equations over $GF(2^n)$ and the Trace Function ..... 112
6.4 Operations in Finite Fields ..... 114
6.4.1 Addition in $\mathbb{Z}_n$ ..... 115
6.4.2 Inverses in $\mathbb{Z}_n$ ..... 115
6.4.3 Multiplication in $GF(p^n)$ ..... 116
6.4.4 Exponentiation ..... 116
6.4.5 Inverses in $GF(p^n)$ ..... 117
6.5 Factoring Polynomials ..... 117
6.5.1 Square-freeness ..... 117
6.5.2 A Test for Irreducibility ..... 118
6.5.3 Finding a Factor ..... 119
6.6 The Discrete Logarithm Problem on a Finite Field ..... 120
6.7 Elliptic Curves over a Finite field ..... 121

**7 Applications to Stream Ciphers** ..... 123
7.1 Introduction ..... 123
7.1.1 Stream Ciphers vs Block Ciphers ..... 123
7.1.2 Design Principles ..... 124
7.1.3 Terminology ..... 125
7.2 Some Notes on Entropy ..... 129
7.2.1 Entropy = Uncertainty ..... 129
7.2.2 Conditional Entropy ..... 133
7.2.3 Information ..... 134
7.2.4 Redundancy ..... 135
7.3 Perfect Secrecy ..... 137
7.4 Linear Feedback Shift Registers ..... 139
7.5 LFSRs: Further Theory ..... 145
7.6 Galois Field Counters ..... 148
7.6.1 Shift Registers in Feedforward Mode ..... 148
7.6.2 Finite Field Multiplication ..... 149
7.6.3 Galois Counters and Authenticated Encryption ..... 149
7.7 Filter and Combining Functions ..... 150
7.8 Linear Complexity ..... 151
7.8.1 Introduction ..... 151
7.8.2 The Berlekamp–Massey Algorithm ..... 153
7.8.3 The Linear Complexity Profile ..... 159
7.9 On the Design of Stream Ciphers ..... 160
7.10 Combination Generators ..... 163
7.11 Filter Generators ..... 166
7.12 Clock Controlled Generators ..... 168
7.12.1 The Stop-and-Go Generator ..... 168
7.12.2 Alternating Step Generator ..... 169
7.12.3 Shrinking Generator ..... 169

7.12.4 Self-Shrinking Generator ..... 171
7.12.5 Bitsearch Generators ..... 172

**8 Boolean Functions** ..... 175
8.1 Introduction ..... 175
8.2 The Algebraic Normal Form ..... 178
8.3 The Walsh Transform ..... 181
8.3.1 Hadamard Matrices ..... 181
8.3.2 Definition of the Walsh Transform ..... 182
8.3.3 Correlation with Linear Functions ..... 185
8.3.4 Correlation Immunity ..... 187
8.3.5 Linear Algebraic Gloss ..... 191
8.4 Autocorrelation ..... 192
8.5 Nonlinearity ..... 195
8.6 Propagation Criteria ..... 196
8.7 Linear Structures ..... 199
8.7.1 Linearity ..... 199
8.7.2 Another Measure of Nonlinearity ..... 201
8.8 Bent Functions ..... 202
8.8.1 The Simplest Bent function ..... 204
8.8.2 The "Dot-Product" Bent Functions ..... 204
8.8.3 The Maiorama Construction ..... 205
8.8.4 Other Constructions ..... 205
8.8.5 Extensions of Bent Functions ..... 206
8.9 Algebraic Immunity ..... 208
8.10 Completeness ..... 212
8.11 The Discrete Fourier Transform ..... 213
8.11.1 Introduction ..... 213
8.11.2 Linear Complexity Revisited ..... 214
8.11.3 DFT over a Finite Field ..... 216

**9 Applications to Block Ciphers** ..... 219
9.1 Block Ciphers ..... 219
9.2 Finite Fields in *Rijndael* ..... 220
9.2.1 Linear Operations ..... 222
9.2.2 The *Rijndael* Substitution Box ..... 224
9.2.3 Properties of the *Rijndael* S-box ..... 224
9.2.4 Properties of the *Rijndael* Round Function ..... 229
9.3 Properties of the Function $F(x) = x^{2^k+1}$ ..... 230
9.3.1 Differential Uniformity ..... 231
9.3.2 Nonlinearity ..... 232
9.3.3 Degree ..... 235
9.4 Perfect Nonlinear S-boxes ..... 236
9.5 Diffusion ..... 237
9.5.1 Introduction ..... 237

9.5.2 Linear Codes ..... 238
9.5.3 Error Detection and Correction ..... 240
9.5.4 Some Properties of MDS Matrices ..... 240
9.5.5 MDS Matrices in Block Ciphers ..... 243
9.5.6 Examples of MDS Matrices ..... 244
9.5.7 Binary Codes ..... 247
9.5.8 Boolean Functions and Codes ..... 248

**10 Number Theory in Public Key Cryptography** ..... 251
10.1 Secret Sharing: Shamir's Mechanism ..... 252
10.2 Access Structures and the Chinese Remainder Theorem ..... 253
10.2.1 Access Structures ..... 253
10.2.2 Disjunctive and Conjunctive Normal Forms ..... 253
10.2.3 Yet Another Appearance of the CRT ..... 255
10.2.4 The Conjunctive Normal Form ..... 255
10.3 Quadratic Residues ..... 257
10.4 The Legendre Symbol ..... 258
10.5 The Quadratic Reciprocity Theorem ..... 261
10.6 The Jacobi Symbol ..... 263
10.7 Solving Quadratic Congruences ..... 267
10.8 The Quadratic Residuosity Problem ..... 268
10.9 Applications of Quadratic Residues ..... 268
10.9.1 Rabin Encryption ..... 268
10.9.2 Goldwasser–Micali Encryption ..... 270
10.9.3 Coin Flipping by Telephone ..... 271
10.9.4 Oblivious Transfer ..... 272
10.9.5 Exchanging Secrets with Oblivious Transfer ..... 273
10.9.6 Commitment ..... 274
10.9.7 Blum–Blum–Shub Pseudo-Random Bit Generation ..... 276

**11 Where Do We Go from Here?** ..... 277
11.1 Further Reading ..... 277
11.2 Further Topics ..... 279
11.2.1 Elliptic Curves ..... 279
11.2.2 Lattices ..... 280
11.2.3 Homomorphic Cryptography ..... 281
11.2.4 Post-Quantum Cryptography ..... 282
11.3 Even More Further Reading ..... 283

**A Probability** ..... 285
A.1 Definitions ..... 285
A.1.1 Introduction ..... 285
A.1.2 Conditional Probability ..... 286
A.1.3 Independence of Events ..... 287
A.1.4 Mode, Mean and Variance ..... 287

A.2 Discrete Probability Distributions ..... 288
A.2.1 The Uniform Distribution ..... 288
A.2.2 The Binomial Distribution ..... 288
A.2.3 The Bernoulli Distribution ..... 288
A.2.4 The Poisson Distribution ..... 289
A.2.5 The Geometric Distribution ..... 290
A.3 Continuous Probability Distributions ..... 290
A.3.1 The Uniform Distribution ..... 290
A.3.2 The Normal Distribution ..... 291
A.3.3 The Exponential Distribution ..... 292
A.4 The Central Limit Theorem ..... 292
A.5 The Chi-Squared Distribution ..... 293
A.6 The Birthday "Paradox" ..... 294
A.7 Bayes' Theorem ..... 295

**Index** ..... 297