Preface xiii

Chapter 1 INTRODUCTION 1
1.1 Themes of Analysis 2
1.2 Information Lessons 4

Part I: ENTROPY: The Foundation of Information

Chapter 2 INFORMATION DEFINITION 9
2.1 A Measure of Information 10
2.2 The Definition of Entropy 12
2.3 Information Sources 14
2.4 Source Combinations 15
2.5 Bits as a Measure 16
2.6 About Claude E. Shannon 17
2.7 Exercises 18
2.8 Bibliography 19

Chapter 3 CODES 21
3.1 The Coding Problem 21
3.2 Average Code Length and Entropy 27
3.3 Shannon's First Theorem 30
3.4 Exercises 33
3.5 Bibliography 34

Chapter 4 COMPRESSION 35
4.1 Huffman Coding 35
4.2 Intersymbol Dependency 40
4.3 Lempel–Ziv Coding 44
4.4 Other Forms of Compression 48
4.5 Exercises 52
4.6 Bibliography 53

Chapter 5 CHANNELS 55
5.1 Discrete Channel 56
5.2 Conditional and Joint Entropies 57

5.3 Flipping a Channel 60
5.4 Mutual Information 62
5.5 Capacity* 65
5.6 Shannon's Second Theorem* 66
5.7 Exercises 68
5.8 Bibliography 69

Chapter 6 ERROR-CORRECTING CODES 70
6.1 Simple Code Concepts 71
6.2 Hamming Distance 73
6.3 Hamming Codes 75
6.4 Linear Codes 77
6.5 Low-Density Parity Check Codes 78
6.6 Interleaving 79
6.7 Convolutional Codes 80
6.8 Turbo Codes 82
6.9 Applications 83
6.10 Exercises 85
6.11 Bibliography 86

Summary of Part I 89

Part II: ECONOMICS: Strategies for Value

Chapter 7 MARKETS 93
7.1 Demand 94
7.2 Producers 97
7.3 Social Surplus 99
7.4 Competition 100
7.5 Optimality of Marginal Cost Pricing 101
7.6 Linear Demand Curves 102
7.7 Copyright and Monopoly 103
7.8 Other Pricing Methods 107
7.9 Oligopoly 108
7.10 Exercises 111
7.11 Bibliography 113

Chapter 8 PRICING SCHEMES 114
8.1 Discrimination 114
8.2 Versions 116
8.3 Bundling 119
8.4 Sharing 124
8.5 Exercises 127
8.6 Bibliography 128

Chapter 9 VALUE 130
9.1 Conditional Information 131
9.2 Informativity and Generalized Entropy* 133
9.3 Decisions 135
9.4 The Structure of Value 135
9.5 Utility Functions* 139
9.6 Informativity and Decision Making* 140
9.7 Exercises 141
9.8 Bibliography 142

Chapter 10 INTERACTION 143
10.1 Common Knowledge 144
10.2 Agree to Disagree? 146
10.3 Information and Decisions 149
10.4 A Formal Analysis* 150
10.5 Metcalfe's Law 153
10.6 Network Economics* 155
10.7 Exercises 159
10.8 Bibliography 160

Summary of Part II 161

Part III: ENCRYPTION: Security through Mathematics

Chapter 11 CIPHERS 165
11.1 Definitions 166
11.2 Example Ciphers 166
11.3 Frequency Analysis 169
11.4 Cryptograms 169
11.5 The Vigenère Cipher 171
11.6 The Playfair Cipher 174
11.7 Homophonic Codes 175
11.8 Jefferson's Wheel Cipher 176
11.9 The Enigma Machine 177
11.10 The One-Time Pad 181
11.11 Exercises 183
11.12 Bibliography 184

Chapter 12 CRYPTOGRAPHY THEORY 186
12.1 Perfect Security 186
12.2 Entropy Relations 188
12.3 Use of a One-Time Pad* 193
12.4 The DES and AES Systems 196

12.5 Exercises 197
12.6 Bibliography 198

Chapter 13 PUBLIC KEY CRYPTOGRAPHY 200

13.1 A Basic Dilemma 200
13.2 One-Way Functions 201
13.3 Discrete Logarithms 202
13.4 Diffie–Hellman Key Exchange 203
13.5 Modular Mathematics 205
13.6 Alternative Puzzle Solution 208
13.7 RSA 209
13.8 Square and Multiply* 211
13.9 Finding Primes* 213
13.10 Performance* 214
13.11 The Future 215
Appendix: The Extended Euclidean Algorithm 216
13.12 Exercises 217
13.13 Bibliography 218

Chapter 14 SECURITY PROTOCOLS 220

14.1 Digital Signatures 220
14.2 Blinded Signatures 223
14.3 Digital Cash 225
14.4 Identification 226
14.5 Zero-Knowledge Proofs 228
14.6 Smart Cards 231
14.7 Exercises 234
14.8 Bibliography 235

Summary of Part III 237

Part IV: EXTRACTION: Information from Data

Chapter 15 DATA STRUCTURES 241

15.1 Lists 241
15.2 Trees 244
15.3 Traversal of Trees 247
15.4 Binary Search Trees (BST) 248
15.5 Partially Ordered Trees 252
15.6 Tries* 254
15.7 Basic Sorting Algorithms 255
15.8 Quicksort 257
15.9 Heapsort 260
15.10 Merges 261
15.11 Exercises 262
15.12 Bibliography 263

Chapter 16 DATABASE SYSTEMS 264
16.1 Relational Structure 264
16.2 Keys 267
16.3 Operations 267
16.4 Functional Dependencies 271
16.5 Normalization 271
16.6 Joins and Products* 277
16.7 Database Languages 279
16.8 Exercises 281
16.9 Bibliography 282

Chapter 17 INFORMATION RETRIEVAL 284
17.1 Inverted Files 285
17.2 Strategies for Indexing 287
17.3 Inverted File Compression* 291
17.4 Queries 293
17.5 Ranking Methods 294
17.6 Network Rankings 296
17.7 Exercises 299
17.8 Bibliography 299

Chapter 18 DATA MINING 301
18.1 Overview of Techniques 301
18.2 Market Basket Analysis 303
18.3 Least-Squares Approximation 306
18.4 Classification Trees 310
18.5 Bayesian Methods 314
18.6 Support Vector Machines 319
18.7 Other Methods 323
18.8 Exercises 325
18.9 Bibliography 327

Summary of Part IV 327

Part V: EMISSION: The Mastery of Frequency

Chapter 19 FREQUENCY CONCEPTS 331
19.1 The Telegraph 334
19.2 When Dots Became Dashes 335
19.3 Fourier Series 338
19.4 The Fourier Transform 339
19.5 Thomas Edison and the Telegraph 342
19.6 Bell and the Telephone 342
19.7 Lessons in Frequency 345
19.8 Exercises 347
19.9 Bibliography 349

Chapter 20 RADIO WAVES 350
20.1 Why Frequencies? 350
20.2 Resonance 354
20.3 The Birth of Radio 354
20.4 Marconi's Radio 355
20.5 The Spark Bandwidth 357
20.6 The Problems 359
20.7 Continuous Wave Generation 360
20.8 The Triode Vacuum Tube 361
20.9 Modulation Mathematics 363
20.10 Heterodyne Principle 365
20.11 Frequency Modulation 367
20.12 Exercises 369
20.13 Bibliography 372

Chapter 21 SAMPLING AND CAPACITY 373
21.1 Entropy 373
21.2 Capacity of the Gaussian Channel 376
21.3 Sampling Theorem 378
21.4 Generalized Sampling Theorem* 380
21.5 Thermal Noise 383
21.6 Capacity of a Band-Limited Channel 384
21.7 Spread Spectrum 385
21.8 Spreading Technique 387
21.9 Multiple Access Systems 388
21.10 Exercises 391
21.11 Bibliography 392

Chapter 22 NETWORKS 393
22.1 Poisson Processes 394
22.2 Frames 395
22.3 The ALOHA System 396
22.4 Carrier Sensing 398
22.5 Routing Algorithms 399
22.6 The Bellman–Ford Algorithm 400
22.7 Distance Vector Routing 401
22.8 Dijkstra's Algorithm 402
22.9 Other Issues 404
22.10 Exercises 405
22.11 Bibliography 406

Summary of Part V 407

Index 409