CRYPTOGRAPHY, INFORMATION THEORY, AND ERROR-CORRECTION

A Handbook for the 21st Century

AIDEN A. BRUEN
MARIO A. FORCINITO
Cryptography,
Information Theory,
and Error-Correction
WILEY-INTERSCIENCE
SERIES IN DISCRETE MATHEMATICS AND OPTIMIZATION

ADVISORY EDITORS

RONALD L. GRAHAM
University of California at San Diego, U.S.A.

JAN KAREL LENSTRA
Department of Mathematics and Computer Science,
Eindhoven University of Technology, Eindhoven, The Netherlands

JOEL H. SPENCER
Courant Institute, New York, New York, U.S.A.

A complete list of titles in this series appears at the end of this volume.
Cryptography, Information Theory, and Error-Correction
A Handbook for the 21st Century

Aiden A. Bruen
Mario A. Forcinito

WILEY-INTERSCIENCE
A JOHN WILEY & SONS, INC., PUBLICATION
Contents

Preface xiii

I Cryptography 1

1 History and Claude E. Shannon 3
  1.1 Historical Background ................................. 3
  1.2 Brief Biography of Claude E. Shannon .................. 8
  1.3 Career ................................................. 9
  1.4 Personal—Professional .................................. 10
  1.5 Scientific Legacy ...................................... 11
  1.6 Modern Developments .................................. 14

2 Classical Ciphers and Their Cryptanalysis 17
  2.1 Introduction ........................................... 17
  2.2 The Caesar Cipher ..................................... 18
  2.3 The Scytale Cipher .................................. 20
  2.4 The Vigenère Cipher .................................. 21
  2.5 The Enigma Machine and Its Mathematics ............... 22
  2.6 Frequency Analysis .................................. 26
  2.7 Breaking the Vigenère Cipher, Babbage–Kasiski ........ 26
  2.8 Modern Enciphering Systems ............................ 31
  2.9 Problems ............................................ 32
  2.10 Solutions ............................................ 33

3 RSA, Key Searches, SSL, and Encrypting Email 39
  3.1 Background ............................................ 41
  3.2 The Basic Idea of Cryptography ......................... 41
  3.3 Public Key Cryptography and RSA on a Calculator ....... 45
  3.4 The General RSA Algorithm ............................. 48
  3.5 Public Key Versus Symmetric Key ....................... 51
## CONTENTS

3.6 Attacks, Security of DES, Key-spaces ........................................... 54
3.7 Summary of Encryption ................................................................. 56
3.8 SSL (Secure Socket Layer) ............................................................... 57
3.9 PGP and GPG ................................................................................ 59
3.10 RSA Challenge .............................................................................. 60
3.11 Problems ....................................................................................... 61
3.12 Solutions ....................................................................................... 64

4 The Fundamentals of Modern Cryptography .................................... 69
4.1 Encryption Revisited ...................................................................... 69
4.2 Block Ciphers, Shannon's Confusion and Diffusion ....................... 71
4.3 Perfect Secrecy, Stream Ciphers, One-Time Pad ......................... 73
4.4 Hash Functions .............................................................................. 76
4.5 Message Integrity Using Symmetric Cryptography ....................... 79
4.6 General Public Key Cryptosystems ................................................ 80
4.7 Electronic Signatures ..................................................................... 82
4.8 The Diffie–Hellman Key Exchange ................................................ 84
4.9 Quantum Encryption ..................................................................... 87
4.10 Key Management and Kerberos .................................................... 89
4.11 DES ............................................................................................. 91
4.12 Problems ..................................................................................... 92
4.13 Solutions ..................................................................................... 92

5 DES, AES and Operating Modes .................................................... 95
5.1 The Data Encryption Standard Code ............................................. 95
5.2 Triple DES ..................................................................................... 101
5.3 DES and Unix ................................................................................ 102
5.4 The Advanced Encryption Standard Code .................................... 102
5.5 Problems ...................................................................................... 109
5.6 Solutions ...................................................................................... 110

6 Elliptic Curve Cryptography (ECC) .............................................. 113
6.1 Abelian Integrals, Fields, Groups ................................................ 113
6.2 Curves, Cryptography ................................................................... 115
6.3 Nonsingularity ............................................................................. 117
6.4 The Hasse Theorem, and an Example ......................................... 117
6.5 More Examples ............................................................................. 118
6.6 The Group Law on Elliptic Curves ................................................. 119
6.7 Key Exchange with Elliptic Curves .............................................. 122
6.8 Elliptic Curves mod \( n \) .................................................. 122
6.9 Encoding Plain Text ..................................................... 122
6.10 Security of ECC ......................................................... 123
6.11 More Geometry of Cubic Curves ...................................... 123
6.12 Cubic Curves and Arcs .................................................. 124
6.13 Homogeneous Coordinates ............................................. 124
6.14 Fermat’s Last Theorem, Elliptic Curves, Gerhard Frey .......... 125
6.15 Problems .................................................................. 126
6.16 Solutions ................................................................ 126

7 Attacks in Cryptography .................................................. 131
7.1 Cryptanalysis ................................................................ 131
7.2 Soft Attacks ................................................................ 132
7.3 Brute Force Attacks ..................................................... 133
7.4 Man-In-The-Middle Attacks ............................................ 134
7.5 Known Plain Text Attacks .............................................. 135
7.6 Known Cipher Text Attacks ............................................ 135
7.7 Chosen Plain Text Attacks .............................................. 136
7.8 Chosen Cipher Text Attacks, Digital Signatures ................. 136
7.9 Replay Attacks ........................................................... 137
7.10 Birthday Attacks ........................................................ 137
7.11 Birthday Attack on Digital Signatures .............................. 138
7.12 Birthday Attack on the Discrete Log Problem .................... 139
7.13 Attacks on RSA .......................................................... 139
7.14 Attacks on RSA using Low-Exponents ............................. 140
7.15 Timing Attack ............................................................ 141
7.16 Differential Cryptanalysis .............................................. 142
7.17 Implementation Errors and Unforeseen States ................. 143

8 Practical Issues ............................................................. 145
8.1 Introduction .................................................................. 145
8.2 Hot Issues .................................................................. 146
8.3 Authentication ............................................................ 147
8.4 E-Commerce ............................................................... 151
8.5 E-Government ............................................................ 152
8.6 Key Lengths ............................................................... 153
8.7 Digital Rights ............................................................. 154
8.8 Wireless Networks ....................................................... 154
8.9 Communication Protocols .............................................. 156
II Information Theory 159

9 Information Theory and Its Applications 161
  9.1 Axioms, Physics, Computation ........................................ 161
  9.2 Entropy ........................................................................ 162
  9.3 Information Gained, Cryptography ................................... 164
  9.4 Practical Applications of Information Theory ...................... 166
  9.5 Information Theory and Physics ....................................... 167
  9.6 Axiomatics of Information Theory ..................................... 168
  9.7 Number Bases, Erdös, and the Hand of God ....................... 169
  9.8 Weighing Problems and Your MBA ................................... 171
  9.9 Shannon Bits, the Big Picture ......................................... 173

10 Random Variables and Entropy 175
  10.1 Random Variables ........................................................ 175
  10.2 Mathematics of Entropy ............................................... 178
  10.3 Calculating Entropy ..................................................... 179
  10.4 Conditional Probability ................................................ 180
  10.5 Bernoulli Trials .......................................................... 184
  10.6 Typical Sequences ....................................................... 185
  10.7 Law of Large Numbers ................................................ 186
  10.8 Joint and Conditional Entropy ........................................ 187
  10.9 Applications of Entropy ............................................... 192
  10.10 Calculation of Mutual Information ................................. 193
  10.11 Mutual Information and Channels ................................. 194
  10.12 The Entropy of \( X + Y \) ............................................. 195
  10.13 Subadditivity of the Function \(-x \log x\) ......................... 196
  10.14 Entropy and Cryptography .......................................... 196
  10.15 Problems .................................................................. 196
  10.16 Solutions .................................................................. 198

11 Source Coding, Data Compression, Redundancy 203
  11.1 Introduction, Source Extensions ..................................... 204
  11.2 Encodings, Kraft, McMillan .......................................... 205
  11.3 Block Coding, The Oracle, Yes-No Questions .................... 211
  11.4 Optimal Codes .......................................................... 212
  11.5 Huffman Coding ........................................................ 213
  11.6 Optimality of Huffman Coding ...................................... 218
  11.7 Data Compression, Lempel-Ziv Coding, Redundancy .......... 219
### CONTENTS

11.8 Problems ........................................... 222
11.9 Solutions ........................................... 223

#### 12 Channels, Capacity, the Fundamental Theorem 225
12.1 Abstract Channels ................................... 226
12.2 More Specific Channels ............................ 227
12.3 New Channels from Old, Cascades ................. 228
12.4 Input Probability, Channel Capacity .............. 231
12.5 Capacity for General Binary Channels, Entropy .. 234
12.6 Hamming Distance .................................. 236
12.7 Improving Reliability of a Binary Symmetric Channel 237
12.8 Error Correction, Error Reduction, Good Redundancy 238
12.9 The Fundamental Theorem of Information Theory .. 241
12.10 Summary, the Big Picture .......................... 248
12.11 Problems ........................................... 248
12.12 Solutions ........................................... 249

#### 13 Signals, Sampling, SNR, Coding Gain 253
13.1 Continuous Signals, Shannon’s Sampling Theorem ... 253
13.2 The Band-Limited Capacity Theorem, an Example ... 256
13.3 The Coding Gain .................................... 259

#### 14 Ergodic and Markov Sources, Language Entropy 261
14.1 General and Stationary Sources .................... 261
14.2 Ergodic Sources .................................... 264
14.3 Markov Chains and Markov Sources ............... 265
14.4 Irreducible Markov Sources, Adjoint Source ...... 269
14.5 Cascades and the Data Processing Theorem ....... 270
14.6 The Redundancy of Languages ..................... 271
14.7 Problems ........................................... 274
14.8 Solutions ........................................... 275

#### 15 Perfect Secrecy: the New Paradigm 277
15.1 Symmetric Key Cryptosystems ....................... 277
15.2 Perfect Secrecy and Equiprobable Keys ............. 279
15.3 Perfect Secrecy and Latin Squares ............... 280
15.4 The Abstract Approach to Perfect Secrecy ......... 282
15.5 Cryptography, Information Theory, Shannon ....... 283
15.6 Unique Message from Ciphertext, Unicity .......... 283
CONTENTS

15.7 Problems ............................................. 284
15.8 Solutions ............................................ 286

16 Shift Registers (LFSR) and Stream Ciphers .......................... 289

16.1 Vernam Cipher, Pseudo-Random Key ................................ 290
16.2 Construction of Feedback Shift Registers ................................. 290
16.3 Periodicity ............................................. 293
16.4 Maximal Periods, Pseudo-Random Sequences ............................. 296
16.5 Determining the Output from 2m Bits .................................... 297
16.6 The Tap Polynomial and the Period ....................................... 300
16.7 Berlekamp–Massey Algorithm ........................................... 301
16.8 Problems ................................................. 304
16.9 Solutions ................................................. 305

17 The Genetic Code ............................................. 307

17.1 Biology and Information Theory ......................................... 308
17.2 History of Genetics ........................................... 308
17.3 Structure of DNA ............................................. 309
17.4 DNA as an Information Channel .......................................... 309
17.5 The Double Helix, Replication ............................................ 310
17.6 Protein Synthesis and the Genetic code .................................... 310
17.7 Viruses ..................................................... 312
17.8 Entropy and Compression in Genetics ..................................... 313
17.9 Channel Capacity of the Genetic Code ..................................... 314

III Error-Correction ................................................. 317

18 Error-Correction, Haddamard, Block Designs ............................ 319

18.1 General Ideas of Error Correction ......................................... 319
18.2 Error Detection, Error Correction ......................................... 320
18.3 A Formula for Correction and Detection .................................... 321
18.4 Hadamard Matrices ............................................. 322
18.5 Mariner, Hadamard and Reed–Muller ....................................... 325
18.6 Reed–Muller Codes ............................................. 325
18.7 Block Designs ................................................. 326
18.8 A Problem of Lander, the Bruen–Ott Theorem ............................. 328
18.9 The Main Coding Theory Problem, Bounds ................................ 328
18.10 Problems ................................................... 333
18.11 Solutions ................................................... 333
CONTENTS

19 Finite Fields, Linear Algebra, and Number Theory 335
  19.1 Modular Arithmetic ........................................... 335
  19.2 A Little Linear Algebra ...................................... 339
  19.3 Applications to RSA ........................................... 341
  19.4 Primitive Roots for Primes and Diffie–Hellman .......... 342
  19.5 The Extended Euclidean Algorithm ......................... 345
  19.6 Proof that the RSA Algorithm Works ....................... 346
  19.7 Constructing Finite Fields ................................. 346
  19.8 Pollard’s $p - 1$ Factoring Algorithm .................... 350
  19.9 Turing Machines, Complexity, P and NP ................. 351
  19.10 Problems ...................................................... 354
  19.11 Solutions ..................................................... 355

20 Introduction to Linear Codes 359
  20.1 Repetition Codes and Parity Checks ....................... 359
  20.2 Details of Linear Codes .................................... 361
  20.3 Parity Checks, the Syndrome, Weights .................... 364
  20.4 Hamming Codes, an Inequality ............................. 366
  20.5 Perfect Codes, Errors and the BSC ......................... 367
  20.6 Generalizations of Binary Hamming Codes ................ 368
  20.7 The Football Pools Problem, Extended Hamming Codes .... 369
  20.8 Golay Codes .................................................. 370
  20.9 McEliece Cryptosystem ...................................... 371
  20.10 Historical Remarks ........................................ 372
  20.11 Problems .................................................... 373
  20.12 Solutions ................................................... 375

21 Linear Cyclic Codes, Shift Registers and CRC 379
  21.1 Cyclic Linear Codes ......................................... 379
  21.2 Generators for Cyclic Codes ............................... 381
  21.3 The Dual Code and The Two Methods ...................... 383
  21.4 Linear Feedback Shift Registers and Codes ............. 384
  21.5 Finding the Period of an LFSR ............................ 386
  21.6 Cyclic Redundancy Check (CRC) ............................. 387
  21.7 Problems ..................................................... 388
  21.8 Solutions ..................................................... 390

22 Reed Solomon, MDS Codes, Bruen-Thas-Blokhuis 393
  22.1 Cyclic Linear Codes and Vandermonde ..................... 394
CONTENTS

22.2 The Singleton Bound .......................................... 396
22.3 Reed–Solomon Codes ............................................. 397
22.4 Reed–Solomon Codes and the Fourier Transform Approach ............... 398
22.5 Correcting Burst Errors, Interleaving ................................ 399
22.6 Decoding Reed–Solomon Codes .................................... 400
22.7 An Algorithm for Decoding and an Example ............................ 403
22.8 MDS Codes and a Solution of a Fifty Year-Old Problem ................. 405
22.9 Problems ................................................................ 408
22.10 Solutions ............................................................... 408

23 MDS Codes, Secret Sharing, Invariant Theory 411

23.1 General MDS Codes .................................................. 411
23.2 The Case \( k = 2 \), Bruck Nets ...................................... 412
23.3 Upper Bounds on MDS Codes, Bruck-Ryser ............................. 414
23.4 MDS Codes and Secret Sharing Schemes ............................. 416
23.5 MacWilliams Identities, Invariant Theory ............................. 417
23.6 Codes, Planes, Blocking Sets ....................................... 418
23.7 Binary Linear Codes of Minimum Distance 4 ........................ 422

24 Key Reconciliation, New Algorithms 423

24.1 Symmetric and Public Key Cryptography .............................. 423
24.2 General Background ................................................... 424
24.3 The Secret Key and the Reconciliation Algorithm ...................... 426
24.4 Equality of Remnant Keys: the Halting Criterion ...................... 429
24.5 Linear Codes: the Checking Hash Function ........................... 431
24.6 Convergence and Length of Keys .................................... 433
24.7 Main Results ................................................................ 438
24.8 Some Details on the Random Permutation .............................. 439
24.9 The Case Where Eve Has Non-zero Initial Information ............... 441
24.10 Hash Functions Using Block Designs .................................. 442
24.11 Concluding Remarks .................................................. 443

ASCII 445

Shannon’s Entropy Table 447

Glossary 449

Bibliography 454
CONTENTS

Index

xiii

462
Preface

It is our privilege and pleasure to welcome all our readers to the dynamic world of cryptography, information theory and error correction. Both authors have considerable industrial experience in the field. Also, on the academic side Dr. Bruen has been a long-time editor of leading research journals such as "Designs, Codes and Cryptography". Prior to his appointment in Calgary he worked in mathematical biology at Los Alamos. The book is an outgrowth both of presentations to industry groups and of a lecture course at the University of Calgary. The course was for undergraduate and graduate students in Computer Science, Engineering and Mathematics.

In addition to the academic topics in that course, we also include material relating to our industrial consulting work and experience in writing patents on the topics in the title of the book. In particular we describe revolutionary new algorithms in chapter 24 for hash functions and symmetric cryptography including quantum cryptography. These have been patented and have already made their way into industry.

This book can be read at many different levels. For example, it can be used as a reference or a text for courses in any of the three subjects or for a combined course. To this end we have included over three hundred worked examples and problems, with answers or solutions as needed. But we were determined to make the work highly accessible to the general reader as well. We hope that the exposition fulfills this goal. Large sections of this book have been written in such a way that little is required in the way of mathematical background. In places this was difficult to do but we believe that the effort has been worthwhile.

The three topics become more and more entwined as science and technology develop. In our opinion, the time when the three topics can be treated in isolation is rapidly drawing to a close. For example, if you search the internet for cryptographic information it is more and more likely that you will run up against terms such as entropy, CRC checksums, random number generators and the like. [Digressing: the main undergraduate course in computer science which is concerned with data structures — and we have all taught it — covers Huffman codes and compression at length but the word entropy is never mentioned. This is a shame].

Thus it seemed quite appropriate to us to try to write a complete but highly accessible
account of the three subjects stressing, above all, their interconnections and their unity. These interconnections can be hidden if one relies only on separate accounts of the three subjects. In addition, as part of information theory, we discuss some potential applications in cell biology. In the last chapter we present some new, exciting algorithms which combine all three of the subjects.

This is not the first time that a book combining the three subjects has been attempted. Several very good recent books, specializing in cryptography, have a few chapters on the other subjects. But our goal was to give a full in-depth account. We should mention that other books have handled nicely two of the three topics. A splendid book, published in 1988 by Dominic Welsh gives an account of all three of the subjects. However, a lot has happened since 1988. Also, our focus, emphasis and level of detail is different.

Let us briefly explain the 3 subjects.

**Cryptography.** This is an ancient subject concerned with the secret transmission of messages between two parties denoted by A and B. This could be done if A, B shared a secret language, say, not known to outsiders. More generally they can communicate in secret by sharing a common secret "key". Then A uses the key to scramble the message to B, who unscrambles the message with a copy of the same key that is owned by A. We may think of military commanders sending secret messages to each other or home movie providers sending movies to authorized customers. Apart from secrecy there are also crucial questions in cryptography involving authentication and identification.

**Information Theory.** This subject, also known as Shannon Theory after Claude Shannon, the late American mathematician and engineer, gives precise mathematical meaning to the term "information". This leads to answers to such questions as the following:

- How much compression of data can be carried out without losing any information?
- What is the maximum amount of information that can be transmitted over a noisy channel?

This fundamental question is answered precisely in Shannon's famous channel capacity theorem which was discovered around 1948.

**Error Correction.** We introduce redundancy ["good redundancy"] for the transmission of messages, as opposed to the "bad redundancy" which was banished using compression. In this way we try to ensure that the receiver decodes accurately within the bounds of the Shannon capacity theorem mentioned in the previous section. The wonderful pictures of far-away planets, that have recently been made available, are just one example of what error-correcting codes can do. With a modern modem we can both compress as well as encode and decode to any required degree of accuracy.
Interconnections. These are spelled out in detail in the text but let us give a few short informal connections. How secure is your cryptographic password? It depends on how hard it is to guess it, i.e. it depends on its entropy as measured in Shannon bits. We then need information theory to properly discuss this.

In cryptography, A is sending information in secret to B, but what exactly is information and how is it measured? Again we need information theory.

Suppose that A is sending a secret key K over a channel to B in order to encrypt, at some future date, a secret message M with K and transmit it to B. Now, a basic property of K is this. If the transmission of K is off by even one bit then B will end up with a message that is completely different from the intended message M. The bottom line is that a transmission error could be catastrophic. The best way to guard against this is for A to use robust error-correction when sending the cryptographic key K to B.

The great Claude Shannon made the following fundamental point. In error-correction, the receiver B is trying to correctly decode what the transmitter A has sent to B over a "noisy channel". Compare this to the cryptographic situation where A is sending secret messages to B. They must contend with the eavesdropper — the evil Eve — who is listening in. We can think of Eve as receiving a "noisy" version of M and trying to decipher, or decode M. We are back to coding theory. [Parenthetically, we mention that Shannon designed an interesting theory of the stock market by regarding the market as a very noisy channel!].

We must point out that this point of view of Shannon is extremely useful and not just as a formal device. We drive the point home with several problems in Chapter 16 where the analogy becomes quite striking. Moreover, in Chapter 24, A and B and Eve may have the same information to start out with, yet A and B have to come up with a way of beating Eve and publicly generating a secret key using a technique known as “Privacy Amplification”.

Here is yet another basic interconnection. Random numbers and pseudo-random numbers are the work-horses of cryptography, especially symmetric cryptography. One of the best ways of generating them is with shift-registers. In fact, as is pointed out in Schneier [Sch96], “stream ciphers based on shift registers have been the workhorse of military cryptography since the beginning of electronics”. But shift registers are central in information theory as they are great proving-grounds [or grave-yards] for questions on entropy. To understand entropy you have to confront shift registers. But — and here is the astonishing part — these shift registers, over any field, correspond exactly to cyclic linear codes which are at the heart of error-correction. For the expert, Reed–Solomon codes, and not just their error-correction, are merely special kinds of shift registers in disguise!

We move on now to a more conventional-type preface and address some standard questions.

Intended Readership. This is a book for everyone and can be used at many different levels. We are writing for many different kinds of readers.
1. All-rounders or renaissance types who have taken some mathematics or computer science or engineering [or none of the above] and who want to find out about these topics and have some fun.

2. Undergraduates or graduate students in mathematics, computer science or engineering.

3. Instructors of algebra and linear algebra who would like some real life practical applications in their courses, such as shift registers.

4. Biologists who may be interested in our discussions of such topics as biological compression and the channel capacity corresponding to the genetic code.

5. IT workers, venture capitalists and others who want an overview of the basics.

6. Academics looking for a good source of important (and doable) research problems.

7. Philosophers and historians of science who want to move on from quantum theory and relativity to a new, practical area which also, incidentally, has strong connections to quantum mechanics.

**Rewards for Readers.** If you make a good effort at understanding this book and working out some of the problems you will be well rewarded. This book covers everything you need. In particular, you will elevate your skills and mathematical maturity to a new level. You will also have an excellent background — better than that of most practitioners — in these areas. You will be ready to think about a career in cryptography or codes or even information theory. The market, especially in such areas as data compression is hot. You will be very well-placed for advanced work in cryptography, error-correction or information theory.

**Our Goals.** We want to help develop your skills and inspire you to new heights. Let this book be your inspiration. Master it and then get out and write those patents!

**Possible Courses Using this Book.** There is more than enough material for a stand-alone course at the undergraduate or graduate levels, in any of the three areas. The extensive list of problems and worked examples will be a big help. For those few chapters that don’t have problems there are opportunities for many fun group-projects geared towards reporting on patents, publications etc. We would recommend some “poaching” among the three parts of the book in such a course. A one year combined course would also work well.

**A Course for Non-Specialists.** Most of Part I, apart from the Chapter on elliptic curves, requires very little mathematical background but covers a lot of ground in cryptography. In information theory, we highly recommend Chapter 10 which gives a panorama of information theory and interesting related topics such as the “MBA problem” on weighings. The chapter
on topics related to the genetic code does not require much background, and should be of considerable interest. We also recommend Chapter 18 introducing coding theory. Chapter 20 tells the amazing story of how the famous perfect Golay code $G_{11}$ was first published in a Finnish soccer magazine in connection with the football pools in that country. Chapter 24 describes what appears to be a breakthrough in symmetric cryptography, error correction, and hash functions. We highly recommend it!

**Level, Mathematical Style, Proofs, Exercises.** We have made a considerable effort to ensure that the chapters are as accessible as possible. In terms of style, our motto, which is the opposite of many mathematicians and engineers, is this: “Never use a symbol if you can get away with a word.”

What about proofs? It really depends. If the proof enhances the ideas we try to present it. Also, some results, such as the Shannon source-coding result are so astonishing that we have to give the details. However, in the case of the noisy channel theorem we have a different approach. From teaching, we found it considerably more effective to give five or six different approaches rather than to just give the standard official proof.

This book was not written just for theoreticians. Much of our time was spent in designing good problems and solution. We urge our readers to take advantage of them.

**Mathematical Prerequisites.** Honestly? We try to cover everything “on the fly” along with one special chapter on specialized topics but here is a short summary of what we need.

- **Calculus:** a small amount having to with the concavity of a graph [second derivative] and function maxima [first derivative, end points].
- **Linear algebra:** Multiplying matrices, subspaces, invertibility and determinants.
- **Elementary probability and statistics:** Mean and variance, Bernoulli trials, the normal curve, law of large numbers.
- **Algebra:** A small amount of material on groups, finite fields, modular arithmetic.

Here and there we go over the top. For example, a bit of Fourier analysis for the Shannon sampling theorem is needed. But generally speaking, the above list covers most of the material and we do discuss the needed background as we go along.

**What’s New.** Most of the Chapter have a “New, Noteworthy” heading where we try to summarize such matters. However, here is a brief summary of “what’s new” in the book. The topics are listed in no particular order.

- An in-depth integrated discussion of cryptography, information theory and error-correction emphasizing their interconnections, including new, clear, accessible proofs of major results, along with new results.
• A discussion of RSA that clears up several issues and shows how, for example, a given encryption index may have several decryption indices: Also, an indication of a possible new attack on RSA.

• A study of potential applications of information theory in cellular biology.

• An overview of important practical considerations in modern cryptography and communication theory.

• A whole new treatment of “perfect secrecy”, including a refutation of the standard assertion concerning the equivalence of perfect secrecy and the one-time pad, together with a proof of the equivalence of perfect secrecy and Latin squares.

• A highly accessible summary of information theory and its applications for non-specialists.

• A detailed look at hash functions from the point of view of linear codes.

• A detailed discussion of shift registers in cryptography, information theory and error correction including several new results and their application to the Berlekamp–Massey theory of Reed–Solomon and BCH decoding.

• A clarification of several points of confusion in the literature relating to security.

• A presentation of five different approaches to Shannon’s noisy channel theorem.

• A detailed discussion of the sampling theorem and Shannon’s fundamental band-limited capacity formula to the effect that $C = B \log \left(1 + \frac{S}{N}ight)$, using precise statistical and geometrical techniques.

• A look at some of the history of cryptography and coding theory including a brief biography of Claude Shannon and an account of the original discovery of the Golay code in a Finnish soccer-pools magazine.

• A description of invariant theory and combinatorics applied to coding theory with particular reference to “the computer algebra theorem of the twentieth century” i.e. the nonexistence of a plane of order 10 and related work of one of the authors.

• Connections between MDS codes, secret-sharing schemes, Bruck Nets and Euler’s “famous problem of the 36 officers”.

• A brief description of research work due to the author and two co-authors solving, in the main, the fifty year old problem of finding the longest MDS code.

• A streamlined approach to Reed–Solomon codes via MDS codes.
• A highly accessible account of the decoding of Reed–Solomon codes.

• A major breakthrough in symmetric (and quantum) cryptography using some new research due to the authors and David Wehlau: the work has been patented and is being used in industry.

Missing Topics. We seem to have covered all the essential topics. We meant to discuss convolutional codes but ran out of space. But they can be covered from the shift register point of view and feed back shift registers have been covered in considerable detail. We also wanted to put in some computer code. We plan on putting some on the website if there is a demand for it.

Professional Acknowledgements. First of all we would like to thank Ted Bisztriczky, Marguerite Fenyvesi and the Department of Mathematics at the University of Calgary, for their support. Richard K. Guy has offered wise counsel and mathematical erudition. We are very grateful to Joanne Longworth, Department of Mathematics for her typing and editorial work including the diagrams. In the same vein we want to thank Dr. Guo of the CPSC department. Richard Cannings was a major catalyst for our involvement with industrial cryptography. Thank you Richard. We also thank, in a similar way, Gerald Stariula for getting us involved and sharing important ideas with us. Dr. David Wehlau has already been acknowledged in Chapter 24. The late Gian Carlo Rota of MIT had a major positive influence and encouraged us to write the book. Professor Bruce Rothschild has been a major source of help and inspiration. The first author would like to thank his brother, Bernard Bruen of New York for his help. He also thanks his sister-in-law, Margit Veldi, an IT worker in Montreal for valuable consultations. Rachael Bevan Bruen kindly supplied important biological insights. Prof Keith Nicholson deserves our gratitude as does the Wiley editorial staff including Susanne Steitz, Steve Quigley and Danielle Lacourciere.

We come to the students-Apichart Intrapanich, Eric Lenza, Reza Pasand, Dave Richardson, Zoron Rodiguez, Paul Tarjan and Feng Zhang. The book could not have been written without their help. In particular, Eric and Paul made new mathematical discoveries which have been included in the book. They also constructed first drafts of chapters. In addition, along with Dave and Zoron they cheerfully criticized, re-drafted, corrected and proof-read. Our thanks to all.

Other friends and colleagues to whom we are grateful include David Torney, Bob Davis, Jose Rueda, Chris Fisher, Tim Alderson, and Richard Biggs who write chapter 5.

Personal Acknowledgements. For some personal acknowledgements, the first author would like to thank his loving wife Katri Veldi, their three children [Trevor, Robin and Merike] and Trevor’s wife Rachael for their love and support. He would also like to mention
his siblings, Phil, Antoinette and Bernard, and their spouses. The book is also partially
dedicated to the memory of his late parents, Edward A Bruen and Bríd Bean de Brún.

The second author would like to thank his beloved wife Claudia Martinez for all her
support and the many hours of patient typing of early versions of Part I and their son
Dante for contributing a daily dose of joy. The book is also partially dedicated to his
parents Alberto Forcinito and Olga Swystun de Forcinito.

Book Website, Corrections. We will maintain a website for the book at


We have done our best to correct the errors but, inevitably, some will remain. We invite our
reads to submit errors to mario@SURengineering.com We will post them, with attribution,
on the website.

About the Authors. Aiden A. Bruen was born in Galway, Ireland. He read mathematics
for his Undergraduate and Master’s degree in Dublin. He received his doctorate at the
University of Toronto, supervised by F. A. Sherk. At Toronto he also worked with H. S. M.
Coxeter, E. Ellers and A. Lehman. He is a Professor of Mathematics and Statistics at the
University of Calgary.

Mario A. Forcinito was born in Buenos Aires, Argentina where he took his Bachelors
degree in Engineering. He obtained his doctorate in Engineering at the University of Calgary
under the supervision of M. Epstein. He is an industrial engineering consultant in Calgary.

Update. New results are constantly being obtained. As this book was going to press, it
was reported in the Toronto Globe and Mail that “encryption circles are buzzing with news
that mathematical functions embedded in common security applications have previously
unknown weaknesses”.

In particular, the report cites security vulnerabilities, discovered by E. Biham and R.
Chen of the Israel Institute of Technology, in the SHA-1 hash function algorithm. SHA-1 is
used in popular programs such as PGP and SSL and is considered the “gold-standard” of
such algorithms. Certified by NIST (the National Institute of Standards and Technology)
it is the only algorithm approved as a Digital Signature Standard by the US government.

In Chapter 24 we discuss the construction of hash functions from error-correcting codes.
Dedications

Dedicated to my beloved wife Katri and to the memory of my late parents, Edward A Bruen and Bríd Bean de Brún (AAB)

Also dedicated to my beloved wife Claudia and to my parents, Alberto Forcinito and Olga Swystun de Forcinito (MAF)
Part I

Mainly Cryptography
Chapter 1

Historical Introduction and the Life and Work of Claude E. Shannon

Goals, Discussion We present here an overview of historical aspects of classical cryptography. Our objective is to give the reader a panoramic view of how the fundamental ideas and important developments fit together. This overview does not pretend to be exhaustive but gives a rough time line of development of the milestones leading to modern cryptographic techniques. The reader interested in a complete historical review is advised to consult the definitive treatise by Kahn [Kah67].

Following this we discuss the life and work of Claude Shannon, the founding father of modern cryptography, information theory and error correction.

1.1 Historical Background

Cryptology is made up of two Greek words: kryptos, meaning “hidden,” and ology, meaning “science.” It is defined in [Bri97] as the science concerned with communications in secure and usually secret form. It encompasses both cryptography (from the Greek graphia meaning “writing”) and cryptanalysis, or the art of extracting the meaning of a cryptogram.

Cryptography has a history that is almost as long as the history of the written word. Some four millennia ago (see [Kah67] p. 71) an Egyptian scribe recorded in stone the first known hieroglyphic symbol substitution in the tomb of Khnumhotep II, a nobleman of the time. Although the intention in this case was to exalt the virtues of the person, rather than to send a secret message, the scribe used for the first time one of the fundamental
elements used by cryptographers throughout the ages, namely, substitution. He used unusual hieroglyphic symbols, known perhaps only to the elite, in place of the more common ones.

In substitution, the sender replaces each letter of a word in a message by a new letter (or sequence of letters or symbols) before sending the message. The recipient, knowing the formula used for the substitution—the secret key—is able to reconstruct the message from the scrambled text that is received. It is assumed that only the recipient and the sender know the secret key.

The other main cryptographic technique used is transposition (or permutation), in which the letters of the message are simply rearranged according to some prescribed formula that would be the secret key in this case.

The Greeks were the inventors of the first transposition cipher. The Spartans [Kah67], in the fifth century B.C. were the first recorded users of cryptography for correspondence. They used a secret device called a scytale consisting of a tapered baton around which was spirally wrapped a strip of either parchment or leather on which the message was written. When unwrapped, the letters were scrambled, and only when the strip was wrapped around an identically sized rod could the message be read.

Today, even with the advent of high-speed computers, the principles of substitution and transposition form the fundamental building blocks of ciphers used in symmetric cryptography.

To put it in a historical perspective, asymmetric or public key cryptography was not invented until the 1970s. Exactly when it was invented, or who should take most of the credit, is an issue still in dispute. Both the NSA¹ and the CESG² have claimed priority in the invention of public key cryptography.

Cryptography has had several reincarnations in almost all cultures. Because of the necessity of keeping certain messages secret (i.e. totally unknown to potential enemies) governments, armies, ecclesiastics, and economic powers of all kinds have been associated throughout history with the development of cryptography. This trend continues today.

The Roman general Julius Caesar was the first attested user of substitution ciphers for military purposes ([Kah67] p. 83). Caesar himself recounted this incident in his Gallic Wars. Caesar found out that Cicero's station was besieged and realized that without help he would not be able to hold out for long. Caesar had a volunteer ride ahead with an encrypted message fastened to a spear, which he hurled into the entrenchment. Basically, Cicero was told to keep up his courage and that Caesar and his legions were on their way.

In the cipher form used by Caesar, the first letter of the alphabet "A" was replaced by the fourth letter "D", the second letter "B" by the fifth, "E", and so on. In other words, each original letter was replaced by a letter three steps further along in the alphabet. To

¹United States National Security Agency
²Britain's Communications Electronics Security Group