

Review of
**CODING THEORY AND CRYPTOGRAPHY: The Essentials, Second Edition,
Revised and Expanded** ¹
**Authors: D.R. Hankerson, D.G. Hoffman, D.A. Leonard, C.C. Lindner, K.T. Phelps,
C.A. Rodger, J.R. Wall**
**Series: Pure and Applied Mathematics, Volume 234
Marcel Dekker, 2000**
Hardcover, x + 350 pages, \$85.00 from the publisher
Reviewer: Robert J. Irwin

1 Overview

It is pretty much taken for granted that data storage and communication are *reliable*. Increasingly, we expect — or hope — that our recorded and transmitted data are *secure*. The theories of coding and cryptography attend to data reliability and security, respectively. Students interested in coding theory are likely also to be interested in cryptography, and vice-versa. Moreover, there is considerable overlap in the mathematical background required to study the two subjects. Given these strong pragmatic ties, it would be a great boon if one could buy a single text suitable for learning both subjects and still get change back from one's \$100 bill.

The book under review is a new and expanded edition of an introductory coding theory text by six of the seven above-named authors [1], all of Auburn University at the time the text was written. The biggest change from the previous edition is the addition of an introduction to cryptography following the text's more extensive coverage of coding theory. Other recent works have covered coding theory and cryptography in one volume, too [4, 5]. I'll say more about them later.

2 Summary of Contents

The book is divided into two parts. Part I: Coding Theory comprises the bulk of the text, nine of its twelve chapters. This part has been used to provide material for a two-semester sequence in coding theory at Auburn for students having at least a “rather elementary knowledge of linear algebra.”. Linear block codes predominate, as one would expect, though an entire chapter is devoted to convolutional codes. Part II: Cryptography presents a short introductory course in that subject. The septumvirate of authors wrote the second part for a “diverse audience of graduate and undergraduate students from computer science, engineering, education and mathematics, some of whom will have had only an introductory course in algebra or number theory at the sophomore level.” This is a mighty broad readership to serve, one that reflects burgeoning general interest in matters cryptological.

2.1 Part I: Coding Theory

As the subtitle indicates, coverage really does stick to the basics. Most of the required mathematics is administered in small doses, just before being applied, so as not to overwhelm weaker hosts. Unutilized mathematical generality is avoided.

The clearly written introductory chapter presents the paradigmatic communication-over-noisy-channel schema and provides some basic information theoretic definitions (pithy quote: “The most important part of the diagram, as far as we are concerned, is the noise, for without it there would

¹©Robert J. Irwin, 2003

be no need for the theory.”). The idea of encoding a message to permit error detection is introduced and the maximum likelihood method (MLD) advanced for decoding with error correction. MLD is then analyzed for reliability on a few simple codes chosen to yield mixed results, thus illustrating and prompting further discussion of criteria for code selection.

The first chapter also establishes the loose definition-theorem-proof format used throughout the text. Most sections begin with a few key definitions which are immediately followed by examples. Similarly, examples and exercises accompany most theorems and algorithms, so that students see codes in action straightaway. Theorems, proofs, algorithms and examples are clearly marked. Definitions are not similarly distinguished, though first uses of new terms are italicized in the narrative and referenced in the index. Overall, the presentation style is relaxed and informal, occasionally enlivened by brief chatty interludes. The text is not at all dry.

After the deft set-up, the authors go to work presenting various families of codes, beginning with a chapter introducing simple linear codes, and the vector space concepts needed to understand their properties. Then Hamming bounds and perfect codes are explored, including Hamming and Golay codes. Extended Golay and Reed-Muller codes are also discussed. Cyclic linear codes are next, following a brief review of polynomials over fields of characteristic 2.

Other important code families are studied, to wit: BCH (Bose-Chaudhuri-Hocquenham; this family includes the Reed-Solomon codes, which are covered in a separate chapter), Burst Error-Correcting, Reed-Muller and Preparata. Occasionally, practical applications of particular code families are mentioned to hold interest. Additional facts about finite fields and polynomials are provided when and as needed — often without proof, however, as by way of review. Combinations of encodings are also discussed, such as the use of Reed-Solomon with convolutional codes for space communications, or using burst error-correcting methods in conjunction with other codes.

Over 300 exercises are provided, many of which offer the kind of drill undergraduates need to test their understanding. Full or partial solutions to almost half of them are given in an appendix.

Overall, the narrative and examples of Part I, such as the extended example of Reed-Solomon-based compact disc encoding, present the highlights of the subject neatly, and the reader is usually alerted to simplifications made and real-world details omitted. Uniformity of tone and structure are maintained within this part remarkably well for a work with seven authors.

2.2 Part II: Cryptography

Cryptography is covered in three chapters spanning 80 pages altogether. Right away, one notices that Part II is distinct from Part I, aside from subject matter. For example, only the cryptography chapters offer footnotes and end-of-chapter remarks. The edifying and amusing footnotes provide intriguing historical tidbits, often about cryptological embarrassments, that give the reader a satisfying “clued-in” feeling. Chapter end notes provide a useful guide to the bibliography — over three quarters of its 105 entries concern cryptography.

“Classical Cryptography,” the lead-off chapter, briskly defines the field and its major application areas: confidentiality, message and sender authentication, message integrity, and non-repudiation. Here, the general communication-with-encryption scenario is limned, the basic vocabulary used in the sequel provided, and a sequence of secret- or symmetric-key encryption schemes is presented. The usual path is taken, starting with simple substitution ciphers and progressing through polyalphabetic block ciphers (the Vigenère cipher) and stream ciphers (the Vernam, or one-time pad cipher), and ending with Feistel ciphers and the Data Encryption Standard (DES). The different flavors of security (unconditional, computational and provable) are informally discussed and Kerckhoffs’s principles for selecting ciphers are considered. The one-time pad cipher is given as an example of an unconditionally secure encryption system per Shannon’s criterion, which is not

rigorously defined, though a reference is provided.

In contrast to the “just in time” approach of the first part, most of the cryptological mathematics expected to be unfamiliar to readers is introduced in a dedicated chapter, “Topics in Algebra and Number Theory.” Here, the groundwork is laid for public-key cryptography in 25 pages unrelievedly devoted to higher arithmetic. Topics include the integers modulo n , quadratic residues, primality testing, factoring and square roots, and discrete logarithms. Complexity matters are briefly, and informally, addressed.

The final chapter, “Public-key Cryptography,” introduces readers to asymmetric encryption schemes. After preliminaries on one-way/trapdoor functions and hashes, the RSA cryptosystem is introduced. Careful mention is made of the fact that, while RSA is based on the difficulty of factoring, it is not known to be equally difficult, nor is factoring itself known to be intractable (intractability is not formally defined in the text). Rabin’s related public-key scheme is then given and its difficulty is shown to be closely tied to that of factoring. The ElGamal encryption scheme, based on the unproven intractability of the discrete logarithm problem rather than on factoring, comes next. Applications of public-key cryptography to digital signatures and non-repudiation are covered. The text proper ends with a discussion of several cryptographic protocols: Diffie-Hellman key agreement, zero-knowledge proofs, coin-tossing and mental poker.

Around 80 exercises appear in Part II; a good mix of drill and more substantial problems, often with references. As for Part I, almost half are fully or partially solved in an appendix.

3 Opinion

The authors have made a fairly good read of the coding theory part, which cannot hope to compete with the inherent cloak-and-dagger cool of the cryptography part. They clearly took pains to make the former subject as painless as possible, if at the expense of fuller disclosure. There is more than a semester’s worth of coding theory material here, up to a year assuming the instructor fills in some gaps. Sharper coverage of which codes are best for particular applications would help the engineering and computer science majors for whom the text seems most suited.

While a bit of linear algebra is cited by the authors as the “minimal prerequisite” for undertaking a coding theory course based on their text, students familiar with discrete probability and the algebra of finite fields will be *much* the happier for it; the book is not self-contained with respect to these subjects. Perhaps the doughty, if under-prepared, reader could orient himself from context, but, e.g., the line “...one which utilizes *Galois fields* [italics added] $\text{GF}(2^r)$.” may appear as though dropped from a helicopter.

Though compact, Part II provides a good selection of essential results in cryptography, in some cases without proof. A short course could be based on this part, but supplemental material would be needed for a full semester course, especially one for graduate students. Too often, the text would have the reader resort to Kahn’s famous techno-history [2] or Stinson’s popular text [3] for fuller examples and proofs. Combined coding theory/cryptography courses, long or short, could be taught from this text. However, its two parts are so completely independent of one another that an instructor seeking a more unified treatment of these subjects should look elsewhere.

The bibliography, while clearly not intended to be complete, is select. It contains considerably more, and more up-to-date, entries for cryptography than for coding theory. Some cryptography entries refer to good expository material held in on-line reports and special proceedings as well as to standard texts and research papers. As to matters of production, the book’s layout is clear and its typography unobtrusive. Such misprints as I detected seemed relatively benign and correctable from context.

I promised further word on the competition. The recent text of Trappe and Washington [4] also covers both coding theory and cryptography, but with the emphasis reversed: 2 chapters comprising about 80 pages are devoted to information and coding theories, with the remainder of this longer text given over to cryptography. Many of the families of error-correcting codes discussed in the text under review are also covered in [4]; convolutional codes, however, are omitted. Trappe and Washington's coverage of cryptography and its applications is much broader than that of Hankerson, et al, including, for example, entire chapters devoted to e-commerce and digital cash, elliptic curves, and quantum cryptography. Overall, [4] is more self-contained mathematically, providing introductory material on finite fields and a brief review of discrete probability (it is less self-contained where vector space theory is concerned, however). The two authors link up coding theory and cryptography via the McEliece cryptosystem, based on the difficulty of finding the nearest codeword for a linear binary code.

Another book, not quite so recent, by Dominic Welsh [5] looks very promising (at the time of this writing I have not finished with it). This introductory text addresses more or less the same audience as those of Hankerson, et al, and Trappe and Washington, but it is more rigorous than either, and so better suited for graduate students or well-disciplined undergraduates, including mathematics majors. At 257 pages, this is the shortest of the texts mentioned, but by dividing coverage about equally between codes and cryptography, it includes more material on information and coding theory than [4], and more material on cryptography than the book under review. Welsh is mathematically forthcoming; e.g., information theory and complexity issues receive formal treatment. In fact, his text seems to be more of an information theory and cryptography book that includes a substantial amount of material on error-correcting codes. Shannon's approach to information theory, coding theory and cryptography is adopted from the outset, so this text provides a more unified treatment than the others. Given its length and balance, it may be an excellent choice for a one-quarter/semester combined course in coding theory and cryptography.

References

- [1] D.G. Hoffman, D.A. Leonard, C.C. Lindner, K.T. Phelps, C.A. Rodger, J.R. Wall. *Coding Theory: The Essentials*. Marcel Dekker, 1991.
- [2] David Kahn. *The Codebreakers: The Story of Secret Writing*. revised edition, Scribner, 1996
- [3] Douglas Stinson. *Cryptography: Theory and Practice*. CRC Press, 1995 (second edition, 2002)
- [4] Wade Trappe and Lawrence C. Washington. *Introduction to Cryptography with Coding Theory*. Prentice-Hall, 2002.
- [5] Dominic Welsh. *Codes and Cryptography*. Oxford U. Press, 1997.