Review of the book

"Codes: The Guide to Secrecy from Ancient to Modern Times"
by Richard A. Mollin
CRC Press, Taylor & Francis Group, 2005

ISBN: 1-584-884-703, 978-1-584-884-705

Kenneth J. Radke
Information Security Institute
Queensland University of Technology

1 Summary of the review

Mollin's *Codes: The Guide to Secrecy from Ancient to Modern Times* is an encyclopaedic work of a very high standard. The 704 page book encompasses the most widely known and used cryptographic codes throughout history up until 2004 (book published in 2005). More than merely a book that describes cryptographic codes, scattered throughout this book are pictures and biographies of key personnel responsible for progressing the world's knowledge and use of codes, as well as exercises and problems conveniently arranged in an appendix to assist readers who are creating courses that will reference this book.

2 Summary of the book

The table of contents, which is itself a very good overview of what the book contains, is four pages long, and hence has been left out of this review. The table of contents information is available on any website that sells this book.

The book, not including its appendices, may be broken down into four main areas:

1. Historical ciphers. Consuming the first 106 pages of the book, this section covers ciphers from antiquity through to the World Wars and from World War II up until the late 1970s.

2. Current cryptography. This section, contained in the next 124 pages, deals with block ciphers and their modes, stream ciphers, public key cryptography (PKC), RSA, digital signatures, and protocols.

3. Cryptographic issues and applications. The next 142 pages cover key management, message authentication codes (MACs), email, the World Wide Web, and wireless security. Smart cards, biometrics (one use of which may be in smart cards), quantum computing and quantum cryptography round out this section.

4. Non-Cryptographic issues. The final 91 pages of the main section of the book starts with definitions and discussions on the topical issues of cybercrime, hackers, and viruses. After this, information theory is outlined, which perhaps could have been introduced far earlier. Finally, after the basic topics of information theory and entropy, non-cryptographic codes such as error-correcting codes are discussed.

The appendices in general are quite substantial, and Appendices A through F are mainly focused on mathematical knowledge and tools. The information provided is comprehensive, from the basics of modular arithmetic, probability theory and set theory, through to more complex topics such as the Number Field Sieve and primality tests.

The last appendix, Appendix G, has a list of problems for each chapter of the book, which could be quite useful for review of content or for establishing a course utilising part or all of this book. There are also exercises for the mathematical content in the appendices. Unfortunately, no solutions, not even for a reduced set of the exercises, were found in the book, thereby substantially reducing the exercises' effectiveness as a self-review tool.

3 Style of the book

As already stated, this book resembles an encyclopaedia of knowledge about cryptography. This encyclopaedic quality is very powerful, since all the information is in the one place, with common threads, consistent symbols and nomenclature, and cross-referencing throughout. If there is a weakness, it is the weakness of all encyclopaedia and that is that whilst all topics are covered, and covered quite well, clearly there is not the depth of detail in each section that there would be in a 200 page book devoted solely to that specific topic.

The story-telling style of the book, written predominantly in the first person as if the author is speaking directly to the reader, most notably in the first 100 pages, will appeal more to the general non-fiction reader than an academic. There are many interesting facts and stories told (the author does describe them as stories), and frequent mini-biographies, often accompanied by a portrait, of the people throughout history who have shaped the topics being considered.

Although there are quite a few diagrams and figures, in certain chapters more visual aids would benefit the reader. For example, many protocols are outlined in words only, and mathematical concepts such as set theory are also only specified in words. Visual thinking readers will find themselves creating their own pictures while reading the book, to aid their understanding.

4 Would you recommend this book?

This is, without question, an excellent book. The range of topics covered, the extra information provided in the forms of cross-referencing, biographies, bibliographical sources, pictures, and diagrams, all contribute to making this book a very worthwhile acquisition. Furthermore, the depth of the knowledge, the provided mathematical background, and simply the correctness and consistency of symbols throughout (which is difficult enough in a single lecture, and hence presumably near impossible in a 700 page volume such as this book), all give indications of the quality and amount of work that has gone into this book.

If there are any concerns or weaknesses with the book, they may be identified in the book's strengths. Firstly, and this may be seen as only advantageous, the book provides significantly more than the title suggests. For example, no part of the title *Codes: The Guide to Secrecy from Ancient to Modern Times* suggests to the prospective buyer that ancient (non-secretive) languages, that no one now knows the meaning of, are going to be discussed. Similarly, no part of the title suggests that biometrics or error-correcting codes are going to be discussed.

Secondly, there is a wealth of anecdotes throughout the book, including mini-biographies, discussions, and examples of how cryptographic techniques have been used (not in the classic "here's how to use public key cryptography (PKC)" sense, but rather "Here's a story about how PKC was used in Nuclear Test Ban Treaty Compliance"), and quotes at the start of each topic. While these are all enjoyable and add to the reader's experience when reading the book, it would be interesting to see how much smaller, and hence quicker to read, the book would be if these additional aspects were removed. Some people may prefer a more condensed version of the book, containing just the salient points.

Finally, the greatest issue with the book is that it attempts to serve too many masters. The book itself, in the preface, states that it is a book for "the merely curious, as well as history-minded readers, amateur mathematicians, engineers, bankers, academics, students, those practitioners working in cryptography, specialists in the field, and instructors wanting to use the book for a text in a course". By trying to cater for so many different groups of people, even though this book will serve each group quite well, it is evident that this book is not the ideal reference for any of the individual groups of people. Particularly the emotive story style of the first 100 pages may not appeal to specialists in the field. At the other end of the scale, for first time users and students, certain topics are introduced at perhaps too fast a pace. Cases in point include that only one transposition cipher example is given, and then the book moves on to the next cipher; and the introduction to modular arithmetic concepts, which was very brief and non-visual (words only).

Therefore, the preeminent use of this book would be for situations where there is a group of people with a range of backgrounds, and the book becomes a reference text for the mixed group. It would be well suited for work teams, libraries (for companies, municipalities, and universities), and undergraduate cryptographic teams made up of a mixture of computer science, mathematics, and engineering students. In these cases, all readers will find this book very useful, and the book is probably the best book currently for the range of users.

The reviewer is a student at the Queensland University of Technology, Australia.