The Book Review Column[1]

by William Gasarch
Department of Computer Science
University of Maryland at College Park
College Park, MD, 20742
email: gasarch@cs.umd.edu

In this column we review the following books. They are all in cryptography!

1. **Cryptological Mathematics** by Robert Lewand. Reviewed by William Gasarch. The book is mostly about pre-RSA crypto. Is this topic worth covering? If so, is this the book to use? Alice and Bob debate his point.

2. **Data Privacy and Security** by David Salomon. Reviewed by Nick Papanikolaou. Despite the title this is also a textbook on cryptography. It covers pre-RSA, RSA, and also Steganography which is unusual.

3. **Cryptography: An Introduction** by V.V. Yaschenko, **Cryptanalysis of Number Theoretic Ciphers** by S.S. Wagstaff, Jr., **RSA and Public-Key Cryptography** by R.A. Mollin, and **Foundations of Cryptography, Vol. 1: Basic Tools**, by O. Goldreich. Jointly reviewed by Jonathan Katz. If you want to be able to tell a good crypto book from a bad one then you must read this review. The most common faults are (1) not being rigorous enough, and (2) really being a number theory text in disguise.

Books I want Reviewed

If you want a FREE copy of one of these books in exchange for a review, then email me at gasarchcs.umd.edu

Reviews need to be in LaTeX, LaTeX2e, or Plaintext.

Books on Algorithms

1. *Combinatorial Optimization: Packing and Covering* by Cornuejols.

2. *Algorithms: Sequential, Parallel, and Distributed* by Berman and Paul.

3. *Algorithms: Design Techniques and Analysis* by Alsuwaiyel.

Books on Complexity, Cryptography, and Combinatorics

1. *Complexity of Classification of Boolean Constraint Satisfaction Problems* by Creignou, Khanna, and Sudan.

2. *Elliptic Curves: Number Theory and Cryptography* by Larry Washington.

3. *Block Error-Correcting Codes: A Computational Primer* by Xambo-Descamps.

4. *Combinatorial Designs: Constructions and Analysis* by Stinson.

5. *Aspects of Combinatorics and Combinatorial Number Theory* by S.D. Adhikari.

Misc Books

1. *Algorithmic Learning in a Random World* by Vovk, Gammerman, Shafer.
2. *Domain Decomposition Methods– Algorithms and Theory* by Toseli and Widlund.
3. *Dynamic Reconfiguration: Architectures and Algorithms* by Vaidyanathan and Trahan.
4. *Semantic Integration of Heterogenous Software Specifications* by Martin Groβe-Rhode.
5. *Handbook of Computational Methods of Integration* by Kyther and Schaferkotter.

Review of[2]
Cryptological Mathematics
Author: Robert Lewand
MAA, 2000, $33.95, Softcover

Reviewer: William Gasarch

Alice has taught a course in crypto. Bob is going to teach one soon.
Bob: Alice, how much pre-RSA crypto do you do when you teach Crypto?
Alice: I go over Monoalphabetic substitutions (for example the Caeser Cipher where every letter is replaced by the letter shifted 3 places, mod 26), Polyalphabetic substitutions (for example, every odd placed letter is shifted by 1, every even placed letter is shifted by 5), Polygraphic substitutions (for example, there is a 3×3 matrix that is multiplied mod 26 by every block of 3 letters), the enigma code from WW II, and the 1-time pad.
Bob: Why do all that?
Alice: There are several reasons

1. They get good and motivated review of modular arithmetic, number theory, probability, statistics, and linear algebra.
2. They see the fallacy of thinking that just because your code was hard to come up with does not mean its hard to break (e.g., a random permutation of $\{a, \ldots, z\}$ can be easily broken with frequencey analysis).
3. They see that many codes that were thought unbreakable were eventually broken; this breeds a heathly skepticisim about current claims.
4. They see that historically crypto has been a tradeoff between how much information you must exchange over a secure line and how secure the code is. For example, the shift cipher requires very little information exchange ahead of time (just a number between 1 and 26), but is not secure, whereas the 1-time pad is unbreakable but needs massive amounts of data to be exchanged over a secure line.
5. (Continuing the above point.) Since the beginning of Crypto, perhaps 4000 years ago, there has been the need for a secure channel or a private meeting to exchange information initially. Public Key crypto offers a way to do crypto and not have this meeting. Hence it can be seen as the solution of a 4000-year old problem. Seeing it in this light really impresses the students about its importance.

6. If you know the pre-RSA material then the introduction of complexity (e.g. how much time it takes to crack a code) as a formal object of study is more striking in its importance and originality.

Bob: You speak in lists! But more importantly, yes, you've sold me. I will do lots of PRE-RSA crypto. Do you have a book to recommend?
Alice: Many crypto books have some of this material. But be warned of books written by people who understand the mathematics but don't quite get the computer science.
Bob: Do you have a book to warn me to stay away from.
Alice: Yes and No. I have just read *Cryptological Mathematics* by Robert Edward Lewand. There are some PROS and CONS.

The table of contents is available at
faculty.goucher.edu/blewand/cryptomath/description.htm

The first chapter is entitled *Monoalphabetic Substitution Ciphers*. This is when you (say) replace a by b, b by c, ..., y by z, and z by a. More complicated bijections are also allowed; however, you want to be able to describe them briefly. Sections 1.1, 1.2, 1.3, and 1.4 are on proof techniques and simple number theory. Section 1.5 is on additive ciphers, multiplicative ciphers, affine ciphers, and keyword ciphers. It is well written and interesting.
Bob: Is the fact that they spend most of the chapter on topics not in the title- is that a bad thing?
Alice: Its fine. Its hard to weave the needed math into the book as you're doing it. One can view this as teaching math of interest in a motivated way.
Bob: So, you recommend the book?
Alice: Not so fast. There are several problems with this chapter.
1) (Page 27) The cast of characters is introduced, and its *not* Alice and Bob and Eve!! Its Beth and Stephanie and Molly!! This was very disconcerting since they are replacing us!
Bob: They don't use Alice and Bob? But that is why we exist!!
Alice: Calm down Bob! Most books use Alice and Bob, so we'll be employed for a while. Now back to the book.
2) (Page 32) The discussion of Multiplicative Inverses mod 26 suggests trying all possibilities. This is fine for mod 26 but is bad for larger values of n. The author misses an oppurtunity to introduce the reader to issues of complexity.
3) (No particular page) A person who makes up a random permuation of $\{a, \ldots, z\}$ for his cipher may think that nobody can possibly crack it since the original permuation is random. But frequency attacks can easily crack such ciphers. There is a valuable lesson in this— a cipher may be able to be cracked by ways its creator never imagined. Hence statements about the security of a cipher have to made very carefully. This is an excellent point to make, which the author does not.

The second chapter is on Polyalphabetic Substitution ciphers. One example of this would be to use the cipher that shifts a letter by 2 on all letters in even places, and use ciphers that shift a letter 3 places on all letters in odd places. More complicated ones are described and used. This is useful in that it hides the frequency of letters (the author makes this point nicely). Sections 2.1, 2.2, 2.3, and 2.4 are on probability and combinatorics, which is needed for this chapter. Again this is a nice way to motivate these topics.

This chapter only has one problem. On page 96 it describes the index of Coincidence which can be used to tell if a code is monoalphabetic or polyalphabetic. If this index is close to 0.064 then the code is probably monoalphabetic. If this index is close to 0.038 then the code is probably not monoalphabetic.
Bob: What if the index is much bigger than 0.064? Inbetween the two numbers? Can that happen? What if the index is much smaller than 0.038?

Alice: Anyone reading the book would ask those questions. Yet the author does not address this point.
Bob: What's in the third chapter?
Alice: The third chapter is on Polygraphic Substitution ciphers. This is where you replace a block of text for another block of text. Section 3.1 introduces the idea. Section 3.2 is about matrices and linear algebra, which the student needs for this chapter. The rest of the chapter describes some systems and also how to crack them.

There is a nice summary of how to crack them on page 133.

There is a problem with the summary. Again he uses the Index of Coincidence. The claim is that if it is close to 0.65 then the code is monoalphabetic (this is true) and that one should

"try attacking the message using monoalphabetic (additive, multiplicative, keyword, and affine transformation)"

This is misleading. Frequency attacks are the best against monoalphabetic ciphers.
Bob: This is all fairly interesting pre-RSA crypto. But do they do RSA?
Alice: Yes. The fourth chapter is on RSA. Its a good exposition with many examples but has two very serious problems.

1. On page 155 they talk about how to calculate powers like $(78390)^{91025} \pmod{180577}$. They mention the sequential method and Mathematica routines, but they never mention repeated squaring!

2. On page 157 they state

   "So the RSA algorithm is as secure as the unfactorability of n"

   This is *not* known to be true. It is known that if factoring was easy then RSA would be breakable. The converse is not known. It is possible that some clever other method may emerge that cracks RSA without factoring. Note that we can test for primality without being able to factor, which would seem counter-intuitive except that we are all used to it.

Bob: Does he mention that there are attacks on the **implementation** of RSA, such as timing attacks?
Alice: Ah, good question. No he does not.
Bob: Well... how important is that for an undergraduate text?
Alice: I think its very important! When I first read about timing attacks it blew my mind! It showed the limits to mathematical proofs of security when dealing with the real world.
Bob: What else is in the book?
Alice: The book has short biographies of four prominent people involved with the origin of crypto: Herbert Yardley, William Friedman, Agnes Meyer Driscoll, and Frank Rowlett. The book also has a very nice Taxonomy of terms used in Crypto.
Bob: What else do they leave out?
Alice: They do not discuss the 1-time pad or issues of key length in general. This is a bad omission since it sets the stage for RSA. They also do not discuss Kerchhoffs's law, which is that you should assume the enemy knows what system you are using.
Bob: At the end of the day, do you recommend this book?
Alice: That is a more profound question than you realize. On the one hand, the book is well written and introduces math of interest in a motivated and fun way. On the other hand, its wrong on some points (though not that many) and misses opportunities at other points. How important is that? Do the PROS outweight the CONS?

Bob: What is the intended audience and what audience do you think it's good for?
Alice: It's intended for a liberal-arts course on math. It could also be used as a supplement in a course for majors. If the teacher knows all the problems with it and points them out then this can be good and has the advantage of teaching students that textbooks can be wrong.
Bob: Lets revisit your list of reasons to teach PRE-RSA and see how this book does.
Alice: Gladly.

1. They get good and motivated review of modular arithmetic, number theory, probability, statistics, and linear algebra. This book does very well on these topics.

2. They see the fallacy of thinking that just because your code was hard to come up with does not mean its hard to break (e.g., a random permutation of $\{a, \ldots, z\}$ can be easily broken with frequencey analysis). The book does talk about frequencey analysis, but doesn't really make this point.

3. They see that many codes that were thought unbreakable were eventually broken; this breeds a heathly skepticisim about current claims. The book does not make this point.

4. They see that historically crypto has been a tradeoff between how much information you must exchange over a secure line and how secure the code is. For example, the shift cipher requires very little information exchange ahead of time (just a number between 1 and 26), but is not secure, whereas the 1-time pad is unbreakable but needs massive amounts of data to be exchanged over a secure line. The book does not make this point; in fact, the book does not even cover the 1-time pad.

5. (Continuing the above point.) When they see that tradeoff they are impressed with Public Key Crypto in that it solves a 4000-year old problem. The book does not make this point.

6. If you know the pre-RSA material then the introduction of complexity (e.g. how much time it takes to crack a code) as a formal object of study is more striking in its importance and originality. The book does not make this point.

Bob: You still speak in lists! You seem to be writing a negative review.
Alice: I view this more as (1) a warning to people who do use the book as to what to look out for, and (2) advice for the author if he writes a second edition. I want to stress that the points I raise can be addressed without a radical rewrite, and I urge the author to make those changes.

Review of[3]

Data Privacy and Security

Author: David Salomon

Publisher: Springer–Verlag, 2003

$51.48, Hardcover

Reviewer: Nick Papanikolaou
(Dept. of Computer Science,
University of Warwick, U.K.)

1 Introduction

The field of cryptology and data security hardly needs any introduction; numerous popular accounts of the subject have appeared over the years, and it is already a core topic in undergraduate computer science. The very term "cryptology" is testimony to the long history of the field; the term is derived from the words $\kappa\rho\upsilon\pi\tau\acute{o}\varsigma$ (meaning hidden), and $\lambda\acute{o}\gamma o\varsigma$ (meaning speech), which have retained their meaning in the Greek language for many centuries.

Cryptology is the study of codes and ciphers, mechanisms through which data can be transformed so as to make their content unreadable to anyone but specially authorized persons. It is traditionally divided into *cryptography,* the development of new codes and ciphers, and *cryptanalysis,* the art of subverting existing ones. While cryptanalysis is regarded as a sort of 'black magic' that has always required special skill (in Alan Turing's days) or extremely fast computers (today), the study of cryptography is of interest to everyone and is becoming increasingly accessible to a wider public. Formally, the purpose of cryptography is to accomplish one or more of the following objectives:

- *confidentiality,* or secrecy of given data;
- *integrity,* or assurance that data has not been tampered with;
- *non–repudiation,* or definitive proof that data was exchanged between parties;
- *authentication,* or proof of the origin of given data.

David Salomon's recent textbook ventures to survey classical cryptography and steganography in an accessible manner. While there already exist several volumes covering these topics e.g. [7, 8, 9], Salomon's book is a practical and readable reference that has much to commend it. Interestingly, it is one of few books to treat steganography on a par with classical cryptographic techniques.

2 Coverage

Salomon starts with a fascinating account of the Zimmermann telegram, which famously contained a plot to discourage the United States from entering the First World War. The telegram was decrypted in England and this, as the author points out, changed the course of history. This highlights the significance of cryptanalysis, and is followed in the book by a definition of all the relevant terminology. Some basic terms of interest are:

Code: A code is a direct transformation of a word, a phrase, or even an entire message.

Cipher: A cipher is a transformation defined over each symbol in a particular *alphabet.*

Nomenclator: A nomenclator is a combination of code and cipher.

Encryption: Encryption is the process of applying a code or cipher to a message, called the *plaintext.*

Decryption: Decryption is the process of recovering the plaintext from an encrypted message, known as the *ciphertext.*

The book's introduction goes on to discuss some simple ciphers, including the *Caesar cipher* and the *one–time pad.* The Caesar cipher is no more than letter shifting; a message is encrypted by replacing each letter with the letter n positions ahead of it. A fashionable version of this cipher is known as **ROT13**, and has $n = 13$, i.e. half the length of the English alphabet. For example, **ROT13** transforms the message `SIGACT NEWS` into `FVTNPG ARJF`.

The one–time pad is a rare example of a *perfect cryptosystem;* a perfect, or unconditionally secure cryptosystem, cannot be broken even if the enemy has unlimited time and computational power. To encrypt a message m with the one–time pad, one must generate a key, k, which is at least as long as m. The same key must be used to encrypt and decrypt the message; the ciphertext is the exclusive-or of k and m. As long as a different key is used for every message, this system provides perfect secrecy — in other words, an enemy cannot obtain any information about the key given only the ciphertext.

The one–time pad cryptosystem suffers from the need to distribute the key to all legitimate receivers of a message; the key itself must be exchanged in secrecy. This so–called *key distribution problem* is addressed in public–key cryptography, and also by using quantum key distribution techniques, described later.

2.1 Chapters 1–3: Substitution and Transposition Ciphers

The first three chapters of the book deal with all the traditional ciphers. In a *substitution cipher,* each letter in a message is replaced with another letter from one or more alphabets. When all letters are drawn from a single alphabet, we have a *monoalphabetic* substitution cipher; these are covered in Chapter 1. When the letters in a message are replaced with letters from several alphabets, we have a *polyalphabetic* substitution cipher, and these are discussed in Chapter 3. *Transposition ciphers* replace a message by a permutation of itself, as explained in Chapter 2 of Salomon's book.

The ciphers discussed in **Chapter 1** include Polybius' cipher, the Playfair cipher, fractionation, and homophonic ciphers. Of these, we will discuss only the Playfair cipher here. In the Playfair cipher, all messages are encrypted with the help of a 5×5 square, which contains all the letters of the alphabet except `J`, which is rarely used in messages anyway. The square serves as an encryption key, and is constructed by choosing a long word with relatively few or no repeating letters. The unique letters of this word are placed, in sequence, into the square, followed by all the other letters in the alphabet. Take, for example, the word `COMPUTATION`; the corresponding square becomes:

```
C O M P U
T A I N B
D E F G H
K L Q R S
V W X Y Z
```

Now, suppose we wish to encrypt the plaintext `FOLLOW ME EARLY`. To do this, we divide the plaintext into pairs of letters (we remove duplicate letters, and pad out with an `X`): `FO`, `LO`, `WM`, `EA`, `RL`, `YX`. Then, for each pair of letters (x, y), we locate x and y in the square and draw the rectangle which has x and y as opposite corners. Next x and y are replaced by the letters in the other two corners of this rectangle. When x and y do not form a rectangle, they are replaced with the letters immediately below (that's when x and y are in the same column) or immediately to the right (that's when x and y are in the same row). Using these rules, we obtain for the pairs in our example plaintext: `EM`, `WA`, `XO`, `WL`, `SQ`, `VZ`. If you would like to know why `YX` maps to `VZ`, and what happens in more complicated cases, you should buy the book!

Chapter 2 deals with transposition ciphers: the turning template, the columnar transposition cipher and the variations due to Myzkowsky and Scott. The author explains how such ciphers can be decrypted, as he does also in Chapter 1. Breaking both substitution and transposition ciphers is actually done by taking advantage of the relative frequency of letters in the English alphabet. Did you know that the probability of finding an 'E' in Shakespeare's plays is 0.1196? It should be added that Matlab code for some of these ciphers is provided in the text.

Chapter 3 discusses a great variety of ciphers, including those due to Beaufort, Trithemius, Vigenère, Gronsfeld, Eyraud, Hill and Jefferson. Let's consider the Hill cipher briefly. In the Hill cipher, all the letters in the alphabet are numbered 0 to 25; a number $n < 26$ is chosen, and the key is formed by generating a $n \times n$ matrix K whose elements are integers in the range 0 to 25. The first n letters of a given plaintext are converted to a column vector, P, and the ciphertext is obtained by computing

$$C = K \cdot P \pmod{m}$$

Decryption in the Hill cipher consists of computing a matrix inverse modulo an integer; in particular, $P = K^{-1} \cdot C \pmod{m}$. Unfortunately, the Hill cipher has limited power and can be subverted using a so–called *chosen–plaintext attack*, in which the enemy knows a finite number of ciphertexts, C_i, and their corresponding plaintexts, P_i.

2.2 Chapters 4 and 5: Random Numbers and The Enigma

Chapter 4 of *Data Privacy and Security* is devoted to random numbers, which are of primordial importance in cryptography. In practice, pseudorandom number generators are used, and algorithms for this purpose are discussed in the text. Also, the author describes the main statistical tests that can be performed to gauge the degree of randomness of a given number sequence. These various topics are covered *in extensis* in Don Knuth's seminal work [2], which is aimed at a more advanced reader.

One of the most attractive features of this book is the material in **Chapter 5,** which details the Enigma machine, used by the Germans in World War II. The historical background is discussed, and the workings of the machine are carefully explained by means of numerous diagrams and pictures.

2.3 Chapters 6–8: Stream Ciphers, Block Ciphers, Public Key Cryptography

Chapters 6–8 of the book cover the more fashionable aspects of cryptography, though no differently from most of the other books [7, 8, 9] on the subject. *Stream ciphers* (Chapter 6) and *block ciphers* (Chapter 7) are the two principal classes of cipher used on modern–day computers. Since all messages are now ultimately reduced to strings of zeros and ones, secure ciphers have to be based on the manipulation of bits. Stream ciphers encrypt a string of bits by treating each bit individually, while block ciphers divide a bit string into blocks and transform each block.

Chapter 6 points out the distinction between symmetric–key and public–key cryptosystems. Symmetric key cryptosystems use the same key for encryption and decryption, while public–key systems use two distinct keys. Linear and nonlinear shift registers are discussed, along with cellular automata, SEAL and the RC4 cipher.

Chapter 7 describes substitution–permutation ciphers, Lucifer and the Data Encryption Standard (DES). This leads on to a presentation of Blowfish, IDEA, RC5 and Rijndael. Rijndael is also known as the Advanced Encryption Standard, or NIST standard FIPS-197. Rijndael involves several rounds and consists of the following operations: byte substitution, row shifting, column mixing, and adding a subkey (or 'round key'). It is not yet known how secure Rijndael is; Salomon states that its security 'can be demonstrated only with time.'

Chapter 8 presents Diffie–Hellman–Merkle key exchange, RSA (the Rivest–Shamir–Adleman public–key cryptosystem), Rabin's system and the El–Gamal scheme. All of these are discussed briefly, with an emphasis on RSA. Threshold schemes and authentication are then covered. Elliptic curve cryptography, now quite *en vogue,* is then described at length. We cannot do justice to the many topics covered, in the framework of this brief review; let us at least reproduce, from page 200 of the book, a two–line implementation of RSA in Perl:

```
print pack"C*",split/\D+/,‘echo "16iII*o\U@{$/=$z;[(pop,pop,unpack"H*",<>
)]}\EsMsKsN0[lN*1lK[d2%Sa2/d0<X+d*lMLa^*lN%0]dsXx++lMlN/dsM0<J]dsJxp"|dc‘
```

2.4 Chapter 9: Quantum Cryptography

Of the cryptographic techniques described in this book, none is more exciting than *quantum cryptography,* which relies for its security on the laws of quantum physics; the BB84 protocol for *quantum key distribution* is presented in **Chapter 9**. It has been proven that this protocol is unconditionally secure against all possible attacks and therefore solves, at least in principle, the age–old problem of key distribution. Combined with an unconditionally secure cryptosystem, such as the one–time pad, quantum key distribution paves the way for truly unbreakable cryptography.

While public–key cryptosystems, such as RSA, resolve the problem of distributing keys in a mathematical way, their security remains largely dependent on the complexity of certain computational problems, such as prime factoring, which can be performed efficiently on a quantum computer. Quantum computers are still mostly objects of theoretical speculation, but small–scale ones have been built in experimental physics labs. Peter Shor famously devised efficient quantum algorithms for factoring and the discrete logarithm; a full–scale quantum computer could run these algorithms and efficiently break several cryptosystems in current use. The security of quantum cryptography, or more specifically, quantum key distribution, is not threatened by the computational power of quantum computers.

Gilles Brassard ran a 'Cryptology' column in *SIGACT News* for years; before I describe quantum cryptography in more detail, let me quote his words on the tie between this newsletter and the subject:

> "The fates of SIGACT News and Quantum Cryptography are inseparably entangled. The exact date of Stephen Wiesner's invention of 'conjugate coding' is unknown but it cannot be far from April 1969, when the premier issue of SIGACT News [...] came out. Much later, it was in SIGACT News that Wiesner's paper finally appeared [*Vol. 15, No. 1, 1983*] in the wake of the first author's [*Gilles Brassard's*] early collaboration with Charles Bennett [...]. It was also in SIGACT News that the original experimental demonstration for quantum key distribution was announced for the first time [*Vol. 20, No.4, 1989*] and that a thorough bibliography was published [*Vol. 24, No. 3, 1993*]. Finally, it was in

SIGACT News that Doug Wiedemann chose to publish his discovery when he reinvented quantum key distribution in 1987, unaware of all previous work but Wiesner's [*Vol. 18, No. 2, 1987*].

Quantum key distribution protocol BB84 allows two parties, 'Alice' and 'Bob,' to establish a secret binary key. The idea is to represent each bit in a given string by either a rectilinearly or diagonally polarized photon. In the *rectilinear basis,* a `0` is represented by a photon polarized at 0°, and a `1` by a 90°–polarized photon. In the *diagonal basis,* a 45°–polarized photon stands for `0` and a 135°–polarized photon stands for `1`. In brief, the protocol proceeds as follows. Alice generates a random bit string, and a random string of encoding bases. Each bit is mapped to a polarized photon using the corresponding basis and then transmitted to Bob. Bob does not know which basis has been used to encode each photon, and so chooses one of the two bases at random in order to make a measurement. Due to the laws of quantum physics, the result of Bob's measurement is only guaranteed to be correct for a given photon if his choice of measurement basis matches the one used by Alice for encoding. When the entire binary string has been transmitted in this way, Bob will have obtained a subset of Alice's bit string. Using a classical —possibly even public— communications channel, Alice tells Bob which of his basis choices were correct.

There is much more to quantum cryptography than we can say here, and the interested reader is referred to [4] for a recent introduction to the subject. It should be added that commercial quantum cryptographic devices do exist already (see `http://www.magiqtech.com` and `http://www.idquantique.com`). Quantum protocols such as BB84 are of special interest to computer scientists today; for example, [3] discusses modelling and analysing the security of these schemes using automated tools.

Salomon's presentation of quantum cryptography in *Data Privacy and Security* is very readable, and is innovative in the sense that not many crypto textbooks deal with this subject. On a lighter note, Schneier [7] exclaims: "this would still be on the lunatic fringe of cryptography, but Bennett and Brassard actually went and built a working model of the thing [...]."

2.5 Chapters 10–12: Steganography

The three final chapters of the book are devoted to *steganography,* or data hiding. The goal of steganography is to hide a message in another item of data, known as the *cover.* If the original message is to be embedded in a text, referred to as *covertext,* the product of the steganographic procedure is termed a 'stegotext.' Messages can also be embedded in images, sounds and video, leading respectively to the use of the terms 'coverimage' and 'stegoimage,' 'coveraudio' and 'stegoaudio,' 'covervideo' and 'stegovideo.' Word-smithing will never go out of style!

The basic ingredients of a data hiding system are: (1) the data to be embedded; (2) the cover, in which embedding will occur; (3) a stego–key; (4) an embedding algorithm; and (5) a decoder. The embedding algorithm produces a *stego–cover* given the first three items above. To recover the data hidden in it, the stego–cover is fed into a decoder along with the stego–key. **Chapter 10** of the book elaborates on these fundamentals and focuses on data hiding *in text.* The principal characteristics of a data hiding algorithm are identified and explained; these are embedding capacity (how much data can be hidden in a given cover), invisibility (how much distortion is caused to the cover), undetectability (a statistical measure of the distortion), robustness (the degree of immunity of the stego–cover to subsequent alterations, such as compression), tamper resistance (the degree of immunity of the stego–cover to direct tampering) and the signal–to–noise ratio. Watermarking is introduced. As an example of data hiding in text, that merely modifying the spaces in a text file is a means of conveying a message. This particular idea is extended in an interesting manner on page 256:

> "The TeX typesetting software permits very fine control over the interword spaces and the spaces following certain punctuation marks. The smallest dimension that TeX can use is called a scaled point (sp). One inch equals 72.27 printers' points (pt), and one pt equals 65,536 scaled points. Thus, the value of a sp is about the wavelength of visible light, and changing the normal interword space by 1 sp is invisible. TeX can also list the precise values of all the components of text [...] Because of these features, TeX may be an ideal tool for hiding data in spaces, although it was originally designed as a high–quality typesetting system for the production of books."

This quotation reminds me of David Salomon's equally commendable TeX volume [5].

Chapter 11 of *Data Privacy and Security* focuses on data hiding in images, both in the spatial domain and the transform domain. Topics covered include LSB encoding, bit–plane complexity segmentation, spread–spectrum steganography and wavelet–based watermarking. Several methods of watermarking are covered, and variations are explained clearly.

The last chapter is concerned with data hiding in audio and video, and goes as far as to describe the remarkable 'steganographic file system' [1]. This file system hides a given set of files f_i in several ordinary files, in such a way that an unauthorized user cannot even determine whether the f_i exist.

The book's appendices deal with important mathematical background associated with the subject, namely convolution, hashing, cyclic redundancy codes and Galois fields. Answers to all the exercises in the text are given, and there is also a 10–page historical timeline of cryptography. This is supplemented by a glossary, a detailed bibliography and a comprehensive index.

3 Opinion and Conclusion

Overall, *Data Privacy and Security* is a handy and concise volume on cryptography and steganography. While the more advanced reader will find alternative references — such as [7] — more satisfying, this book is clearly written and self–contained. All the important cryptosystems are covered, and the discussion of recent developments, including Rijndael and quantum cryptography, is welcome.

References

[1] Anderson, R., Needham, R., and Shamir, A. The steganographic file system. In *2nd Information Hiding Workshop* (1998).

[2] Knuth, D. E. *Seminumerical Algorithms.* Addison-Wesley, 1981.

[3] Papanikolaou, N. Techniques for design and validation of quantum protocols. Master's thesis, Department of Computer Science, University of Warwick, 2005.

[4] Papanikolaou, N. Introduction to quantum cryptography. *ACM Crossroads Magazine 11.3* (Spring 2005 Issue).

[5] Salomon, D. *The Advanced TeXbook.* Springer Verlag, 1995.

[6] Salomon, D. *Data Privacy and Security.* Springer–Verlag New York, Inc., 2003.

[7] Schneier, B. *Applied Cryptography*, 2nd ed. Wiley, 1996.

[8] Smart, N. *Cryptography: An Introduction.* McGraw–Hill Education (UK), 2003.

[9] Welsh, D. *Codes and Cryptography.* Clarendon Press, 1998.

Joint review[4] of

Cryptography: An Introduction

V.V. Yaschenko, ed.

American Mathematical Society, 2002, 229 pp., $39.00

and

Cryptanalysis of Number Theoretic Ciphers

by S.S. Wagstaff, Jr.

Chapman & Hall/CRC Press, 2003, 318 pp., $79.95

and

RSA and Public-Key Cryptography

by R.A. Mollin

Chapman & Hall/CRC Press, 2003, 291 pp., $79.95

and

Foundations of Cryptography, vol. 1: Basic Tools

by O. Goldreich

Cambridge University Press, 2001, 372 pp., $75.00

Reviewed by Jonathan Katz

Dept. of Computer Science, University of Maryland

With the growing interest in cryptography — from students and researchers as well as from the general public — there has been a corresponding increase in the number of cryptography textbooks available. Many of these, however, remain somewhat mired in the past, and present cryptography from a pre-1980s point of view. Indeed, there are very few published books which even make an attempt (let alone a successful one) at covering *modern* cryptography. This unfortunate state of affairs results in a serious lack of books describing the fundamental advances in the field that have taken place since the mid-1980's; this is especially true at the undergraduate and beginning graduate levels, where there is a severe need for suitable texts in this area.

The central contributions of modern (i.e., post-1980) cryptography include an emphasis on precise definitions, formalizations of cryptographic goals, and *provably-secure* constructions of higher-level tasks (e.g., signatures) from lower-level primitives (e.g., one-way functions). Without precise definitions and rigorous proofs of security, cryptography is reduced to a "game" in which the goal is merely to design a scheme that one's friend or colleague cannot "break". Any exposition of cryptography failing to recognize and emphasize the difference between the former and the latter approaches misses a substantial fraction of what current cryptographic research is about, and is a disservice to the field. Sadly, however, almost all cryptography textbooks of which I am aware fall into this category.

A classic example of the problems with an "ad-hoc" approach to cryptography is the following simple test I often use to discriminate "good" cryptography books from "poor" ones: flip to the section on digital signatures and see whether it is stated anywhere that "textbook RSA" signatures are *completely insecure*. It is a simple exercise to show that this is the case (the same holds for "textbook RSA" encryption, but it is somewhat more difficult to demonstrate), yet most books make no mention of this (central!) fact, and instead leave the reader with the impression that secure signature schemes based on the RSA problem are easy to design.[5]

[5]Fortunately, security professionals know not to use "textbook RSA" signature and encryption schemes in real-world systems.

Some might argue that there is no place for rigorous definitions and proofs in a book directed toward undergraduates, but I take this misconception as a thinly-guised insult to undergraduate computer science majors. Undergraduates in other majors are taught quantum mechanics, thermodynamics, analysis, and abstract algebra, to name a few, all difficult subjects that are taught rigorously (to varying degrees, perhaps). Why should an undergraduate course on cryptography be expected to be any *less* rigorous than these?

Continuing the disappointing trend discussed above, neither of the first three books reviewed here qualify as (what I would consider) appropriate for introducing the interested reader to the field of cryptography. *Cryptography: An Introduction* gets a number of things right, but overall is a muddled, poorly written, and disorganized text whose intended audience is unclear. *Cryptanalysis...* is a useful book which I am glad to have on my shelf, but it fails at its stated goal of serving as a suitable text for an introductory cryptography course. It would serve better as a book on elementary number theory (with applications to cryptography, perhaps), and I wish it had been advertised and organized as such. A somewhat similar book, *RSA and Public-Key Cryptography* suffers from the same criticisms; furthermore, I found its treatment of number theory to be not quite on par with that in Wagstaff's book.

In contrast to these, *Foundations of Cryptography* presents a clear and accurate picture of the foundations underlying modern cryptography; in fact, it is currently the *only* published book I am aware of which does so. Its primary drawback is that it is likely to be inaccessible to the beginning student; it is more appropriate for a researcher or an advanced graduate student who has previously been exposed to the basics of cryptography, either of whom would benefit from a careful reading of this book cover-to-cover.

1 "Cryptography: An Introduction," by Yaschenko

Cryptography... passes the "signature" test described above with flying colors: in addition to giving a formal definition of security for signature schemes, the book also describes — and sketches a proof of — the Lamport one-time signature scheme. Even more surprisingly, it describes in some detail (and correctly!) the Naor-Yung extension of the Lamport scheme, which results in a full-fledged signature scheme based on quite weak assumptions. The book also gives accurate, formal definitions of many other cryptographic primitives.

In fact, one of the drawbacks of this book is that it covers *too* much material in a disjointed and seemingly disorganized fashion. Chapter 1, for example, gives a very informal (and informally written) overview of cryptography, running through (over?) substitution ciphers, the one-time pad, and Diffie-Hellman key exchange. This is followed by Chapter 2 which — in 11 pages! — gives a relatively formal introduction to one-way functions, pseudorandom generators, and zero-knowledge proofs. Although I appreciated the level of formality here (it was heartening to see that the details were mostly correct), I doubt that someone new to the field would be able to learn much from such a terse description of these topics. In addition, the English and writing style throughout are quite poor (it appears the book has been translated from Russian), making the book that much less accessible.

The choice of topics in the remainder of the book is equally baffling. Chapter 3, titled "Cryptographic Protocols", does a reasonable job covering digital signatures and also discusses electronic cash, coin flipping, and secret sharing (among others). There was not much rationale given to the choice of topics, nor was their relation to each other made clear. Chapter 4 covers some of the number-theoretic problems underlying cryptography, such as generating primes and testing primality. Chapter 5 discusses secret sharing schemes for arbitrary access structures — an advanced topic that I would not expect to be included in an introductory text — and the book then devotes more than 1/3 of its pages to simple cryptanalysis problems. In an elementary book, I would expect to see more discussion on fundamentals like signature schemes and public-key encryption schemes rather than the relatively esoteric topics that were included.

In all, the intended audience for this book is simply unclear to me. Students approaching this material for the first time would encounter a strange mix of topics, would miss some fundamental concepts, and might be turned off by the poor writing and dense exposition. Advanced students would likely be annoyed at the lack of coherence and organization, as well as the overall poor level of writing.

2 "Cryptanalysis of Number Theoretic Ciphers," by Wagstaff

The preface of *Cryptanalysis...* states that the book arose from an undergraduate cryptography course taught by the author. As an introduction to cryptography, however, the book fares poorly. On the other hand, for the most part the book does contain well-written explanations of various aspects of number theory related to cryptography. The book would be much improved had it concentrated on, and expanded upon, the number-theoretic aspects alone instead of cramming in many spurious and unrelated (not to mention inaccurate and confusing) chapters on security and cryptography.

I will start with the positive features of the book. Section I gives a decent (though at times fast-paced) overview of some of the basic mathematics necessary to understand cryptography. Chapters 1–9 introduce probability, efficient computation with large integers, prime numbers and their distribution, modular arithmetic, Euler's theorem, Legendre/Jacobi symbols, information theory, and basic group/field theory. Chapters 10–15 of Section I treat more advanced topics including sub-exponential factoring algorithms, primality testing, and algorithms for computing discrete logarithms. A chapter on elliptic curves and their application to factoring and primality testing is also included. Overall, the chapters in this section are quite good: the first 9 chapters are well-written, and should prove useful to undergraduates approaching number theory for the first time. The latter chapters were quite thorough in their coverage of advanced topics; these could serve well as a reference for researchers who are already somewhat familiar with these topics.

On the negative side, I found some of the coverage of the advanced topics to be a little terse and difficult to read (although on a whole the coverage of these topics was fine). For example, Chapter 12 introduces elliptic curves *as well as* elliptic-curve algorithms for factoring and primality testing in a total of 12 pages! An undergraduate using this text would clearly benefit from a slower presentation of this topic. Also, the author gets himself into trouble as he moves from number theory to cryptography: An example is Chapter 15 titled "Random Number Generation", where the author merges discussions of linear feedback shift registers (which, to be fair, are noted by the author to be insecure) and the Blum-Blum-Shub provably-secure random number generator, and then throws in a section on hash functions without carefully describing their relation to the subject matter of the chapter. In all, I think the book would be better had the author cut most of Chapter 15 and Section II (which both deal with cryptography and security) and focused all his effort on the number-theoretic underpinnings of cryptography which form the subject matter of Section I.

Section II includes chapters on Rijndael (i.e., AES), public-key encryption schemes (confusingly called "ciphers"), signature schemes, key-exchange protocols, advanced cryptographic protocols such as oblivious transfer, zero-knowledge proofs, and electronic cash (among others), and the security protocols Kerberos and PGP. No formal definitions or proofs of security are given, and some fundamental concepts (such as pseudorandom functions) are not even mentioned. In addition to the fact that the style and choice of topics are (in my view) not the most desirable for an introductory course on modern cryptography, I also found Section II to be disorganized and poorly written, with little motivation or connection between topics in what is currently a "grocery list" of (seemingly-arbitrary) crypto protocols. Although there are occasional nuggets of information to be gleaned from the text, for the most part I found the presentation disjointed and confusing.

There are also a number of errors/inaccuracies in Section II: for example, Pohlig-Hellman is mentioned as a plausible candidate for private-key encryption (in practice, it is too inefficient to ever be used as such); "textbook" RSA encryption is described as secure (as noted earlier in this review, it is not); and no mention is made of RSA signatures alone (instead, the book only discusses them in the context of signcryption, an odd choice). Furthermore, the definition given for a "block cipher" is wrong; the book confuses secrecy with integrity in the context of symmetric-key encryption (a common mistake, but an inexcusable one); the text contains an inaccurate definition of a one-way function; and the discussion of PGP is confusing and seemingly wrong. Even if one accepts that this is not a book on modern cryptography, the book tries to cover too much too quickly, and with little sense of perspective: hopping from Rijndael to X.509 certificates, or from oblivious transfer and zero-knowledge protocols to a discussion of PGP (where most topics are only touched on briefly) does not help to make this latter section accessible.

In summary, Section I of this book may serve well as a companion piece for an undergraduate course in number theory with applications; it may also be useful for students of cryptography to supplement their knowledge of algebraic cryptanalysis (and especially algorithms for primality testing, factoring, and computing discrete logarithms). The book would also serve as a good reference text on algebraic cryptanalysis for researchers already familiar with the area. The book is simply unsuitable as an introduction to modern cryptography, however, and I would not recommend it as a textbook for such a course.

3 "RSA and Public-Key Cryptography," by Mollin

Although this book does not claim to serve as a text for an introductory course in cryptography, I have included a review here due to its similarities with the previous book. In fact, there is quite a significant overlap in terms of topics covered: the first five chapters of *RSA and Public-Key Cryptography* also cover the discrete logarithm problem and Diffie-Hellman key exchange, the RSA and El Gamal cryptosystems, primality testing, and sub-exponential factoring algorithms. Chapter 6 discusses some attacks on RSA, including timing/power attacks (which, more properly, should be said to attack *implementations* of RSA) and low-exponent attacks. Identification and signature schemes are presented in Chapter 7, as well as a scheme for digital cash. "Key management" issues (including secret sharing, key pre-distribution schemes, and PKI) are covered in Chapter 8. Chapter 9 discusses some security protocols in very general terms.

As in the case of the previous book, the strongest portions of this book are those that deal with number theory; the sections dealing with cryptography and security were presented rather poorly on the whole, and with seemingly little connection between topics. Examples of the "ad-hoc" approach to cryptography taken by this book abound: one such example that caught my eye was in the context of discussing the Schnorr identification protocol. The author claims that "nobody has ever proved that the protocol is secure." Of course, it is impossible to evaluate this statement because a definition of a secure identification protocol (even an informal one) is never given by the author. Furthermore, this statement is somewhat misleading: the Schnorr protocol *has been* proven secure, but only against *passive* attacks. Presumably, the author was referring to security against *active* attacks but this does not come across clearly from the text.

The description of RSA encryption — in contrast to what one might expect from the book's title — is similarly lacking. To the author's credit, he does mention that "textbook" RSA encryption is insecure. But his discussion of padding techniques needed to ensure security is, at best, confusing: an exponential-time attack which recovers the message is presented as more problematic than the simple fact that "textbook" RSA encryption is deterministic and therefore inherently insecure. Furthermore, the author mixes discussions of semantic security and chosen-ciphertext security (without defining either, of course); a reader who is not already aware of the relevant cryptographic literature would come away from this book without any idea as to how secure encryption can be based on the RSA problem (nor, for that matter, would they come away with any idea of what secure encryption means).

Comparing the present book and the previous book on their strengths — namely, their treatment of number theory which is relevant to cryptography — I much preferred Wagstaff's book. I found the writing style as well as the organization in Wagstaff's book to be more conducive to a good understanding of the material, and in addition Wagstaff's book assumed less prior knowledge on the part of the reader. Mollin's book, in contrast, is quite terse (the many examples and exercises actually take away space that might otherwise have been used for additional exposition), and covers less material than Wagstaff's book. Mollin, for whatever reason, puts more emphasis on RSA at the expense of other cryptosystems and this somewhat limits his coverage.

4 "Foundations of Cryptography, vol. 1: Basic Tools," by Goldreich

Foundations of Cryptography contains what is currently the best published treatment of the formal aspects of modern cryptography and serves as "required reading" for anyone interested in research in the field. The approach taken in this book and its clear differences from, say, the previous two books reviewed in this column are clear from the first few paragraphs of the Preface:

> The design of cryptographic schemes is a very difficult task. One cannot... be content with countermeasures designed to withstand specific attacks, because the adversary... will try to attack the scheme in ways that typically will be different from the ones the designer envisioned.... cryptographic schemes based on make-believe are broken, typically sooner rather than later.
>
> In view of the foregoing, ... it is our opinion that the design of cryptographic systems has to be based on *firm foundations*, whereas ad hoc approaches and heuristics are a very dangerous way to go...

The present book does indeed succeed at its stated goal of presenting firm foundations for cryptography. Throughout, definitions are complete and detailed; proofs are rigorous and given in full. Chapter 1 contains a survey of the topics covered in the book, and then jumps into a (brief) review of probability theory and computational complexity (including P, NP, and NP-completeness). The chapter concludes with some motivation for the rigorous treatment of cryptography advocated by this book, along the lines of the text quoted above. In Chapter 2 the author motivates and presents definitions for one of the central primitives of cryptography: one-way functions. A variety of subtle variations on the primary definition are introduced, and connections between these definitions are explored. The chapter spends a considerable amount of time on two topics which serve, in particular, as nice illustrations of the dictum that "proofs are preferable to ad-hoc reasoning" (and the author does a nice job of expounding on this point): the first is a proof that so-called "weak" one-way functions (which, informally, are only moderately-hard to invert) imply "strong" ones (which, again simplifying things, are impossible to invert except with exponentially-small probability); the second is a proof of the existence of *hard-core bits* for every (strong) one-way function. The text's inclusion of latter result is in sharp contrast with some other texts which claim (or at least imply) that if a function f is one-way then it must "scramble" its input in such a way that $f(x)$ hides all information about x. Unfortunately, this is easily seen to be untrue! On the other hand, work of Goldreich and Levin shows that this intuition is true to a more limited extent: very informally, if f is a one-way function then there exists (constructively) one bit of information $h(x)$ about x which is "hidden" by $f(x)$. Formalizing and rigorously proving this simple-sounding idea were landmarks in the theory of cryptography, and it is nice to have a self-contained and very readable proof available in this book.

Chapter 3 introduces pseudorandom generators (PRGs) and pseudorandom functions (PRFs) in some detail. The chapter begins with a discussion of computational indistinguishability (which pervades much of modern cryptography even beyond the applications in this chapter) and then presents various definitions and implications of PRGs. The core of the chapter is a proof that PRGs can be constructed from one-way permutations. In fact, an important result of Haståd, Impagliazzo, Levin, and Luby is that one-way *functions* suffice, and some weaker versions of this result (i.e., constructing PRGs using one-way functions with some structure) are described here. The chapter ends with a proof that PRGs can be used to construct PRFs, followed by a section on pseudorandom permutations.

The last chapter is devoted entirely to zero-knowledge (ZK) proof systems. This chapter is without a doubt *the* best reference for this material, especially if one is interested in understanding the subtleties of the definitions and constructions. A tremendous amount of material is covered: following a brief background on interactive proof systems generally (and a presentation of a proof system for graph non-isomorphism), the chapter describes a ZK proof system for graph isomorphism as well as a ZK proof system for all of NP. In a sequence of more advanced sections, other topics are discussed: these include (among others) the notion of witness-indistinguishable proof systems, non-interactive proof systems, as well as proofs of knowledge.

Each chapter ends with historical notes, suggestions for further reading (the bibliography is extensive and quite good, and easily leads the reader to the relevant results in the literature), and a brief list of open questions. An appendix provides a brief review of some material on computational number theory which is only used at a few points in the book.

It is certainly surprising to find a book on cryptography that does not cover encryption, authentication, or digital signatures! These topics are all covered in a second volume by the same author published in 2004 . . . which brings me to the drawbacks of this volume. Clearly, this volume alone cannot be used for an introductory course on cryptography. The author admits as much in the Preface, but suggests that volumes 1 and 2 together could be used for such a course. It seems to me that this is a bit optimistic. The material is presented at an extremely high level which makes this book an excellent resource for those readers seeing the material a second (or even third) time; however, I wonder whether someone with no prior exposure to cryptography — even a theoretical computer scientist — might not be lost in a sea of notations and (seemingly unimportant to the novice) subtleties. Similarly, although I understand the motivation of the author to present ZK proofs before, say, encryption, my impression is that students prefer to see some real-world applications before delving further into the theory.

With that in mind, the book remains a "must-read" for all graduate students and researchers interested in this area, and is well-suited for an advanced course (or upper-level graduate seminar) on cryptography. Kudos to the author for publishing the first book which truly covers *modern* cryptography, and for doing an excellent job of it!

5 Summary

It remains the case that few (if any) textbooks cover *modern* cryptography at a level appropriate for an introductory undergraduate course, and none of the books reviewed here quite fill this role. Nevertheless, at least two of the books here fill other roles: Wagstaff's book might be useful as a basic introduction to some of the number theory used in cryptography, and would be appropriate as a reference as well; Goldreich's book is an outstanding work covering modern cryptography at a level more suited to advanced students and researchers, and would be excellent for an advanced graduate course in cryptography.