Exercise. Why do I object to each of these statements?

Many readers will find Gullberg's book valuable, despite its imperfections. However, it is not the book I hoped for. Although it has history and culture, and lots of vocabulary and grammar, it does not get to literature and poetry; nor does it give any inkling that most of the mathematics that exists was created in the twentieth century. I would not dare to give this book to my niece, for it would only confirm her belief that mathematics is just boring formulas, but I would have been a grateful recipient if someone had given me this book when I was a high school freshman. It would have opened my eyes to what an extensive game mathematics is, and I would have had fun playing with the formulas and trying to figure out why they work.

Gullberg produced camera-ready copy for this book himself, which was a tremendous job. I wonder why he did not enlist the aid of a professional typesetter, who could have warned him against solecisms such as increasing the inter-letter spacing of a widow word on the last line of a paragraph. The typesetting is a metaphor for the mathematics in the book: it is serviceable, but it does not look quite right to an expert eye.

I continue to wait for someone to write a book that treats mathematics as a foreign language. I want to give a copy to my kindergarten teacher.

—Harold P. Boas

Handbook of Applied Cryptography. By Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone. CRC Press, Boca Raton, 1997, 780 + xxviii, $79.95.
The Cryptographic Imagination: Secret Writing from Edgar Poe to the Internet. By Shawn James Rosenheim. Johns Hopkins University Press, Baltimore, 1997, 264, $47.50.

Reviewed by **Jeffrey Shallit**

Cryptography is the art and science of writing and reading concealed messages. David Kahn, in his monumental work, *The Codebreakers* [**9**], traces its origin to 1900 B.C.E., in an inscription carved on the tomb of Khnumhotep II. Not surprisingly, modern cryptography has a strong mathematical component. Indeed, just weeks before the Japanese attack on Pearl Harbor in World War II—a war where cryptography would play a crucial role—algebraist A. A. Albert stated in a regional meeting of the American Mathematical Society, "It would not be an exaggeration to state that abstract cryptography is identical with abstract mathematics." [**1**]

As we make the transition to a wired society, cryptography is becoming more and more fundamental. Cryptography can be used to preserve the privacy of messages exchanged over the Internet, to provide a means for electronically signing messages (so that recipients can be assured the message really came from the stated author), to prevent unauthorized access to sensitive information, and to provide a secure system for "electronic cash." Of course, like any useful tool, it can also be used to conceal evidence of lawbreaking, which is one reason why the debate over cryptography policy is so heated [**8**]. The United States government continues to restrict export of certain kinds of cryptographic software, although

lately there have been some signs of weakening of this policy. As I write this, Senators Conrad Burns (R MT) and Patrick Leahy (D VT) have introduced the "Promotion of Commerce Online in the Digital Era (Pro-CODE) Act," a bill designed to relax government controls on encryption.

Although some (notably Dorothy Denning [**5**]) continue to endorse some kinds of government control over cryptography, most observers concede that the genie is out of the bottle, and no law can stuff it back in. Some of the mathematics involved in cryptography is so elementary that a bright high-school student can devise encryption software essentially uncrackable with currently available techniques.

Modern cryptography has traveled a long way from the simple substitution cipher, where messages are encoded by applying a permutation of the letters $\{A, B, C, \ldots, Z\}$. As a glance at the proceedings of the latest conferences on the subject (CRYPTO, EUROCRYPT, AUSCRYPT, ASIACRYPT) demonstrates, modern cryptography is based largely on number theory, combinatorics, and algebra. Although some cryptographic techniques are quite elementary, others involve the deepest and most modern aspects of these areas.

The so-called *public-key cryptosystem* is a fundamental discovery of modern cryptography. In older methods based on secret keys, the same key is used to encode and decode a message. Losing the key means that the secrecy of the message is compromised. In 1976, however, Whit Diffie and Martin Hellman invented a new kind of cryptosystem in which the encryption and decryption keys differ [**6**]. To employ the system, a user U publishes the encryption key e for all to see. By using the key, anyone can send an encoded message to U. But U keeps the decryption key d a secret, and the system is designed so that obtaining d from e is a problem that appears to be computationally intractable. In practice, then, without enormous computing resources or extraordinary luck, only U can read the message because only U knows the decryption key d.

The RSA scheme—the name comes from the initials of its inventors, Rivest, Shamir, and Adleman—is the most famous example of a public-key cryptosystem [**11**]. It is based on the apparent intractability of computing kth roots modulo composite numbers. Invented in 1977, the system continues to withstand the various attacks devised against it, although research has provided some caveats about how best to choose the particular parameters involved. More recent proposals are based on number theory, and draw their inspiration from the discrete logarithm problem, the quadratic residuacity problem, and the theory of elliptic curves.

Another advance of modern cryptography is the *digital signature*. Here the goal is to attach a number to a message depending on (a) some secret key known only to the signer and (b) the content of the message itself. A good digital signature scheme allows the user to verify a message's authenticity and prevents later repudiation of signatures. Secure digital signatures are essential if electronic commerce is to become a reality.

In their *Handbook of Applied Cryptography*, Menezes, van Oorschot, and Vanstone convincingly demonstrate the serious mathematical content of applied cryptography. The authors have significant expertise in both theoretical and practical aspects of cryptography. Vanstone, for example, is a founder of a corporation that makes encryption products, and is the author of at least two dozen papers in the literature on cryptographic topics. Menezes wrote his Ph.D. dissertation on public-key cryptography [**10**], and van Oorschot is employed as a cryptographer.

The approach taken in this book is encyclopedic. Nearly every aspect of modern cryptography—stream ciphers, block ciphers, public-key cryptography, hash func-

tions, digital signatures, key establishment protocols, etc.—is covered in its 800 pages. Each chapter contains a "Notes" section, with valuable historical remarks. The book contains over 1200 citations to the literature.

The *Handbook* strongly emphasizes practical aspects of cryptography. For example, Chapter 14 discusses how to perform extended-precision arithmetic efficiently (essential for modern cryptography, which routinely deals with numbers of 100 to 400 digits).

The *Handbook* probably isn't appropriate as a textbook or gentle introduction to cryptography—for that, see instead [**3**] or [**12**]. It is probably more appropriate as a reference work, and in that it succeeds admirably. There are, however, some minor flaws. For example, the surname of Franz Mertens is misspelled twice. More seriously, Definition 2.73 erroneously states that "A problem is **NP**-hard if the existence of a polynomial-time algorithm for its solution implies that **P** = **NP**." While this is correct if, as most suspect, **P** ≠ **NP**, it is incorrect if **P** = **NP**. The correct definition is that a problem X is **NP**-hard if every problem in **NP** reduces to X in polynomial time. Similarly, Definition 3.1, which defines polynomial-time reduction, is regrettably imprecise, drawing no distinction between Turing reduction and many-one reduction. Other errors can be found in the world-wide-web page for the book, `http://www.dms.auburn.edu/hac/`.

Another annoyance is that the index is inadequate. For example, there is no entry for either "**NP**" or "nondeterministic polynomial time." Also missing is an index to names, so that it is very difficult to determine where a particular paper is cited in the text. Nevertheless, despite these minor problems, the *Handbook* should prove to be a very useful reference for mathematicians and cryptographers.

The contrast between the *Handbook* and Shawn Rosenheim's *The Cryptographic Imagination* couldn't be more marked. Rosenheim, a professor of English and American Studies at Williams College, has produced a rambling, disjointed meditation on cryptography, Edgar Allan Poe, espionage, Thomas Pynchon, and the Internet.

Unfortunately, Rosenheim's attempts to discuss technical matters are nearly always marked by severe misunderstandings of the mathematics and physics involved. For example, consider his definition of quantum cryptography, which appears in the glossary:

> A form of cryptography in which, under certain experimental conditions, pairs of photons may be created that exert an influence over one another that cannot be explained by quantum mechanics. Measuring the polarization of one particle immediately and identically changes the spin on its antiparticle. Such polarization takes place regardless of the relative positions of the two particles in the universe, in a result that seems to violate the second law of classical theory. It is theoretically possible that a stream of such polarized photons could be used to encipher messages that could be sent over space in literally no time at all.

There are so many errors in just these four sentences that it is difficult to know where to begin. First of all, the behavior of entangled photon pairs is, contrary to the claim, perfectly explicable through quantum mechanics. Second, practical quantum cryptography is not currently based on entangled photon pairs—although Ekert [**7**] did propose such a scheme—but a different mechanism proposed much earlier by Wiesner [**13**] and Bennett and Brassard [**3**]. Third, the reference to the "second law" is, of course, utter nonsense. Finally, quantum cryptography is not simply a theoretical possibility, but a practical reality [**2**].

Other blunders in *The Cryptographic Imagination* include conflating monkeys and apes, misstating Zipf's law, wildly overestimating the amount of pornography

on the Internet, misstating the name of the Usenet newsgroup alt.sexual.abuse.recovery, and comically misspelling the name of one of the inventors of RSA as "Ronald Rivers." Rosenheim even makes mistakes in his own field: he claims that Georges Perec's book *La Vie: Mode d'Emploi* was written without the letter "e," when in fact it is another book by Perec entitled *La Disparition.*

This is not to say that I didn't get anything out of Rosenheim's book. I was intrigued to learn about Lizzie Doten, a 19th century mystic who "channeled" ersatz poems of Poe and other writers such as Shakespeare and Burns. But the book is marred by the usual postmodernist excesses: making much of tenuous or nonexistent connections, second-rate wordplay (the series in which *The Cryptographic Imagination* is published is entitled "re-visions of culture and society"; among postmodernists, this sort of gratuitous hyphen insertion is apparently considered essential), and opaque exposition. Consider the following two examples:

> When I claim that Poe helped end World War II, the "Poe" in that sentence represents both a particular author and the literary genre he helped create and for which he serves as a synecdoche. (p. 15)

> Such a homeopathic technique for the creation of mysteries produces highly cathected readers; the surface of the cipher produces a crypt in us, which we proceed to fill with our imagination, just as the semantic vacuity of Khumnhotep's [sic] glyphs contextually signified Khumnhotep's [sic] power and his resistance to comprehension. (p. 48)

The Cryptographic Imagination will be of little interest to anyone wanting to learn about cryptography. In fact, I can scarcely think of a reason to read it, except perhaps to see an example of what passes for scholarly work in some academic disciplines.

REFERENCES

1. A. A. Albert, Some mathematical aspects of cryptography, in R. E. Block et al., eds., *A. Adrian Albert: Collected Mathematical Papers*, American Mathematical Society, 1993, pp. 903–920.
2. C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, Experimental quantum cryptography, *J. Cryptology* **5** (1992) 3–28.
3. G. Brassard, *Modern Cryptology*, Lecture Notes in Computer Science #325, Springer-Verlag, 1988.
4. C. H. Bennett and G. Brassard, Quantum cryptography and its application to provably secure key expansion, public-key distribution, and coin-tossing, *IEEE Int. Symp. Information Theory*, September 1983, p. 91.
5. Dorothy E. Denning, Resolving the encryption dilemma: the case for Clipper, *Technology Review* **98** (5) (July 1995) 48–55.
6. W. Diffie and M. E. Hellman, New directions in cryptography, *IEEE Trans. Info. Theory* **22** (1976) 644–654.
7. A. K. Ekert, Quantum cryptography based on Bell's theorem, *Phys. Rev. Lett.* **67** (1991) 661–663.
8. Lance J. Hoffman, *Building in Big Brother: The Cryptographic Policy Debate*, Springer-Verlag, 1995.
9. David Kahn, *The Codebreakers: The Story of Secret Writing*, Macmillan, 1967.
10. A. R. Menezes, *Elliptic Curve Public Key Cryptosystems*, Kluwer, 1993.
11. R. L. Rivest, A. Shamir, and L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, *Commun. ACM* **21** (1978) 120–126.
12. D. R. Stinson, *Cryptography: Theory and Practice*, CRC Press, 1995.
13. S. Wiesner, Conjugate coding, *SIGACT News* **15** (1) (1983) 78–88.

Department of Computer Science, University of Waterloo, Waterloo, Ontario N2L 3G1, Canada
shallit@graceland.uwaterloo.ca