



Review: [Untitled]

Reviewed Work(s):

Mathematics: From the Birth of Numbers. by Jan Gullberg
Arnold Allen

The American Mathematical Monthly, Vol. 106, No. 1. (Jan., 1999), pp. 77-85.

Stable URL:

<http://links.jstor.org/sici?sici=0002-9890%28199901%29106%3A1%3C77%3AMFTBON%3E2.0.CO%3B2-N>

The American Mathematical Monthly is currently published by Mathematical Association of America.

Your use of the JSTOR archive indicates your acceptance of JSTOR's Terms and Conditions of Use, available at <http://www.jstor.org/about/terms.html>. JSTOR's Terms and Conditions of Use provides, in part, that unless you have obtained prior permission, you may not download an entire issue of a journal or multiple copies of articles, and you may use content in the JSTOR archive only for your personal, non-commercial use.

Please contact the publisher regarding any further use of this work. Publisher contact information may be obtained at <http://www.jstor.org/journals/maa.html>.

Each copy of any part of a JSTOR transmission must contain the same copyright notice that appears on the screen or printed page of such transmission.

The JSTOR Archive is a trusted digital repository providing for long-term preservation and access to leading academic journals and scholarly literature from around the world. The Archive is supported by libraries, scholarly societies, publishers, and foundations. It is an initiative of JSTOR, a not-for-profit organization with a mission to help the scholarly community take advantage of advances in technology. For more information regarding JSTOR, please contact support@jstor.org.

REVIEWS

Edited by **Harold P. Boas**

Mathematics Department, Texas A & M University, College Station, TX 77843

Mathematics: From the Birth of Numbers. By Jan Gullberg, W. W. Norton, 1997, xxiii + 1093 pp., \$50.

Reviewed by **Arnold Allen**

Gullberg's book has worthy competitors for the title *The People's Guide to Mathematics*. In fact, at this time there is a veritable cornucopia of excellent mathematics books for the general reader. Ones that I particularly like are those by Courant and Robbins (revised by Stewart) [3], Devlin [4, 5], Dunham [6], Hildebrandt and Tromba [8], Jacobs [9], and Stewart [12, 13] for surveys of mathematics. For enlightenment in more specialized areas, I like Casti [1], Conway and Guy [2], Körner [10], and Vilenkin [14]. Gullberg's book is clearly the overall winner. This book will appeal to a range of MONTHLY readers as well, from undergraduate math majors to instructors. It is a wonderful read. I take it with me everywhere I go: to the dentist's office, waiting in the doctor's office, to boring meetings—wherever I have an opportunity to read.

The book lived up to its description on the dust jacket, which included:

This gently guided, profusely illustrated Grand Tour of the world of mathematics takes the reader on a long and fascinating journey—from the dual invention of numbers and language, through the primary realms of arithmetic, algebra, geometry, trigonometry, and calculus, to the final destination of differential equations, with excursions into symbolic logic, set theory, topology, fractals, probability, and assorted other mathematical byways. . . . The text is interspersed with more than 1,000 original, high-quality technical illustrations, a multitude of reproductions from mathematical classics and other relevant works, and a generous sprinkling of humorous asides ranging from limericks and tall stories to cartoons and decorative drawings.

The sentence following the ellipsis explains some of the special charm of the book. Gullberg has made even more innovative use of the margin than Graham, Knuth, and Patashnik [7] did with their irreverent student "graffiti." Gullberg has excellent quotes and quips throughout the book, including the margin, but he also uses the margin for noting things mentioned in the preceding paragraph as well as for pointers to related topics, biographies of famous mathematicians, labels concerning the nearby text, photographs, and other uses too numerous to catalog.

Let me describe my ramblings in this remarkable book. The first chapter discusses the birth of numbers or "Where did numbers come from, anyway, and what are their properties?" This chapter is followed by two excellent chapters that describe systems of enumeration and types of numbers. The next chapter, "Cornerstones of Mathematics," is my favorite chapter and will appeal to beginners and old hands as well. I was amazed to learn in this chapter that the pencil-and-paper multiplication algorithm we learned in grade school is not the *only* such multiplication algorithm. Gullberg demonstrates "the Egyptian method of duplation" algorithm for multiplication. (He also displays a multiplication table

from the *Bomberger Rechenbuch* of 1483 which indicates that $7 \times 3 = 12$. Murphy's law had already been passed!) I loved his example of the "Russian peasant" method of "multiplication by successive duplation and mediation." I learned a dividing and averaging method, originating with the ancient Babylonians, for finding the square root of a number; it is efficient, too. I learned how to approximate $\sqrt{6}$ by a continued fraction and how to convert $221/41$ to the continued fraction

$$5 + \frac{1}{2 + \frac{1}{1 + \frac{1}{1 + \frac{1}{3 + \frac{1}{2}}}}}$$

I saw Pascal's triangle as Pascal drew it. Gullberg shows it as found in Pascal's book *Traité du Triangle Arithmétique*, Paris, 1665. We see it in another form from a book written in 1303 by the Chinese mathematician Chu Shih-chieh. Pascal was unaware of this earlier work and drew his triangle very differently from the way we now draw it. I learned how to use an abacus for multiplication and division. The decorative drawings in Figure 1 appear in the margin of the book next to the last four instructions for dividing 377 by 26 with the abacus.

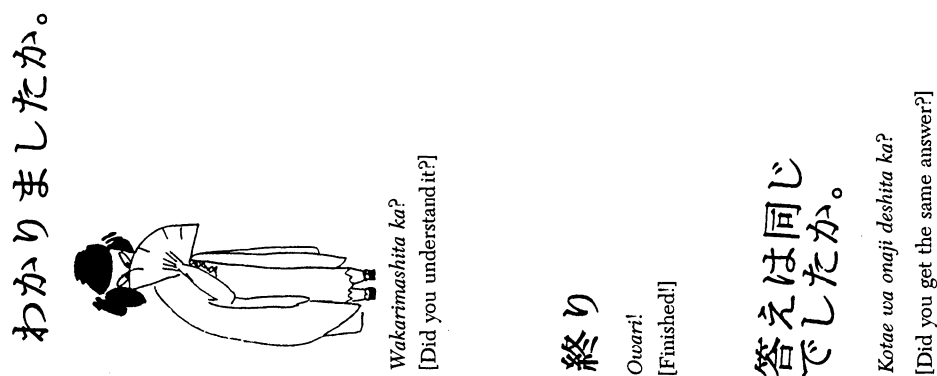


Figure 1

I was delighted by Gullberg's clear and brief chapter on combinatorics. In it he discusses several interesting combinatorial problems and their solutions. I especially liked the section on graph theory and the section on magic squares and their kin. In the former, he discusses the famous seven bridges of Königsberg problem. He even provides a map of Königsberg circa 1740! He describes Euler's solution of the problem as well as the history of the related four-color map problem. Gullberg describes and displays several famous magic squares, such as Dürer's remarkable order 4 magic square, constructed in 1514, and Benjamin Franklin's order 8 magic square with some unbelievable properties. Yes, *the* Benjamin Franklin. Franklin's magic square shown in Figure 2 appears in the margin of Gullberg's book.

Fibonacci's sequence and related sequences are well treated in the chapter on sequences and series. Immediately after his statement of Fibonacci's original

FRANKLIN Benjamin
(1706–1790)

52	61	4	19	20	29	36	45
14	3	62	51	46	35	30	19
53	60	5	12	21	28	37	44
11	6	59	54	43	38	27	22
55	58	7	10	23	26	39	42
9	8	57	56	41	40	25	24
50	63	2	15	18	31	34	47
16	1	64	49	48	33	32	17

Franklin's Magic Square

Figure 2

problem, Gullberg provides an amusing drawing of a cluster of rabbits. Then, in a magical two pages, he provides a great deal of interesting information about the Fibonacci (F_n), Lucas (L_n), and Pell (P_n) sequences, including a discussion of the golden ratio and the Binet formulas for F_n and L_n . Another peak experience for me in this chapter was reading the section on figurate numbers. Using graphic software to produce displays representing numbers by dots, Gullberg develops the properties of triangular, oblong, and pentagonal numbers in the plane. Then, using three-dimensional displays of dots, he derives the properties of cubic, tetrahedral, and square pyramidal numbers. Finally, he demonstrates how to extend tetrahedral numbers to superhedral numbers. An enjoyable chapter!

Fermat's last theorem has been in the news, but I found it difficult to explain to friends. Now I refer them to Gullberg's two-page discussion; it is at exactly the right level for those who are mathematically disadvantaged, but with some sophistication as well. Friends do not have to endure a discussion of elliptic curves and the Taniyama-Shimura conjecture as a journalism-educated friend of mine did when she bravely attended a math meeting with me.

The chapter "Theory of Equations" that contains the material on Fermat's last theorem also demonstrates, with worked examples, how to solve almost any kind of equation: quadratic, cubic, quartic, Diophantine; systems of linear equations, systems of linear and quadratic equations; and others. A pleasure to read!

I enjoyed Gullberg's brief but fascinating "Overture to the Geometries." It has the history and a quick sketch of the various branches. There are nice pictures, illustrations, and diagrams, including some elegant drawings of knots and other topological entities. I also liked the five chapters on geometry that follow, especially the section in the trigonometry chapter on solving triangles. Gullberg shows how to keep difficult geometry problems from becoming boring; he solves them with élan.

The most complete coverage of any subject in the book is given to mathematical analysis. There are chapters on differential and integral calculus and power series; detailed chapters on the major applications of calculus; a chapter on harmonic analysis with Fourier series; a chapter on methods of approximation; and an excellent introductory chapter on differential equations. Each chapter features theory as well as the solution of non-trivial problems.

I loved the probability chapter. There is a wonderful section on the history of probability with the names and achievements of most of the major players.

Gullberg also provides an excellent survey, with examples, of basic probability and statistics. He describes the basic distributions, such as normal and binomial, with their distribution functions and examples of how they are used. There is a photograph of a mustached gambler and his moll that looks suspiciously like Gullberg and his wife.

I bought my copy of Gullberg's book after leafing through it at a bookstore. It impressed me so much that I showed it to my colleagues at the office (I am part of a small R & D group). Everyone wanted to borrow it! I had to hide it in my desk to keep it from disappearing. One colleague got his wife a copy for her birthday—she is a high school math teacher. She loved it and showed it to their son's math teacher who is now an enthusiastic owner, too. To improve mathematics education in the USA we might begin by providing every high school math teacher with a copy of the book.

Later I learned that the large first printing was sold out almost immediately. Then I discovered that the Book-of-The-Month-Club had chosen it as one of its selections, and that the MAA has made it available to its members. The book has had the success that an author might dream of on writing a first book. Sometimes there is a bit of luck involved in becoming a best-selling author, perhaps an invitation to be a guest on Oprah Winfrey's show. But the success of Gullberg's book is not due to luck, or to Oprah: this really is a wonderful book! The dust jacket contains rave reviews from Martin Gardner, Philip Morrison, and Harold Jacobs. In addition, Peter Hilton wrote a forward "Mathematics in Our Culture."

What is the appeal of this book to the general reader? I could use a real estate analogy and say "Coverage, coverage, coverage." The book has excellent chapters on the standard material that most MONTHLY readers—as well as many engineers, scientists, and general readers (the "two cultures folks")—have studied somewhere before but would like to review. In addition, there are special chapters or sections of chapters on subjects that many of us have never seen before—such as the first several chapters that cover the birth of numbers and their applications; two algorithms in Chapter 4 for finding cube roots (Gullberg says, "We have found the good physician Trenchant's method an excellent cure for insomnia") as well as several methods for approximating cube roots; the section on the abacus, the slide rule, Napier's bones, and the quipu; and the incredible Chapter 11, "Overture to the Geometries," with much interesting material known only to specialists.

I am surrounded by engineers who do not use mathematics on a daily basis but who occasionally have special problems that need some mathematical analysis. Since I am the only one around who has a Ph.D. in mathematics, they sometimes come to me to ask basic mathematical questions. Now I can just refer them to the Gullberg book for standard material. I believe it will become a general reference for many MONTHLY readers. There are other uses of the book for MONTHLY readers. The possibilities for undergraduate student readers include:

- Reading the book to broaden their understanding of mathematics beyond their course work.
- Using it as a supplement to many of their courses, such as calculus, college algebra, geometry, and statistics.

The possibilities for instructors include the following:

- Using it as a textbook for courses such as *Mathematics for Poets* or *Calculus for Poets*. An experiment like this is being tried by Dennis Watson and his colleagues at Clark College in Vancouver, Washington.

- Using it as a supplementary textbook.
- Using it for extra credit research study and reports.

As an author, I must note possible uses of the book for authors of undergraduate textbooks. These include:

- Saving time and money for special figures or material by referring their readers to the book, rather than including the special material in their books. For example, I plan to refer readers of the book I'm writing to Gullberg's book for the history of probability and to show them what Pascal's triangle looked like to Pascal as well as to ancient Chinese mathematicians. This will be better than writing a history myself or getting the necessary permissions to make copies of the Pascal triangles.
- Using it as a source of ideas for material to discuss and for examples to emulate.

Gullberg's book is a gigantic book in every sense of the word. It weighs four pounds and thirteen ounces and has 1100 pages. (While reading this book is most enjoyable, it gives a whole new meaning to the phrase "heavy reading.") It took a giant effort to produce such a masterpiece. Gullberg spent more than ten years writing it, mostly at night after a full day as an active physician and surgeon. However, he got a lot of help, especially from his family. His son persuaded him to write it, provided most of the mathematical graphics, helped him keep his computer running, and counseled him about content. His wife, Ann, proofread the manuscript and drew many of the illustrations. Some others were done by their twin sons, Kamen and Kalin, when they were nine or ten years old. Gullberg also has talented friends in various disciplines who reviewed what he was doing, and he got some help from outside professionals. As he says in the preface, "My draft text was later polished with the help of distinguished professional mathematicians, linguists, and historians."

Although he got others to help him with the writing of the book, he did the actual writing using a Macintosh Plus and Microsoft Word 3.0. These were state-of-the-art when he began his writing, but are ancient relics now. It was a most challenging task to keep the Macintosh Plus going all those years and to hack the equations without LaTeX or a commercial software package. However, he did it. As he notes on the copyright page: "Camera-ready copy for this book was produced entirely by the author, utilizing a combination of modern desktop-publishing and traditional paste-up methods." This was an incredible achievement.

Peter Renz [11] describes some of the problems Gullberg had with his computer and how and why the book was written. Renz also gives a biographical sketch of Gullberg and some details of the production and publication of the book.

These are my three wishes for an encore from Dr. Jan Gullberg:

- Set up a web site so that we can have two-way communication with him. For example, instructors who are using his book could let him know why they decided to use it, and Dr. Gullberg could make this information available to others. Everyone could suggest new exercises, or potential improvements, or corrections, and he could post additional material, corrections, etc.
- Write a solutions manual for the exercises or commission someone to do so.
- Write a second volume containing material he hadn't time or room enough to put in the present book, such as Green's theorem, wavelets, encryption techniques such as trap door ciphers—the kind of material that is described

in Barry Cipra's series for the American Mathematical Society on what's happening in the mathematical sciences.

Jan Gullberg's book is a giant leap forward for mathematics and all those who love it!

REFERENCES

1. John L. Casti, *Five Golden Rules*, Wiley, 1996.
2. John H. Conway and Richard K. Guy, *The Book of Numbers*, Springer, 1996.
3. Richard Courant and Herbert Robbins, *What is Mathematics?*, second edition revised by Ian Stewart, Oxford University Press, 1996.
4. Keith J. Devlin, *Mathematics: The Science of Patterns*, W. H. Freeman, 1994.
5. Keith J. Devlin, *Mathematics: The New Golden Age*, Penguin Books, 1988.
6. William Dunham, *The Mathematical Universe*, Wiley, 1994.
7. Ronald L. Graham, Donald E. Knuth, and Oren Patashnik, *Concrete Mathematics: A Foundation for Computer Science*, 2nd ed., Addison-Wesley, 1994.
8. Stefan Hildebrandt and Anthony Tromba, *The Parsimonious Universe*, Springer, 1996.
9. Konrad Jacobs, *Invitation to Mathematics*, Princeton University Press, 1992.
10. T. W. Körner, *The Pleasures of Counting*, Cambridge University Press, 1996.
11. Peter Renz, A Long Loving Look at Mathematics, *Math Horizons*, April 1997, 16–22.
12. Ian Stewart, *Nature's Numbers*, Basic Books, 1995.
13. Ian Stewart, *From Here to Infinity: A Guide to Today's Mathematics*, Oxford University Press, 1996.
14. Naum Yakovlevich Vilenkin, *In Search of Infinity*, Birkhäuser Boston, 1995.

Hewlett-Packard Advanced Technology Center, 8000 Foothills Boulevard, MS 5740, Roseville, California 95747

arnolda@jps.net

EDITOR'S CORNER. I am a mathematician today because of an experience in kindergarten. I have always been interested in analyzing patterns, and from an early age I was excited by all sorts of intellectual games having a strong element of pattern recognition: chess, go, Scrabble, crossword puzzles, and so forth. The first really sophisticated pattern-recognition task that young children face is learning to read, and I was starting to read at home before I began formal schooling. However, because reading was on the syllabus for first grade, my kindergarten teacher viewed reading as a proscribed activity and successfully quashed my initial enthusiasm for the printed word. Consequently, I redirected my energies toward arithmetic, which the teacher apparently did not recognize as a subversive subject. The result was that later on, I was always a year ahead of my schoolmates in mathematics, and so I ended up a mathematics major in college. Thus, it is thanks to my kindergarten teacher that I am today a specialist on the theory of the Bergman kernel function rather than on, say, the works of Jane Austen.

There is a moral in this story for the public school system, but I should like to address instead what this story suggests about how to teach mathematics effectively. It is a familiar metaphor that mathematics is a language, and in my early experience mathematics and language were both difficult—and therefore interesting—for the same reason. Both subjects to me were games presenting an artificial universe operating by well defined, albeit arbitrary, rules. The goal was to understand the rules and their consequences so thoroughly that they became internalized and automatic, in which case one could justifiably claim to have solved the game. It is in this sense that a sixth-grader who can unscramble Rubik's cube rapidly while blindfolded can assert mastery of that game.

Now if mathematics is a language, why are the standard methods of teaching mathematics not even remotely similar to the standard methods of teaching

languages? The way to become fluent in a language is total immersion. Has anyone tried to foster mathematical ability by the same method? Actually, yes: intensive summer programs for teenagers, such as the famous one developed at Ohio State by Arnold Ross, have indeed proved effective. However, the standard mathematics program in a typical American school is more akin to wading than to immersion. If our children spend one-fourth the time on mathematics that they spend watching television, is it any wonder that they fared poorly in the recent Third International Mathematics and Science Study? (See <http://www.csteep.bc.edu/timss> for detailed information about TIMSS.)

Children seem automatically to soak up their native language. A foreign language is a better comparison to mathematics. In French class, for example, students get practice in speaking French, reading French, and writing French; drill on French vocabulary and grammar; and exposure to French culture and history. Compare this with mathematics instruction. It is an uncommon mathematics class that pays much attention to mathematical culture and history. Although the so-called "reform" movement supports giving students practice on reading and writing mathematics, this idea is spreading slowly. If you have not tried the experiment, assigning your mathematics class a writing task will be an eye-opening experience. At the beginning of the semester, I assigned a class of engineering students to write a short essay interpreting part of the introductory chapter in their differential equations textbook. Ten percent of the students immediately dropped the course. I was chagrined to discover that of those students who completed the assignment, about one-third had not understood the book's discussion of implicit solutions versus explicit solutions because they did not know the meaning of the word "implicit." It is a struggle to teach students in a way that is different from the way they were taught in grade school and high school.

Please note that I am not complaining that students are getting worse and that the world is going to the dogs. (This is true, and has been true throughout recorded history, but that is another story.) Actually, teaching college mathematics is a rewarding experience if one takes advantage of the skills that modern students have. My students cannot do arithmetic rapidly and may not comprehend words derived from Latin roots, but they have well developed social skills, know how to work collaboratively in groups, can give coherent oral presentations, and are highly creative if given a little encouragement. I fondly remember one response to an examination question I posed requiring the students to invent a scenario involving a swimming pool for which a given differential equation would be an appropriate model. The solution I expected was a mixing problem concerning the concentration of chlorine, but one student's (mostly correct) answer began: "Kim drops a calculator into a swimming pool from a height of 100 meters . . ." It is not the case that today's students cannot think, but it is true that their intellectual and cultural backgrounds are different from those of their teachers. My point is that, like generals who prepare to fight the previous war, textbook expositors tend to write prose for the previous generation.

In a standard mathematics book, what gets taught is primarily mathematical vocabulary and rules of mathematical grammar. Perhaps in advanced undergraduate classes, students may begin to learn some principles of mathematical composition, but it is only in graduate school that one gets exposed to the mathematical analogues of fine literature and poetry.

It would be wonderful to have some textbooks that go beyond mathematical vocabulary and grammar to incorporate the mathematical equivalents of literature, poetry, culture, and history in a way that students can understand and appreciate.

Reading Arnold Allen's review of Jan Gullberg's *Mathematics: From the Birth of Numbers* made me think that it might be such a book, so I obtained a copy and read it. My impressions of the book are those of a university professor of mathematics active in both research and teaching.

The first impression one gets from Gullberg's massive tome is that producing it was a tremendous effort. Gullberg is a remarkable person: not a professional mathematician, he had the motivation, enthusiasm, and dedication to spend a decade learning about mathematics and recording his findings. His book is an epic written by an amateur.

It is not surprising that the best parts of the book are the ones that do not involve advanced mathematics. An amateur has the opportunity for originality of presentation when discussing the history of mathematics and those topics generally known as "recreational mathematics." It is here that Gullberg shines. Even professionals will find some amusing tidbits in the book. For example, I did not know that the circumcenter, centroid, and orthocenter of a triangle are on the same line, and reading this statement in Chapter 12 sent me to the library to look for a geometry book with proofs in it.

The second half of the book, where Gullberg tackles calculus and other parts of the university mathematics curriculum, disappointed me. Presumably Gullberg learned his calculus from a standard textbook, and his sections on calculus read like a distillate of any traditional calculus book. In Gullberg's encyclopedic work, there is little space for discursive exposition, and the impression that comes across is that mathematics consists of rules, formulas, and algorithms. If an educated layperson with extraordinary motivation has this concept of mathematics after studying our textbooks, then we writers of mathematics books have failed miserably.

In any book of over 2^{10} pages, there are mistakes. I found fewer than expected. There are some typographical errors, such as on page 570 where the eccentricity of an ellipse is given as $\epsilon < 0$ instead of $\epsilon < 1$. Then there are some mathematical misconceptions, such as the confused statement and proof of Cauchy's mean-value theorem on pages 718–719, where Gullberg demands that the two functions have matching values at the endpoints (which makes the theorem rather trivial). I found only one true howler: on page 735, Gullberg comes unstuck calculating the indefinite integral of the function f defined by $f(x) = 1/(\sqrt[3]{x} + \sqrt[4]{x})$ and obtains a wrong answer that is even singular at $x = 1$.

Gullberg is writing at the limit of his knowledge, and it shows. Every college mathematics teacher who reads this book will wince at some statements that are not exactly wrong, but that will certainly mislead naive readers. Here are some examples—admittedly taken out of context—of statements that make me queasy.

- "with the assistance of computers, we can easily obtain approximate values of virtually any convergent series" (page 282)
- "points on the graph of a function may approach successively nearer to a straight line, the **asymptote**" (page 341)
- "**topology** is a **non-metric geometry**" (page 369)
- "Unlike matrices, which may be of any rectangular shape, determinants are always square." (page 646)
- " $i^i = e^{-\pi/2}$ " (page 793)
- "A differentiable function of one independent variable has a maximum or a minimum where its first derivative is zero." (page 816)

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