Thurston's approach to the Riemann Mapping Theorem via circle packings was completed by Rodin and Sullivan [Rodin-Sull]. Given a bounded, simply-connected domain Ω in the complex plane, the goal is to approximate a Riemann mapping that takes the open unit disk D onto Ω by circle packing mappings. One chooses a penny size, say $1/i$, and fills Ω as nearly as possible with a connected portion P_i of the hexagonal penny packing H_i, where the underlying triangulation K_i defined by P_i is a closed topological disk. The Discrete Uniformization Theorem yields a packing P_{K_i} of the open unit disk D by circles whose tangencies correspond exactly to the edges in K_i and whose outer, or boundary, circles are all tangent to the boundary circle of D. The correspondence between the circles of P_{K_i} and those of P_i can be used to define a mapping from most of D to most of Ω. The Rodin-Sullivan Theorem claims that, after a minor normalization, these partial mappings converge to a Riemann mapping from D onto Ω. (Figure 8)

The original proof made strong use of the combinatorics of the hexagonal penny-packing. Other authors have removed many of the restrictions involved. The best result to date seems to be that of He and Schramm (see the references in this book).

REFERENCES

[Andreev] Andreev, E. M., "Convex Polyhedra in Lobaĉevskii Space," *Mat. Sbornik* 81, No. 123 (1970a). [Russian]

"Convex Polyhedra in Lobaĉevskii Space," *Math. USSR Sbornik* 10 (1970b): 413–440 [English].

"Convex Polyhedra in Lobaĉevskii Space," *Mat. Sbornik* 83 (1970c): 256–260 [Russian].

"Convex Polyhedra of Finite Volume in Lobaĉevskii Space," *Math. USSR Sbornik* 12 (1970d): 255–259 [English].

[Ford] Ford, Lester R., "Fractions," *American Mathematical Monthly* 45 (1938): 586–601.

[Kapovich] Kapovich, Michael, *Hyperbolic Manifolds and Discrete Groups*, Birkhäuser, Boston (2001): 467 pages.

[Koebe] Koebe, P., "Kontaktprobleme der konformen Abbildung," *Ber. Sächs. Akad. Wiss. Leipzig Math.-Phys. Kl.* 88 (1936): 141–164.

[Morgan] Morgan, John W., "On Thurston's Uniformization Theorem for Three-Dimensional Manifolds," in *The Smith Conjecture*, Morgan, John W., and Bass, Hyman, eds., Academic Press, Orlando, San Diego, San Francisco, New York, London, Toronto, Montreal, Sydney, Tokyo, São Paulo (1984): 37–125.

[Rodin-Sull] Rodin, Burt, and Sullivan, Dennis, "The Convergence of Circle Packings to the Riemann Mapping," *J. Differential Geometry* 26 (1987): 349–360.

[Thurs1] Thurston, William P., "The Geometry and Topology of 3-Manifolds," *Princeton University Notes*, preprint.

[Thurs2] Thurston, William P., "The Finite g Mapping Theorem," invited talk (An International Symposium at Purdue University in Celebration of de Branges' Proof of the Bieberbach Conjecture, March 1985).

J. W. Cannon
Department of Mathematics
Brigham Young University
Provo, Utah 84602
USA
e-mail: Cannon@math.byu.edu

W. J. Floyd
Department of Mathematics
Virginia Tech
Blacksburg, VA 24061
USA
e-mail: floyd@math.vt.edu

W. R. Parry
Department of Mathematics
Eastern Michigan University
Ypsilanti, MI 48197
USA
e-mail: walter.parry@emich.edu

Introduction to Cryptography with Coding Theory, Second Edition

by Wade Trappe and
Lawrence Washington

SADDLE RIVER, NJ, PRENTICE-HALL, 2006,
592 PP., US$ 90.20, HARDCOVER,
ISBN 0-13-186239-1

REVIEWED BY MICHAEL ANSHEL
AND KENT D. BOKLAN

Most ten-year-old boys and girls run around a lot. Many play video games. Some accidentally download computer viruses. And quite a few invent secret codes, their very own means of disguising their communications from parents and peers. Children quickly learn the rules of cryptography: their techniques must be efficient and their methods must be able to be undone, too. (Budding cryptanalysts, who spend their efforts breaking the systems of their classmates, are scarcer than young cryptographers.) It's the bread and butter of cryptography, the encrypting, and there's a popular mythology to Top Secret ciphers and spy intrigue—with the television shows with the *strong encryption* that somehow always manages to get broken. Today we are inundated with media pronouncements of *strong* (or *strongest!*) protections with such ubiquitous phrases as, "128 bit encryption." It seems that everyone does it or claims to do it. Even I can do it, with the Captain Midnight decoder badge that I bought on e-bay. But exactly how does it all work? Cryptography is not just the latest trend, like the hula hoop, Betamax, and the Spice Girls. It's here, it's not going away, and someone needs to know how it really works—and if it's really strong.

Ah, but a man's reach should exceed
his grasp, or what's an SSL for?

An excellent first step toward the understanding of the black boxes of (commercial) encryption is to work through *Introduction to Cryptography with Coding Theory*, second edition, by Wade Trappe and Lawrence Washington (which we dub WaTr for purely metrical purposes). Read it and you'll learn the answer to that mysterious question, "What's [in] that SSL thing?" You may still fumble, though, when your friends ask you, "Should I really trust amazon.com with my credit card number?" An introduction to cryptology, the sum of cryptography and the cryptanalysis, usually starts with a fundamentals class at the elective undergraduate or early graduate level. WaTr fills about two of these courses, two semesters worth, and it's aimed at an audience of computer science, engineering and mathematics students. But this text is not just replete with the classical ciphers—the Vigenères and the Enigma's—but is full of the flotsam and jetsam that fill the ether about them, those cryptographic primitives and applications (like the key distribution protocols and the digital signatures) that are the backbone of the few high-profile protocols upon which so much of today's data security rests.

WaTr provides pedagogy in two distinct voices. Unfortunately, this duality is often distinguished by the strengths of the expositions. As we are told in the preface, WaTr plans to "cover a broad selection of topics from a mathematical point of view." To be comprehensive is a near Herculean labor. Some volumes, like [2] and [6], do very well to touch upon almost all of the notable features of cryptography today, but they are not texts for a first lesson in the mechanics of *how* and *why* and the mathematics behind it all. WaTr features a sound balance of methods and attacks; it is a pleasure to read. There are the occasional proofs of the mathematical statements, when the proofs are elementary, but WaTr is about a wider introduction. Certainly, a lot lurks hidden beneath the surface, including the hidden Markov models. Trappe and Washington fittingly point to many of the deeper ideas, especially in the theory of elliptic curves, and they keep the reader both aware and enticed for further study. On the down side, the privation of implementation details and implementation issues in WaTr is a real loss for the student who wants to run with the encryption ball; the devil, after all, is in the cryptographic small print. There are exceptions, though, and WaTr does include the very clever work of [4]. But this is a first text and, as such, serves well.

This second edition of WaTr features several important additions to the first edition, including identity-based public key cryptography, an elegant construction which holds substantial promise in future applications. Significant cryptanalytic advances in the theory of hash functions are included. The study of hash functions (and collision-finding) is experiencing a revival due to exciting work beginning with [3] and culminating in [7]. Thanks to these efforts, we're now looking for new hash algorithms because our faith in the old ones has been ruffled. Also new to the second edition of WaTr is a chapter on lattice methods (including the Lenstra-Lenstra-Lovasz method for finding short vectors). Notable by its absence, though, in both the first and second editions of WaTr is the Merkle-Hellman Knapsack scheme, the Icarus of public key cryptosystems. Knapsack was all the rage in the late 1970s: it was elegant and based upon a known NP-hard problem (unlike the RSA system). Shamir, in 1982, shook the foundation and certainly the confidence of the young field of modern cryptography by cracking it—and in so doing changed the face of (public key) cryptography and cryptanalysis to this day. The story of Knapsack is part of the history. It makes for great reading, it's high drama, and it provides a strong lesson. But it's not in WaTr and it should be.

What is in WaTr and is a highlight of the text is the gentle introduction to DES, (which was) the **D**ata **E**ncryption **S**tandard. WaTr presents it slowly, a few rounds at a time. Block ciphers, like DES, 3DES ("triple DES") and Rijndael (the new standard, the **A**dvanced **E**ncryption **S**tandard) are the load-bearers of data encryption. They are each composed of rounds, and a single round is a structured shaking of the input. Starting with the plain text input to the first round and repeated on the output of the previous round, a block cipher is designed with enough rounds so that the result, the cipher text, is jumbled enough—meaning that the influence of the input on the output (and vice versa) is fully diffused. The mixing steps are usually a combination of permutations and substitutions and some non-linear lookups (DES has some famous S-boxes that do this) all the while being designed to be invertible so plain text can be recovered. WaTr explains the workings of DES in parallel with the cryptanalytic method of differential cryptanalysis. By so doing, it becomes clear(er) why DES has 16 rounds. The discourse does get a bit technical. However, the parallel presentation is well worth the effort of careful study. The best cryptographic algorithm designs are structured around what attacks are known and then laid out to be resistant to them.

For symmetric key protocols, like block ciphers, it's all about the muddling and the repetition of the processes. For asymmetric schema, as in public key cryptography, designs are predicated upon mathematical problems that are "easy" (computationally efficient) to perform but believed to be "hard" (computationally infeasible) to invert—without some extra piece of knowledge, a key. These problems are called trapdoor one-way functions and are not to be confused with one-way functions for which there is no key to undo them. (Hash functions are one-way functions.) There is no real proof that trapdoor one-way functions exist since obtaining lower bounds for these kinds of complexities seems near impossible. There is faith, based upon many years of very limited success, in a few select problems: the discrete logarithm problem and that of finding, for some e, an e-th root modulo a number of unknown factorization.

The paradigm of "easy to do but hard to undo" lies at the heart of cryptography.

Discrete logarithm problems (dlp's), as involved in, for example, the classical Diffie-Hellman key agreement protocol, take a form such as: find x if

$$7^x \equiv 24347112357648226690407\!30 \pmod{40834971043785538712805\!49}.$$

WaTr's treatment of the discrete log problem and approaches to solve it, the Pohlig-Hellman algorithm and the index calculus, are exemplary for first-year students. The hard (but nevertheless toy-sized) dlp above can be solved on your laptop. When the modulus has several hundred digits, things get very tough. (The index calculus approach, while sub-exponential complexity, does not scale well enough to be efficient.)

The RSA architecture involves raising a message, m, to a fixed known power, e, modulo a number n whose factorization is a secret (and e and n are relatively prime). A result may look something like this (for $e = 31$):

$$\begin{aligned} &m^{31}\\ &\equiv 19705178523446373241426321\!45\\ &\quad 56420972406776330386397873104\!57\\ &\quad 022491789\\ &\quad (\mathrm{mod}\ 495960937377360\\ &\quad 604920383605744987602701101399\!3\\ &\quad 99359259262820733407167). \end{aligned}$$

Breaking RSA is about finding m. If n can be factored, this is easily accomplished. (Raise both sides of the equation above to the power d where

$$d^{-1} \equiv e \pmod{\phi(n)}.$$

That recovers m. The proof is a simple application of Euler's generalization of Fermat's Little Theorem.) It is unknown if there is a way to find m that is more efficient than factoring the modulus. Since factoring special types of large numbers is believed to be hard, the RSA system, with a sufficiently large, hard modulus is currently considered secure. (The example presented here is, hopefully, a small step towards dispelling the common misconception that an RSA modulus need be the product of two large primes. For efficiency, it ought to be—or close. It need not be, though.) WaTr gives a quick overview of some factoring techniques; enough to convince the would-be RSA codebreaker that things can be tremendously challenging.

The questions of the (computational) equivalence of the RSA problem and of factoring—and of the discrete logarithm problem and the Diffie-Hellman protocol—are amongst the most important open issues in cryptology today. Progress has been made on the latter question (see [5]) in the affirmative direction. On the former, the recent work is less than convincing.

WaTr really shines in its initiation into the world of elliptic curves and elliptic curve cryptography. From a simple introduction to the group law to H. Lenstra's beautiful elliptic curve factoring method (which can solve the RSA question in this review) to the elliptic curve analogue of the discrete logarithm problem and the Diffie-Hellman protocol, WaTr provides a fine rendering for the initiate. The elliptic curve one-way trapdoor function is simple: given an elliptic curve E defined over a finite field, a point P on E and k some positive integer, find k given kP (where $kP = P + P + P + \cdots + P$, k times). Again, it seems (computationally) difficult—or infeasible—to do this for large enough carefully chosen examples. There's a lot of data security (and commercial products) banking on that.

There are unfortunate omissions in WaTr. There's no real discussion of (algorithmic) complexity where it may have been well-placed to provide the reader with a sense of appropriate key sizes and protocol (and attack) strength. And there's the sporadic lack of the sense of largeness, the why's of *why are things like this?*. More generally, what is incidental and what is of real import in the digital world is not always clear. These gaps, though, are alleviated in part by an assortment of excellent (and detailed) end-of-chapter exercises and computer problems that allow and encourage the reader to identify some of the subtleties and gain a deeper appreciation of the why's.

WaTr skips almost the whole field of stream ciphers. That's a shame. Stream ciphers are a major component of encryption technology today. And WaTr features only a cursory look at linear feedback shift registers, the primary constituent of most stream ciphers over the past century and many very good random-number generators. Linear feedback shift registers (and their associated tap polynomials) are rich in mathematical theory and can be designed and combined to provide very satisfactory output. Bad random-number generators, at least for cryptographic purposes, are based upon simple linear congruential generators of the form

$$x_n \equiv Ax_{n-1} + B \pmod{m}$$

where m is fixed and A and B (and x_0) are unknowns (but chosen so that the period of the generator is large). One can easily deduce the next "randomly" generated number from knowledge of the previous three—and this predictability makes for a very bad random-number generator. (Yet this is how many *rand* functions work!) Stream ciphers are needed for real time encryption when you can't wait for a whole block of plain text to arrive before you use your block cipher. Stream ciphers aren't just for voice communication anymore.

Cryptography sells, from the great propaganda of "the only provably secure system" (one-time pads) to the introduction of quantum cryptography. Using principles of quantum mechanics for cryptographic applications is an idea now a few decades old—and remains ever intriguing. It also makes for great press. Most notable among quantum methods is the key exchange protocol introduced by Bennett and Brassard which allows legitimate participants to (probabilistically) recognize the existence of an eavesdropper on their communication. It's a lovely idea that requires substantial overhead (a channel so clean that a photon in transit is undisturbed). WaTr presents the ideas, this glimpse of a possible future with quantum cryptography and with quantum computers (if substantial ones can ever be built). Then, with Shor's algorithm, the pre-eminent quantum computational cryptanalytic tool, most everything would change—for security, for the Internet, and for cryptology—leading us to wonder, in the words of Buffy, "Where do we go from here?"

A world of post-quantum cryptography is being studied in anticipation of one plausible future. Non-abelian approaches have been suggested which do not seem to succumb to quantum attacks. Though such ideas are not in WaTr, for they are still in their early development, these considerations are providing new avenues of investigation. ([1] offers an analogue of the Diffie-Hellman key establishment protocol wherein, instead of a discrete logarithm problem, the restricted conjugacy search problem serves as the trapdoor one-way function.)

WaTr tries to cover a lot: the past, the present, and the (uncertain) future. It is occasionally uneven in its mathematical level, the knowledge expected of the reader. The Information Theory and the Error Correcting Codes chapters are not as carefully composed as much of the rest of the book and do not have the same (encouraging) instructional rhythm. The latter part could benefit from some compression and reordering, and the Information Theory section could afford some expanded coverage of language recognition. (How does your computer know an acceptable decryption when it finds one?)

WaTr is the best book of its kind. Appendices of Matlab, Maple, and Mathematica exercises support the rhetoric of the individual chapters because in cryptology small examples can give a false sense of security. We can quibble with what's not in WaTr, but you can't do it all at once. And what WaTr does is almost always done well. To do it all—that would be as daunting as the task of breaking "128 bit encryption," whatever that is.

REFERENCES

[1] I. Anshel, M. Anshel, D. Goldfeld, An algebraic method for public-key cryptography. *Math. Res. Lett.* 6 (1999), 287–291.

[2] Menezies, van Oorschot and Vanstone, *Handbook of Applied Cryptography*, CRC Press 1997.

[3] A. Joux, Multicollisons in iterated hash functions. Application to cascaded constructions, *Advances in Cryptology—CRYPTO 2004, Lecture Notes in Computer Science* 3152, Springer-Verlag, 2004, 306–316.

[4] P. Kocher, Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems, *Advances in Cryptology—CRYPTO 96, Lecture Notes in Computer Science* 1109, Springer-Verlag, 1996, 104–113.

[5] U. Maurer, Towards the Equivalence of Breaking the Diffie-Hellman Protocol and Computing Discrete Logarithms, *Advances in Cryptology—Crypto '94, Lecture Notes in Computer Science* 839, Springer-Verlag, 1994, 271–281.

[6] B. Schneier, *Applied Cryptography*, 2nd edition, John Wiley, 1996.

[7] X. Wang, Y. Yin, H. Yu, Finding collisions in the Full SHA-1, *Advances in Cryptology—Crypto 2005, Lecture Notes in Computer Science* 3621, Springer-Verlag, 17–36.

Michael Anshel
Department of Computer Sciences
The City College of New York, CUNY
138th Street and Convent Avenue
New York, NY 10031
USA
e-mail: anshel@cs.ccny.cuny.edu

Kent D. Boklan
Department of Computer Science
Queens College, CUNY
65-30 Kissena Boulevard
Flushing, NY 11367-1597
USA
e-mail: boklan@boole.cs.qc.edu

Dr. Euler's Fabulous Formula: Cures Many Mathematical Ills

by Paul J. Nahin

PRINCETON, NJ, PRINCETON UNIVERSITY PRESS, 2006. xxii + 380 PP. $29.95 ISBN: 978-0-691-11822-2; 0-691-11822-1

REVIEWED BY PAMELA GORKIN

It was an uninteresting assignment, except for the tenth problem: Evaluate

$$\int_0^\infty \frac{\sin x}{x}\,dx.$$

I remember thinking, "You can't do that." Then I figured it out. It was one of those mathematical moments that makes you say "wow." Paul J. Nahin's book, *Dr. Euler's Fabulous Formula: Cures Many Mathematical Ills*, is filled with such moments. The book, like its title and cover, is clever, creative, and unique. It contains every short story Nahin can think of that uses $e^{\pi i} + 1 = 0$, plus a few that don't. You might know that Euler's formula was one of the most frequently cited "great equations," according to a poll conducted by *Physics World* in 2004. In 1990, readers of *The Mathematical Intelligencer* voted it the most beautiful of 24 formulas, with a score of 7.7/10. Why did this equation receive such a high score? Many people cite its simplicity and brevity, as well as the connection between five important constants in mathematics. Though there are dissenters, most mathematicians agree: this formula needs no introduction.

Nahin has a gift for recognizing good stories and has put together a collection of mathematical "tales" about Euler's formula that would make a fine addition to a differential equations or complex analysis class. The reader should, however, be forewarned: although the back cover informs us that the book is "accessible to any reader with the equivalent of the first two years of college mathematics," to read and enjoy this book, most readers will need more mathematical maturity. In addition, though Euler's formula may need no introduction, applications of Euler's formula need motivation—and they don't always get it in this book.

Many of the formulas and computations included are among the highlights of a typical complex analysis course (Wallis's formula, for example). There are also many stories that will be new to readers. There is an account of the Gibbs phenomenon, which is a story with a fascinating history. (A longer version of this history, without Nahin's biography of the overlooked Henry Wilbraham, appeared in an article by Edwin Hewitt and Robert E. Hewitt in 1979.) A wonderful chapter titled "Vector Trips" features R. Bruce Crofoot's story about his dog Rover. Crofoot runs a pretty complicated path, which he sketches for the reader, each morning. He is the proud owner of a well-trained dog who always runs exactly one foot to his owner's right. Given the path, the owner, and the dog, it turns out that Crofoot runs farther than Rover. The question is: How much farther did Crofoot run? I liked the article when I read it in *Mathematics Magazine* and I liked it here too. It's not really an application of Euler's formula, but it is a nice use of complex numbers and vectors.

On the other hand, the discussion of the vibrating string problem (as well as a development of a solution to the wave equation) really does use the fact that $e^{ix} = \cos x + i \sin x$ in an essential way. This serves as the introduction to the story of what "was probably (almost certainly) the first 'Fourier series'." When you think of Fourier series you probably don't think of funny stories, but in Nahin's hands they become amusing. He presents Euler's "remarkable claim" that

$$\frac{\pi - t}{2} = \sum_{n=1}^{\infty} \frac{\sin(nt)}{n}$$
$$= \sin(t) + \frac{\sin(2t)}{2} + \frac{\sin(3t)}{3} + \cdots.$$

As Nahin points out, this is indeed remarkable, in part because it is not true (check out what happens at $t = 0$). But now Nahin has your attention; now you should want to know the story behind Euler's claim.

Other stories would have benefitted from a little motivation. Nahin presents the "beautiful formula"

$$\sum_{n=1}^{\infty} (-1)^{n+1} 1/n^2 = \pi^2/12$$

and Euler's result "which made him world famous":

$$\sum_{n=1}^{\infty} 1/n^2 = \pi^2/6$$

These are followed by more sums, including one "dazzling result," a "spectacular application of Parseval's formula," a "pretty result," and "an even *more* beautiful generalization" of it that will appear in the succeeding chapter. Now, "excited" is not the first word that comes to mind to describe my students