from *SIAM News*, Volume 34, Number 4

A Tale of Two Technothrillers . . .

Cryptonomicon. *By Neal Stephenson, HarperPerennial Library, New York, 2000, 918 pages, $16.00 (paper).*
The Bear and the Dragon. *By Tom Clancy, Putnam Publishing Group, New York, 2000, 1028 pages, $28.95 (hardcover).*

The reader's first clue that Neal Stephenson's 1999 novel *Cryptonomicon* is a little unusual comes at the top of page 10, with, of all things, a displayed equation:

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \ldots,$$

where, the author notes, "*s* is a complex number." A quick thumb-through reveals other displayed equations, graphs, and some computer code. There's even an appendix, for crying out loud. And footnotes.

What the heck kind of novel is this?

That's easily answered: *Cryptonomicon* is a technothriller. And as technothrillers go, it's a good one. Especially if you like a little mathematics mixed in with your technothrills.

Everything You Always Wanted To Know about Specs . . .

BOOK REVIEW
By Barry A. Cipra

The term "technothriller" entered the language as a descriptor for Tom Clancy's 1984 submarine novel *The Hunt for Red October*. Clancy, whose day job was selling insurance, had pored over unclassified military manuals and documents and turned what he learned into detailed descriptions of weapons systems, sonar, and other technutiae of the nuclear-powered cat-and-mouse game played by U.S. and Soviet submariners. In *Red October*, the human characters are barely one-dimensional, but the *techno*-characters are fully fleshed (or hardwared) out. The real hero of *Red October* is not Clancy's future president, Jack Ryan; it's the *U.S.S. Dallas* attack submarine. (Personal note: In a short stint as a mathematical consultant working on a project for the U.S. Navy, I spent two and a half fun-filled weeks on the *Dallas*. I fully agree with Clancy in his admiration for the professionalism of officers and crew who spend months at a time underwater.) Here's a typical Clancy passage:

> A P-3B was cruising at nine hundred feet about fifty miles southeast of Norfolk. The FLIR showed nothing, no heat signature on the surface, and the MAD gear detected no measurable disturbance in the earth's magnetic field, though one aircraft's flight path took her within a hundred yards of the *Alfa*'s position. The *Konovalov*'s hull was made of non-magnetic titanium.

Actually, Clancy (or his editor) has toned down the techno-passages considerably in his recent bestsellers. It's too bad, really. Part of the pleasure in reading Clancy comes from the feeling that you're learning something about the way things work (or in some cases don't work the way they're supposed to). But there's still a soft spot in Clancy's word processor for technical detail. For example, his latest opus, *The Bear and the Dragon*, opens with one of the main characters getting into a bullet-proof Mercedes 600, "the big one with the S-class body and twelve cylinders of German power under the hood":

> The windows were coated with dark plastic, which denied the casual onlooker the sight of the people inside, and the windows were thick, made of polycarbonate and specced to stop anything up to a 12.7-mm bullet, or so the company had told Golovko's purchasing agents sixteen months before.

Clancy's chief device for keeping you reading is to switch scenes every couple of pages. *Bear/Dragon* is slowly woven together out of seemingly disjoint story lines: the killing of a Russian mobster, the seduction of a Chinese politician's secretary by an American spy posing as a Japanese businessman, the discovery of oil *and* gold in Siberia, and the arrival in China of a diplomat-cum-spook from the Vatican, just for starters. Overseeing the action is President Jack Ryan, former spy and all-around good guy, who rails against the constraints of office and other people's inability or unwillingness to simply do what's right for the nation, and damn the political fallout.

Internet's Rainbow

Like Clancy, Stephenson weaves several story lines together. In fact, *Cryptonomicon* is almost two separate novels. One is a World War II tale of survival and espionage, the other a modern-day story of high-tech corporate intrigue involving an Internet venture. The stories hang together by threads of genealogy and geography: The main character in the modern-day story is the grandchild of one of the main characters from the WWII story, and much of the action in both takes place in the Philippines.

The Internet story mainly follows Randy Waterhouse, a thirtysomething Silicon-Valley type who joins an Internet startup that plans to create a "data haven" in the Philippines. Stephenson paints a delightful picture of the cut-throat world of e-business, with

a wonderful send-up of how a business plan is put together and what the boilerplate really means. There are also some techno-passages on the justifiably paranoid nature of computer security experts.

The World War II story follows three main characters: Lawrence Pritchard Waterhouse (grandfather of Randy), Bobby Shaftoe (whose son and granddaughter appear in the modern-day setting), and Goto Dengo (who actually appears in both stories). Lawrence Waterhouse is a mathematician and pipe-organ enthusiast who discusses decidability with Alan Turing at Princeton and becomes part of the Ultra crowd at Bletchley Park. Shaftoe is the classic dogface soldier who carries out the grunt work of war. And Goto is his Japanese counterpart.

The Shaftoe/Goto stories of survival are reminiscent of Norman Mailer's *The Naked and the Dead.* Stephenson is no Mailer, but he's oodles better than Clancy. Stephenson's forte is the lengthy, page-consuming build-up of descriptions, often in the form of extended analogies. Here's part of a page-long paragraph detailing Shaftoe's first encounter with a Vickers machine gun, whose size and power remind him of a saw he saw in high school:

> But then one summer he worked in a mill where they had a bandsaw. The bandsaw, its supply of blades, its spare parts, maintenance supplies, special tools and manuals occupied a whole room. It was the only tool he had ever seen with *infrastructure*. . . . Anyway, the most noteworthy thing about the bandsaw was that you could cut anything with it and not only did it do the job quickly and coolly but it didn't seem to notice that it was doing anything.

Not all of Stephenson's similes work, and a multipage, character-building excursus on Randy Waterhouse's penchant for Cap'n Crunch goes off track when Stephenson ascribes the cereal to General Mills. Cap'n Crunch is made by Quaker Oats. This is not a completely trivial point: Part of the appeal of a technothriller is the feeling that all the details are accurate. Publishers of the genre owe it to their clientele to employ fact checkers.*

But let's get back to those displayed equations.

Cryptic Passages

There are occasional references to math in Clancy, usually in connection with cryptography. Here's *The Bear and the Dragon* on a supercomputer built by Thinking Machines, Inc., for the National Security Agency: "This machine, whose manufacturer had gone bankrupt some years before, had been both the pride and joy and the greatest disappointment in the huge collection of computers at NSA, until quite recently, when one of the agency's mathematicians had finally figured out a way to make use of it." There are also allusions to quantum computing, as when Ryan's national security adviser tells him that "The guys at Fort Meade are playing with using quantum-physics equations to crack ciphers, and evidently they're having some success, but if you want an explanation, you're going to have to ask somebody else. I didn't even pretend to listen." But it's safe to say you won't ever see a displayed equation in a Clancy novel.

Not many novels have displayed equations of any kind, of course. *Gravity's Rainbow,* Thomas Pynchon's masterpiece (to which *Cryptonomicon* is occasionally compared, mostly because of the World War II setting), has a couple, including the joke equation

$$\begin{aligned}\int \frac{1}{\text{cabin}}\, d(\text{cabin}) &= \log \text{cabin} + c \\ &= \text{houseboat}.\end{aligned}$$

The 1987 novel *First Light,* by Charles Baxter, has three, including the Cauchy inequality

$$\left(\sum_{i=1}^{n} u_i v_i\right)^2 \le \sum_{i=1}^{n} u_i^2 \sum_{i=1}^{n} v_i^2,$$

and Rebecca Goldstein's recent *Properties of Light* is arguably motivated by a wave equation,

$$dQ/dt = \left(\hbar/m\right)\mathrm{Im}\left(\nabla\psi/\psi\right).$$

Mailer's *The Naked and the Dead* doesn't have any equations, but it does have some diagrams of asymmetric parabolas in a passage on projectiles. Among his footnotes(!) in *Infinite Jest,* David Foster Wallace digresses on the mean value theorem, with diagrams and equations. But Stephenson really goes to town.

There's lots of math in *Cryptonomicon,* which is not to say that mathematicians have much to learn from Stephenson's novel—there are plenty of expositions of the math presented here, and you don't have to plow through 918 pages to get it—but it's fun to see *any* math being used in a novel, especially a bestseller.

As in Clancy, most of the math has to do with cryptography. Stephenson lavishes several pages on the inner workings of the World War II German Enigma machine. He gives a bicycle-chain example of the way in which the least common multiple (lcm) of two small numbers can be either large or small, depending on the numbers' greatest common divisor. (There's a mistake here, however: Stephenson correctly gives the lcm of 20 and 101 as 2020, but incorrectly says the lcm of 20 and 100 is 200. Most readers—and

*In another minor instance Stephenson has Shaftoe describing distance in terms of "clicks," which is a neologism of the Vietnam War. Clancy too stumbles on occasion, as when he casually dates the Apple II to 1975, a year before the Apple I appeared.

almost certainly Stephenson himself—read right past that without thinking about it. But it would be interesting to know how many readers *think* it's wrong but *aren't sure*.)

Lawrence Waterhouse mulls over the information content of seemingly random sequences; in particular, he ponders the very real problem faced by the Allies in trying to take maximum advantage of the advance knowledge they received through Bletchley Park without tipping off the Axis that they had broken their codes. And the zeta function isn't there just for decoration. It plays a pivotal role in the cryptographic story!

The appendix, which was written by Bruce Schneier (the author of a textbook on cryptography and a recent IMA "public lecturer"—see article below), gives a detailed description of a clever Enigma-style cipher system invented by Schneier that can be done with a deck of cards, including two jokers. Very roughly speaking (and the cryptographic devil, of course, is in the details), Schneier's system has you look at the top card in a shuffled deck, do a simple alphabetic shift on the first letter in your message based on that card's value, and then rearrange the deck by an algorithm keyed to the positions of the two jokers. The pseudorandom sequence produced by this algorithm presumably cycles through a substantial fraction of the 54! permutations of the cards. (It's actually not clear whether that's the case. Schneier gives a URL for his company, promising details on the security analysis for Solitaire, but so far there's nothing there.)

True to Type

Mathematics, including graphs and equations, enters in a somewhat silly, but nonetheless entertaining, way in a couple of other places. At one point, Waterhouse grandpère graphs his "horniness index" σ as a function of time and worries about its relationship with his clarity of mind C_m. Unfortunately, there are some awkward errors here. The equation as it appears in the novel, is $C_m \alpha \lim_{n\to\infty} 1/(\sigma - \sigma_c)^n$, "which amounts to saying that the moment σ rises above the threshold σ_c it becomes totally impossible for Waterhouse to break Nipponese cryptographic systems." The first of the problems is that alpha: It's used elsewhere, in the displayed equation $\sigma \alpha (t - t_0)$, and in both cases is clearly supposed to be the "proportional to" symbol, $\propto$. (But it's only clear, I dare say, to mathematicians; I wonder how many readers of *Cryptonomicon* failed to make sense of these equations.) But the bigger problem is in the limit, which is actually *undefined* when σ is less than σ_c, goes abruptly to *infinity* just above the threshold (even though C_m is "calibrated" so that "$0 < = C_m < 1$," another typesetting infelicity), drops to 1 when $\sigma = \sigma_c + 1$ (although this requires specifying actual *units* of horniness!), and to 0 when σ goes higher than that. One is left to guess what Stephenson really meant here.

With respect to typesetting errors, the page-10 zeta function, while mathematically OK, is rather inelegantly typeset (the superscript *s*'s are irritatingly tiny). But such sloppiness isn't unique to *Cryptonomicon.* Virtually all the examples given above contain typesetting infelicities. Someone should tell these guys about TEX.

Elsewhere, in a section in which the Waterhouse family is divvying up some family heirlooms, Randy's Uncle Red, who chairs the math department at the fictitious Okaley College, lectures on the problem of partitioning an inhomogeneous set of *n* objects "into *m* subsets (S_1,S_2, . . . ,S_m) such that the value of each subset is as close as possible to being equal." The displayed equations there really don't add much, especially since they are ostensibly spoken. While the scene is entertaining, Stephenson muffs a chance to do a real number on the problem of fair division.

Overall, *Cryptonomicon* is more an Internet novel than a novel about mathematics. Stephenson's point is that *information* has become the world's most valuable commodity. Clancy too stresses the value of information, mostly in the form of military intelligence. (Curiously, though, the story in both novels is driven in large part by the age-old greed for *gold.*) Their books are interesting to read for the appearance of math in each, and enjoyable in their own right as technothrillers. But if you're hankering for good literature about mathematicians doing mathematics, you won't be satisfied. The Great American Math Novel has yet to be written.

Barry A. Cipra is a mathematician and writer based in Northfield, Minnesota.

Copy Protection a Lost Cause, Says Internet Security Expert

Would you believe an advertisement for a doorlock that guaranteed to keep your house from being burgled?

Of course not, says Bruce Schneier, president of Counterpane Internet Security, Inc., in San Jose, California. Windows (of the glass variety) being what they are, locks on doors do little more than discourage the casual intruder. Even safes come not with guarantees but with ratings for the amount of time it takes to break into them.

By the same token, Schneier says, we shouldn't buy into the high-tech hype of schemes that "guarantee" ownership protection for digital files. Speaking at the University of Minnesota on February 12, in a public lecture sponsored by the Institute for Mathematics and Its Applications, Schneier outlined some of the inherent problems of attempts to restrict the way people use software—all of which, he maintains, inevitably run afoul of what he calls the "natural laws of the digital world."

The generic term for restrictions on the distribution of software is "copy protection." Protective measures range from simple warnings that a disk is not to be copied to elaborate digital watermarking systems that weave authenticating messages into the

software itself. “Nowadays this is called ‘digital rights management,’” Schneier says. That’s “one of those icky terms to make you like it better.”

Copy protection has become big business. “It’s a big deal to a lot of people,” Schneier says. “Disney is really scared that copies of Little Mermaid will appear on everybody’s desktop. Disney’s terrified of that. For a lot of people there’s a lot of money behind making this work. Unfortunately the money is behind making it work in ways it can’t work.”

Simple schemes may baffle the ordinary user. But hackers have a history of defeating even the most intricate of roadblocks thrown up by corporate interests, from the Content Scrambling System for DVDs to the Secure Digital Music Initiative. And pirates—digital analogs of the guys who make fake Rolex watches and Gucci handbags—will attack anything that seems worth the effort, even if it’s just by re-recording a piece of music.

“There are examples of things that haven’t been broken—generally because no one’s bothered,” Schneier says. “On a general-purpose computer, nothing works against a dedicated and skilled attacker. Period.”

The problem, he says, is that “unlike atoms, bits are fundamentally copyable, easily and perfectly. That’s just the way bits work. You can’t change that with engineering. You can’t suddenly make bits scarce. Bits are infinite.” Moreover, anything done on a computer is open to unlimited duplication. Even an encrypted music file, for example, must at some point be decrypted so that appropriate instructions can be sent to the speakers; those bits can be intercepted, copied, and recopied.

Once a copy-protection scheme has been broken, two other facts of digital life come into play, Schneier says: “automation” and “action at a distance.” Automation simply means that, even though the attack may have required cleverness and computer know-how, the resulting hack can be packaged for anyone to use. For example, you don’t have to understand the Content Scrambling System to download DeCSS. And action at a distance means that geography is no longer a barrier. Knowledge on the Internet can spread in ways that make wildfires look tame.

Consequently, Schneier argues, high-tech fixes based on sophisticated mathematical cryptography are doomed to fail. “Certainly cryptography is one of the two cool things you can do with mathematics in your lifetime,” he says. “The question is, from a business point of view, does it actually solve a business problem? And in this case, I maintain it doesn’t.”

There is one high-tech solution, according to Schneier: Stop making general-purpose computers. “Most attacks work because we’re on a computer—because I can write software to defeat your software,” he explains. “As you move toward special-purpose hardware, this gets much harder.” A dedicated DVD player or video game console, for example, is hard to attack because there’s no point of entry. (This won’t stop pirates, of course. But neither does a bank vault stop professional thieves.) If most people owned what Schneier calls a “controlled Internet entertainment platform” capable of running only authorized software, restrictions would be fairly simple to implement. Your machine, for example, would check to see that you’d paid for that Metallica song before playing it, or it might automatically e-mail a note to ASCAP (or Big Brother) so you could be billed for it.

It’s not difficult to believe that the general public would acquiesce to the disappearance of general-purpose computers, especially if their controlled replacements were cheap and easy to use. Schneier would prefer to see other, more imaginative solutions, based on a mix of advertising, packaging, sponsorship, and patronage. Many things can be profitably given away if they create demand for other items. This is how broadcast radio and TV work, and it’s why bartenders set out free bowls of salted nuts. An artist might promise to release a new work once enough people had pledged enough money. This is basically how public radio and TV work, and it’s essentially what Stephen King did with his online novel, “The Plant.” (King’s self-publishing venture was reportedly a failure, Schneier points out, but it actually made the writer a ton of money.) And people will always pay for timeliness, which is what keeps first-run movie theaters in business, not to mention companies that sell financial advice (“you should have sold that stock last week” is not valuable information).

In the long run, Schneier says, the winners will be the companies that develop new methods of e-commerce. “The trick is not to fight the natural laws of digital content.”