Book Review

Cryptonomicon

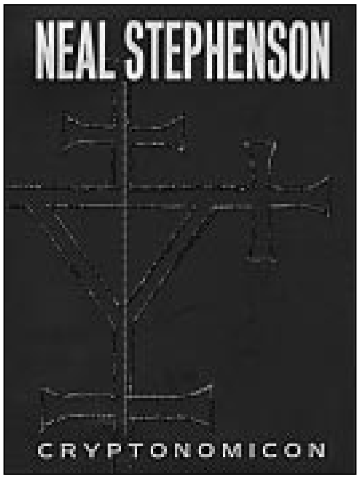
Reviewed by Alex Kasman

Cryptonomicon
Neal Stephenson
Avon Books, 1999
ISBN 0-380-97346-4
918 pages, $27.50

Neal Stephenson's latest novel, *Cryptonomicon*, is a story of adventure, conspiracy, and war, laced with a good deal of computer science and mathematics. Although mathematics is not the main subject of the book, any amount of mathematics in a novel is rare, and *Cryptonomicon* contains so much that even traditional reviews of this *New York Times* bestseller emphasize its mathematical aspects. These aspects will be the focus of my review.

There is nothing quite like Stephenson's two previous novels, *Snow Crash* and *The Diamond Age*. However, as novels that take place in the future and focus largely on technologies beyond our present means, both books fit nicely into the established and popular genre of "science fiction". *Cryptonomicon* is different. It follows two storylines: a computer-oriented one that takes place in the present and a more mathematical one that takes place during World War II. Because of the mathematical content, *Cryptonomicon* is an example of what I like to think of as "mathematical fiction".

The modern storyline concerns computer programmer Randy Waterhouse, whose company is involved in a massive project to build a "data haven" (a secure computer site free of government influence). This project and the problems the company faces in trying to create it provide a plausible scenario for considering some serious issues in modern cryptography. For instance, the book touches both on possible government abuse in the absence of a secure code available to users of the Internet and on the potential use of the data haven for organized crime.



Of course, cryptography is necessary for a project such as the data haven, and, as the title would imply, discussions of codes and ciphers run throughout the book. Mathematicians with a background in cryptanalysis might be especially interested in a new output-feedback mode stream cipher formally introduced in this book for the first time. The code is described in greater detail in an appendix written by its creator, Bruce Sheier, the president of a computer security company. As Sheier explains, the code is based on the permutation group S_{54} and can be implemented using a standard deck of 52 playing cards with two distinguishable jokers. The code takes advantage of the fact that the number of standard cards is twice the number of letters in the English alphabet (a

Alex Kasman is professor of mathematics at the College of Charleston. His e-mail address is kasman@math.cofc.edu.

coincidence that is too good to ignore). Moreover, this code benefits in a nonquantifiable way from the ubiquity of decks of cards in our society. For example, it is used in the book by two characters occupying adjacent jail cells who are able to communicate securely without arousing the suspicion of the guards by passing a deck of cards back and forth. (Note that the Perl script for implementing the code that appears in the text apparently has an error in it and that a corrected version can be downloaded from the Web site mentioned in the appendix.)

Randy's attention is temporarily drawn away from the data haven when the crew laying the underwater cables for his company finds a sunken Nazi submarine which is mysteriously connected to his grandfather. This discovery provides a link to the historical portion of the novel, which follows Randy's grandfather, mathematician Lawrence Waterhouse. It was the elder Waterhouse's job to break codes used by the Axis powers and to hide from them the fact that this had been done. This mission is achieved through mathematical methods as well as such "brute force" techniques as setting up fake spy stations behind enemy lines to "discover" things mentioned in coded messages and leaving a dead body at sea with false papers for the Germans to find. Of course, the last of these tricks is well known to have actually been used by the Allies during the war. Although Stephenson declares in the acknowledgments, "[J]ust for the record, let me state that I made all of this up—honest!", there are some grains of truth hidden within the fiction, and it is difficult to tell where the facts end and the fiction begins.

There are many historical figures who appear as characters in the book, such as Hermann Göring and Isoroku Yamamoto. I was able to recognize at least two real mathematicians. Alan Turing is a major character in this book. Of course, Turing's life has previously been "fictionalized" in the biographical play *Breaking the Code.*[1] Whereas that play was a character study exploring Turing's humanity, in *Cryptonomicon* he is more like a deity, having mythological significance because of the impact his work has had on modern computer science. There is also a brief appearance by Abraham Sinkov, who is the author of a well-known text on mathematical aspects of cryptography.[2]

Recognizing actual historical events or characters in the book was harder than distinguishing real mathematics from "fictional mathematics". Stephenson is **not** a mathematician, as becomes clear during a section in which he attempts to describe a functional relationship between Waterhouse's sex drive and his ability to concentrate on breaking enemy codes. Certainly the mathematical notation is being used in this context only as a joke, but I could not help being disturbed by the fact that the notation was being used incorrectly. (Specifically, he writes

$$\lim_{n\to\infty} \frac{1}{(\sigma - \sigma_c)^n} \ ,$$

which according to the description in the text should be a decreasing function of σ which is zero when $\sigma > \sigma_c$.) A more entertaining bit of "fictional mathematics" is the bizarre fair division algorithm his family uses for dividing his grandmother's possessions among her children. Implementation of this algorithm involves physically placing the possessions in appropriate positions in an empty parking lot representing the two-dimensional space of monetary and emotional values.

Along with the real historical events spread throughout the novel, there is also real mathematics, including at least a small sample each of Gödel's theorem, Turing's work on computability, Russell's *Principia Mathematica*, the Riemann zeta function, modular arithmetic, probability distributions, information theory, and, of course, cryptanalysis. It is in its presentation of real mathematics that this book differs most from other recent works of "mathematical fiction", such as the films *Pi* and *Good Will Hunting*. In the former, a mathematician discovers a theoretical relationship between chaos and the decimal expansion of the number π, which leads to an integer of tremendous interest to a Kabbalistic religious sect, an ability to predict the stock market, and extremely serious mental health problems. In the latter, a custodian at a university attracts the attention of a Fields Medalist by elegantly solving difficult problems written on a blackboard, and the ensuing events lead to soul searching and an answer to the question of whether he really wants to become a mathematician. Another piece of recent mathematical fiction, though not as well known, is the novel *Distress* by Greg Egan, in which a "Theory of Everything" is discovered by participants at a mathematical physics conference and literally changes the world. In each of these, a mathematical result is important, but no mathematics is presented to the audience. It is presumed that they are interested in the story but not in the math.

Cryptonomicon is unique among these recent works of mathematical fiction in that it makes a serious attempt to explain some mathematics to the reader. On the other hand, unlike *Flatland*,[3] the classic example of mathematical fiction, the mathematics in *Crytponomicon* is secondary to the story

[1] Breaking the Code, *by Hugh Whitemore, opened in the West End in November 1986 and ran on Broadway until April 1988.*

[2] *A. Sinkov,* Elementary Cryptanalysis: A Mathematical Approach, *New Mathematical Library, no. 22, Math. Assoc. of America, Washington, DC.*

[3] *Edwin A. Abbott,* Flatland, *1880.*

being told. Many of the mathematical ideas that *Cryptonomicon* communicates are spread casually throughout the text, and most are related to the idea of discerning useful information from apparently (but not actually) random data. However, there are also some more detailed passages during which the author can really say something mathematical.

The first of these occurs when Lawrence Waterhouse first arrives at Princeton as a very bright but inexperienced mathematician who has a new result on a problem combining mathematics with mechanics. He runs into Turing (and fictional mathematician Rudy von Hacklheber) at Fine Hall, and, when they realize that they are interested in similar problems, they start a collaboration. It rapidly becomes clear to Turing, however, that Waterhouse needs a quick review of the mathematical history leading up to Turing's famous work on computing machines. This short lesson in the history of mathematics is made more interesting by the disagreements between Turing and Hacklheber (who believes that Turing is not giving sufficient credit to Leibniz for his work in symbolic logic) and by Waterhouse's naïveté. For instance:

> [Turing]: But—you know Einstein?
>
> [Lawrence]: I'm not very good with names.
>
> [Turing]: The white-haired chap with the big mustache?
>
> [Lawrence]: Oh yeah, I tried to ask him my sprocket question. He *claimed* he was late for an appointment or something.

There is an especially long mathematical digression whose purpose is to teach readers about modular arithmetic so that they can understand the Enigma code used by the Germans during the war. The idea is introduced during a bike ride Waterhouse and Turing take together in the English countryside.

> The chain of Turing's bicycle has one weak link. The rear wheel has one bent spoke. When the link and the spoke come into contact with each other, the chain will part and fall onto the road. This does not happen at every revolution of the wheel—otherwise the bicycle would be completely useless. It only happens when the chain and the wheel are in a certain position with respect to each other.

Stephenson goes on to introduce variables including l for the number of links in the chain and n for the number of spokes and the notation $in \mod l$ ("where $i = (1, 2, 3, \dots, \infty)$" [sic]) for the position of the chain after i revolutions of the wheel. Through an example he is able to convey the important qualitative difference that occurs in the case where l and n are relatively prime.

Someone with little mathematical confidence, experience, or interest may simply skip the five pages that introduce these ideas and that eventually describe the three- and four-wheeled Enigma machines (or perhaps even skip the rest of the book). To someone already familiar with these mathematical ideas, this section is easy reading and interesting mainly because this is a clever way to present the concept of modular arithmetic. Still, for many readers I am sure that the easily understood example of the bicycle chain and the life-or-death significance of the Enigma code will combine to make this an accessible and exciting introduction to a new mathematical topic.

I really enjoyed reading *Cryptonomicon*, but it may not appeal to everyone. Although the plots are clever and the presentation is compelling, the characters remain essentially one-dimensional throughout the entire book. The female characters in particular seem more like plot contrivances than like actual people. The writing style struck me as a combination of the styles of Kurt Vonnegut, Robert Anton Wilson, and Thomas Pynchon—authors whose books appeal only to a limited but devoted following of readers. Moreover, *Cryptonomicon* has enough sex, violence, and drugs to be a major Hollywood movie (and so also enough to disturb some readers).

Even if they do not read it, all mathematicians might want to know something about this book and the other examples of the rare genre of "mathematical fiction".[4] Common science fiction devices such as transporters that instantly "beam" people from a planet to their orbiting ship, faster-than-light travel through "hyperspace", and chemical solutions that bestow eternal youth may have as much to do with the average person's view of the value of scientific research as the latest issue of *Nature*. A fictional story about a biological experiment leading to a violent mutant roaming through city sewers can have real consequences when it comes to legislation concerning genetically altered food. For the same reason, the interest that we as mathematicians have in portrayals of mathematics and mathematicians should go beyond simply our own enjoyment of the stories.

Consider again the films *Pi* and *Good Will Hunting*. The argument could be made that the lesson each protagonist learns by the end of the movie is

[4] *I am attempting to compile an extensive list of works of mathematical fiction at my Web page,* `http://math.cofc.edu/faculty/kasman/MATHFICT`. *I would be grateful for any additions others might be able to suggest.*

that if one thinks about mathematics, one will miss out on the really important things in life. As a result, neither film is a particularly good advertisement for mathematics.

The photo of the author on the jacket flap of *Cryptonomicon* shows him as a young boy reading *The First Book of Codes and Ciphers.*[5] Apparently Stephenson has a long-standing interest in this subject. The mathematicians in the story echo the author's own interest in the mathematical aspects of cryptography, and it is clear that Stephenson expects his readers to learn something about them from this novel and to share his interest as well. Moreover, readers see a definite "real world" application of the abstract mathematics in helping the Allies to win the Second World War. In other words, in *Cryptonomicon* mathematics looks the way mathematicians wish everyone could see it: as interesting (even to nonmathematicians like Stephenson himself) and useful.

Some mathematicians can recall a particular book, article, or incident that sparked their initial interest in mathematics. Perhaps the best thing I can say about *Cryptonomicon* is this: I would not be at all surprised if many years in the future I hear people refer to Stephenson's novel when explaining how they chose a career as a mathematician.

Acknowledgments: Thanks to Allyn Jackson, Laura Kasman, Steve Newman, Hugo Rossi, Sam Schillace, and the anonymous reviewer for their extremely helpful comments and corrections.

[5] *Sam and Beryl Epstein,* First Book of Codes and Ciphers, *Watts Publishing, 1956.*