Cryptonomicon cypher-FAQ

("Frequently Anticipated Questions")

by Neal Stephenson

Purpose of this document

It is likely that cypherpunks and other persons interested in crypto will feel some curiosity about my novel CRYPTONOMICON. If so, they will probably find the available information, which is aimed mostly at non-specialists, to be annoyingly long on sales pitch and frustratingly short on technical detail. The purpose of this document is to make available the sort of information that is lacking in sites and PR documents aimed at the general public.

Note

One of the peculiarities of being a novelist is that there is an irremediable numerical imbalance between outgoing and incoming bandwidth. In other words, a novelist writes a single document and sends it out into the world, which is a fairly low-bandwidth procedure. But if the novel is read by many people who try to send communications back the other way, the novelist is quickly overwhelmed and becomes unable to function. There is nothing that can be done about this imbalance, and so I apologize in advance if I do not respond to incoming e-mails. I will not take offense if e-mail is sent to me, but in return I ask that you not take offense if I fail to answer.

1. Overview of the Project

For several years I have been working on a series of novels on the general subject of cryptology. Since cryptology is mathematics, which most people do not consider interesting reading, I have broadened my scope a little bit to include related fields such as Money (e.g. digital currency), War (e.g. the Enigma), and Power (e.g. crypto export controls) which can provide the basis for a more engaging yarn.

The series, when it is finished, will cover a long span of history, however the first novel to be actually published (CRYPTONOMICON, May 1999) is set in the 20th Century. It has two timelines, one set during World War 2 and the other in the present day. Other volumes, set farther in the past or in the future, will follow as soon as I can get them written.

The series will incorporate many characters and stories, tied together by a few common threads. For example, certain family names keep popping up. Crypto, money, and computers seem to find their way into all of the storylines.

The ongoing presence of crypto as an important force in the characters' lives is symbolized by a fictitious book called the *Cryptonomicon* which, according to the story, is originally published in the 1600s as a compendium of cryptographic lore. As new generations of cryptologists come and go, they add new information to this original document until it develops into a kind of Talmudic compilation of whatever has been written about crypto in the last few centuries.

2. Contributions by Others

One of the noteworthy features of the novel CRYPTONOMICON is that it contains a new cryptosystem invented by Bruce Schneier, called Solitaire (though in the actual text of the novel it goes by a different name for a while). Bruce has written a technical appendix, printed in the back of the book, giving a full description of Solitaire. Not only that, but Ian Goldberg has written a perl script that encrypts and decrypts messages using the solitaire algorithm. The full text of Ian's perl script appears in the body of the novel. Since Solitaire is strong enough to be export-controlled, this means that when the text of the novel is rendered in electronic form it becomes an export-controlled munition.

As Bruce explains in the appendix, Solitaire is specifically designed to offer security against high-tech cryptanalysis, but it is implemented on a low-tech system: an ordinary deck of playing cards. In other words, it is intended for use by people who are living under political regimes where the possession of crypto tools (computers, crypto software, etc.) is itself grounds for confiscation, punishment, etc.

What is a new cryptosystem like Solitaire doing in a novel? It is a mutually beneficial relationship. I needed such a system to play a certain role in the book. But by including Bruce's full description of the algorithm, and Ian's perl script, in the actual text of the novel, we can hopefully leverage the wide publicity and distribution of the book to get this cryptosystem out to places it might not otherwise reach.

3. What is up with the title?

It has been pointed out that the word "Cryptonomicon" bears obvious similarities to "Cyphernomicon," which is the title of a cypherpunk FAQ document by Tim May. This leads to the question of am I committing some form of plagiarism, or rendering homage, or what? The answer, strangely enough, is neither. I was completely unaware of the existence of Tim May's Cyphernomicon at the time I came up with "Cryptonomicon." According to the fictional storyline that I have been writing, the original *Cryptonomicon* was written by an English scholar with a Classical education (for those of you who are crypto history buffs, it is modeled after John Wilkins's 1641 book entitled *Mercury*). Accordingly, I wanted to give it a Latin-sounding title, and "Cryptonomicon" is what I came up with. It is the sort of title that would blend in pretty well with any 17th-Century English book list. According to all of the library and Web searches I have done since then, the term "Cryptonomicon" has never appeared anywhere else.

Since becoming aware of the existence of Tim May's "Cyphernomicon" I have been in touch with him about this near-collision in namespace. Of course I am not authorized to speak on his behalf, but having had an exchange of messages with him, I am now going forward with the understanding that he has no problems or complaints.

4. Does it mention Cypherpunks?

To write a novel about the modern-day crypto world without showing any awareness of the Cypherpunk phenomenon would suggest carelessness or even dishonesty on the part of the author. However, if I were a Cypherpunk, I would view this kind of attention as a double-edged sword. Making members of some group into characters in a novel could be interpreted as a way of honoring

the group mentioned. On the other hand, anyone who is unhappy with some aspect of how the book is written is likely to construe it as slander. In my view it is best to avoid giving offense or misleading readers.

In this novel there is a fictitious group called the Secret Admirers. Knowledgeable persons will probably perceive similarities between the cypherpunks and the Secret Admirers, however intelligent readers should keep in mind that this is a work of fiction and that the two groups cannot be simply equated. To put it another way, for "Secret Admirers" don't mentally substitute "Cypherpunks." Instead, mentally substitute "the existence of cryptologically sophisticated persons not affiliated with governments or other traditional power structures, loosely inspired by the existence of such persons in the real world, but liberally embroidered on and fictionalized by a novelist whose job it is to make stuff up."

The Secret Admirers are not a huge part of the novel. They are part of the general backdrop against which the modern-day storyline plays out. The main characters in the modern-day storyline are high-tech entrepeneurs organizing a startup company to build a data haven and issue a digital currency.

5. Are some of the characters based on real people?

This is not a *roman a clef.* A *roman a clef* is a novel that is simply a literal depiction of events with the names changed, and that can be decrypted by figuring out direct correspondences between characters in the novel and actual persons. I would never write a book like that. In the World War 2 storyline I have included some actual historical figures under their own names, such as Alan Turing and Douglas MacArthur, but all of the other characters are simply made up.

The usual way of explaining what novelists do is to say that their characters are composites. But this implies that every single characteristic of a fictional character can be attributed to some actual person somewhere. This is very far from being the case. The "composite" explanation does not do justice to the amount of content that novelists simply invent. Or to put it another way, it gives us too much credit for being hard workers. Making up composite characters would be tremendously labor-intensive. Fabricating stuff from whole cloth is much easier.

Since I began writing novels I have had many startling conversations with total strangers who were convinced that I had somehow based fictional characters on them personally. For example, when doing a signing in Oakland I was approached by a somewhat bewildered young man who was half African-American and half Japanese and who had been working as a pizza delivery driver when he had encountered my book SNOW CRASH, which features a similar character. When he saw that the book had been written several years previously, he understood that it was just a coincidence, but still found it to be a little eerie.

This kind of thing happens more frequently than one might expect. The characters in CRYPTONOMICON come from a fictional world very similar to the real one and so many parallels can be observed, but none of them is based on an actual person.

6. Does it express views that Cypherpunks will find agreeable?

My expectation is that most Cypherpunks will find this novel unobjectionable. Cypherpunks are sometimes caricatured as "survivalists" or other types of fringe elements. By placing modern-day

concerns in a larger context going back at least to World War 2, this book might help to explain some of the concerns that motivate many Cypherpunks.

It is important to remember that novels are works of art, and like other works of art, get much of their power from indirectness and ambiguity. Consequently, any readers looking for explicit statements about anything are apt to find this work frustrating.

7. Is Neal Stephenson a cypherpunk?

No. I read the list sometimes. But the Cypherpunks are a blend of mathematics and politics. I don't have enough knowledge to talk about the math, and as an artist I consider myself obligated to avoid politics.

8. It says on the dust flap that you were born in Ft. Meade, Maryland, the home of the NSA. What is up with that?

My dad was in the army there. He was/is an electrical engineer, specializing in antennas, particularly microwave antennas. He left the Army and we moved away from Ft. Meade when I was 6 months old. So this is an interesting factoid, but it was not an important part of my life.

9. Is the novel technically accurate?

Any novel that addresses technical subjects sooner or later includes some oversimplifications that make knowledgeable readers cringe. I have tried to go about this project competently, and have aimed for a higher level of accuracy than might be found in some other documents. It contains a few long digressions about crypto that have already gotten me lambasted by reviewers. But (a) it is fiction after all, and (b) I am not perfect, and (c) even if I were there would probably be cases in which it was better to simplify certain topics to avoid alienating normal readers.

10. Should I invest time and money in reading this novel?

Of course everyone has differing tastes in literature, however I can offer a few guidelines.

- There is a fair amount of expository material about crypto that will be familiar to any Cypherpunk, hence not a reason to read the novel, and possibly a reason to avoid it.
- As it takes place during WW2 or the present day, the book is less "science-fictiony" than other things I have written, and so people who are looking for speculation about the future, hypothetical technologies, etc. may be disappointed. People who are interested in WW2 and/or contemporary techno-thriller literature might like it on the other hand.
- However, the book is lengthy and somewhat discursive. If I can risk a blanket generalization about my own work, it has a somewhat more literary style than, say, a typical techno-thriller. Comparisons have already been drawn with works by Thomas Pynchon such as Gravity's Rainbow. Some people like this kind of writing and others don't.
- The book is lengthy (> 900 pages). People who like quick reads will therefore have a problem

with it. People who like to get lost in long books may prefer it.

- There is a fair amount of violence, which I have tried to present without glorifying it (a la Saving Private Ryan). There is not a great deal of sex, but what there is might seem odd or objectionable to some readers.
- The WW2 part of the book is set in an era when the concept of racial sensitivity had not even been dreamed of yet, and so the characters see the world, and express themselves, accordingly. To me this seems more constructive than presenting a sugar-coated view of history, and the fact that the single most admirable character in the whole book is Japanese should put to rest suspicions about my motives. However, people who object to, e.g. "Huck Finn" on the grounds that it contains racial slurs may want to avoid this novel.
- Some of the characters espouse religious/spiritual views that many Cypherpunks will find ludicrous.
- The book addresses the subject of the Holocaust, generally in the sense of "look at what happens when power gets too centralized." But that is such a sensitive topic that it can hardly be mentioned without alienating at least someone.

I hope that this document has covered most of the questions that readers of the Cypherpunks list are likely to have. Thank you for reading it.

This page maintained by neal@well.com