20. README

20.1. copyright

THE CYPHERNOMICON: Cypherpunks FAQ and More, Version 0.666, 1994-09-10, Copyright Timothy C. May. All rights reserved. See the detailed disclaimer. Use short sections under "fair use" provisions, with appropriate credit, but don't put your name on my words.

20.2. README--BRIEF VERSION

20.2.1. Copyright Timothy C. May.

All rights reserved. For what it's worth.

20.2.2. Apologies in advance

for the mix of styles (outline, bullet, text, essays), for fragments and incomplete sections. This FAQ is already much too long and detailed, and writing suitable connective material, introductions, summaries, etc. is not in the cards anytime soon. Go with the flow, use your text searching tools, and deal with it.

20.2.3. Substantive corrections welcome,

quibbles less welcome, and ideological debate even less welcome. Corrections to outdated information, especially on pointers to information, will be most appreciated.

20.3. Copyright Comments

20.3.1. It may seem illogical

for a Cypherpunk to assert some kind of copyright. Perhaps. But my main concern is the ease with which people can relabel documents as their own, sometimes after only adding a few words here and there.

20.3.2. Yes, I used the words of others

in places, to make points better than I felt my own words would, to save time, and to give readers a different voice speaking on issues. I have credited quotes with a "[Joe Foobar, place, date] attribution, usually at the end of the quote. If a place is not listed, it is the Cypherpunks list itself. The author and date should be sufficient to (someday) retrieve the source text. By the way, I used quotes as they seemed appropriate, and make no claims that the quoted points are necessarily original to the author--who may have remembered them from somewhere else--or that the date listed is the origination date for the point. I have something like 80 megabytes of Cypherpunks posts, so I couldn't do an archaeological dig for the earliest mention of an idea.

20.3.3. People can quote this FAQ

under the "fair use" provisions, e.g., a paragraph or two, with credits. Anything more than a few paragraphs constitutes copyright infringement, as I understand it.

20.3.4. Should I give up the maintaining of this FAQ

and/or should others get involved, then the normal co-authorship and inheritance arrangements will be possible.

20.3.5. The Web. WWW and Mosaic offer amazing new opportunities for on-line documents.

It is in fact likely that this FAQ will be available as a Web document. My concern, however, is that the integrity and authorship be maintained. Thus, splitting the document in a hundred or more little pieces, with no authorship attached, would not be cool. Also, I intend to maintain this document with my powerful outlining tools (Symantec's "MORE," on a Macintosh) and thus anyone who "freezes" the document and uses it as a base for links, pointers, etc., will be left behind as mods are made.

20.4. A Few Words on the Style

20.4.1. Some sections are in outline form

- like this
- with fragments of ideas and points
- with incomplete sentences
- and with lists of points that are obviously only starting points for more complete analyses

20.4.2. Other sections are written in more complete essay form,

as reasonably self-contained analyses of some point or topic. Like this. Some of these essays were taken directly out of posts I did for the list, or for sci.crypt, and no attribution H (since I wrote the stuff...quotes from others are credited).

20.4.3. The styles may clash,

but I just don't have the hundreds of hours to go through and "regularize" everything to a consistent style. The outline style allows additional points, wrinkles, rebuttals, and elaborations to be grafted on easily (if not always elegantly). I hope most readers can understand this and learn to deal with it.

20.4.4. Of course, there are places where

the points made are just too fragmentary, too outlinish, for people to make sense of. I've tried to clean these up as much as I can, but there will always be some places where an idea seemed clear to me at the time (maybe not) but which is not presented clearly to others. I'll keep trying to iron these kinks out in future versions.

20.4.5. Comment on style

- In many cases I merged two or more chunks of ideas into one section, resulting in many cases in mismatching writing styles, tenses, etc. I apologize, but I just don't have the many dozens of hours it might take to go through and "regularize" things, to write more graceful transition paragraphs, etc. I felt it was more important to get the ideas and idea fragments out than to polish the writing. (Essays written from scratch, and in order, are generally more graceful than are concatenations of ideas, facts, pointers, and the like.)

- Readers should also not assume that a "fleshed-out" section, made up of relatively complete paragraphs, is any more important than a section that is still mostly made up of short one-liners.
- References to Crypto Journals, Books. Nearly every section in this document *could have* one or more references to articles and papers in the Crypto Proceedings, in Schneier's book, or whatever. Sorry, but I can't do this. Maybe someday--when true hypertext arrives and is readily usable (don't send me e-mail about HTML, or Xanadu, etc.) this kind of cross-referencing will be done. Footnotes would work today, but are distracting in on-line documents. And too much work, given that this is not meant to be a scholarly thesis.
- I also have resisted the impulse to included quotes or sections from other FAQs, notably the sci.crypt and rsadsi FAQs. No point in copying their stuff, even with appropriate credit. Readers should already have these docs, of course.

20.4.6. quibbling

- Any time you say something to 500-700 people, expect to have a bunch of quibbles. People will take issue with phrasings, with choices of definitions, with facts, etc. Correctness is important, but sometimes the quibbling sets off a chain reaction of corrections, countercorrections, rebuttals, and "I would have put it differently"s. It's all a bit overwhelming at times. My hope for this FAQ is that serious errors are (of course) corrected, but that the List not get bogged down in endless quibbling about such minor issues as style and phrasing.

20.5. How to Find Information

20.5.1. This FAQ is very long,

which makes finding specific questions problematic. Such is life--shorter FAQ are of course easier to navigate, but may not address important issues.

20.5.2. A full version of this FAQ is available,

as well as chapter- by-chapter versions (to reduce the downloading efforts for some people). Search tools within text editors are one way to find topics. Future versions of this FAQ may be paginated and then indexed (but maybe not).

20.5.3. I advise using search tools

in editors and word processors to find sections of interest. This is likely faster anyway than consulting an index generated by me (which I haven't generated, and probably never will).

20.6. My Views

20.6.1. This FAQ,

or whatever one calls it, is more than just a simple listing of frequently asked questions and the lowest- common-denominator answers. This should be clear just by the size alone. I make no apologies for writing the document I wanted to write. Others are free to write the FAQ they would prefer to read. You're getting what you paid for.

20.6.2. My views are rather strong in some areas.

I've tried to present some dissenting arguments in cases where I think Cypherpunks are really somewhat divided, such as in remailer strategies and the like. In cases where I think there's no credible dissent, such as in the wisdom of Clipper, I've made no attempt to be fair. My libertarian, even anarchist, views surely come through. Either deal with it, or don't read the document. I have to be honest about this.

20.7. More detailed disclaimer

20.7.1. This detailed disclaimer is probably not good

in most courts in the U.S., contracts having been thrown out if favor of nominalism, but here it is anyway. At least nobody can claim they were misled into thinking I was giving them warranteed, guaranteed advice.

20.7.2. Timothy C. May hereby disclaims

all warranties relating to this document, whether express or implied, including without limitation any implied warranties of merchantability or fitness for a particular purpose. Tim May will not be liable for any special, incidental, consequential, indirect or similar damages due to loss of business, indictment for any crime, imprisonment, torture, or any other reason, even if Tim May or an agent of his has been advised of the possibility of such damages. In no event shall Tim May be liable for any damages, regardless of the form of the claim. The person reading or using the document bears all risk as to the quality and suitability of the document. Legality of reading or possessing this document in a jurisdiction is not the responsibility of Tim May.

20.7.3. The points expressed may or may not represent the views of

Tim May, and certainly may not represent the views of other Cypherpunks. Certain ideas are explored which, if implemented, would be illegal to various extents in most countries in the world. Think of these explorations of ideas as just that.

20.8. I've decided to release this

before the RSA patents run out...

Revision #1
Created 23 June 2022 04:08:26 by c0mmando
Updated 23 June 2022 04:08:46 by c0mmando