WIKIPEDIA

Cypherpunk

A **cypherpunk** is any individual advocating widespread use of strong cryptography and privacy-enhancing technologies as a route to social and political change. Originally communicating through the Cypherpunks electronic mailing list, informal groups aimed to achieve privacy and security through proactive use of cryptography. Cypherpunks have been engaged in an active movement since the late 1980s.

Contents

History

Before the mailing list

Until about the 1970s, cryptography was mainly practiced in secret by military or spy agencies. However, that changed when two publications brought it out of the closet into public awareness: the US government publication of the Data Encryption Standard (DES), a block cipher which became very widely used; and the first publicly available work on public-key cryptography, by Whitfield Diffie and Martin Hellman.[1]

The technical roots of Cypherpunk ideas have been traced back to work by cryptographer David Chaum on topics such as anonymous digital cash and pseudonymous reputation systems, described in his paper "Security without Identification: Transaction Systems to Make Big Brother Obsolete" (1985).[2]

In the late 1980s, these ideas coalesced into something like a movement.[2]

Origin of the term, and the Cypherpunks mailing list

In late 1992, Eric Hughes, Timothy C. May and John Gilmore founded a small group that met monthly at Gilmore's company Cygnus Solutions in the San Francisco Bay Area, and was humorously termed *cypherpunks* by Jude Milhon at one of the first meetings - derived from *cipher* and *cyberpunk*.[3] In November 2006, the word was added to the Oxford English Dictionary.[4]

The Cypherpunks mailing list was started in 1992, and by 1994 had 700 subscribers.[3] At its peak, it was a very active forum with technical discussion ranging over mathematics, cryptography, computer science, political and philosophical discussion, personal arguments and attacks, etc., with some spam thrown in. An email from John Gilmore reports an average of 30 messages a day from December 1, 1996 to March 1, 1999, and suggests that the number was probably higher earlier.[5] The number of subscribers is estimated to have reached 2000 in the year 1997.[3]

In early 1997, Jim Choate and Igor Chudov set up the Cypherpunks Distributed Remailer,[6] a network of independent mailing list nodes intended to eliminate the single point of failure inherent in a centralized list architecture. At its peak, the Cypherpunks Distributed Remailer included at least seven nodes.[7] By mid-2005, al-qaeda.net ran the only remaining node.[8] In mid 2013, following a brief outage, the al-qaeda.net node's list software was changed from Majordomo to GNU Mailman[9] and subsequently the node was renamed to cpunks.org.[10] The CDR architecture is now defunct, though the list administrator stated in 2013 that he was exploring a way to integrate this functionality with the new mailing list software.[9]

For a time, the cypherpunks mailing list was a popular tool with mailbombers,[11] who would subscribe a victim to the mailing list in order to cause a deluge of messages to be sent to him or her. (This was usually done as a prank, in contrast to the style of terrorist referred to as a mailbomber.) This precipitated the mailing list sysop(s) to institute a reply-to-subscribe system. Approximately two hundred messages a day was typical for the mailing list, divided between personal arguments and attacks, political discussion, technical discussion, and early spam.[12][13]

The cypherpunks mailing list had extensive discussions of the public policy issues related to cryptography and on the politics and philosophy of concepts such as anonymity, pseudonyms, reputation, and privacy. These discussions continue both on the remaining node and elsewhere as the list has become increasingly moribund.

Events such as the GURPS Cyberpunk raid lent weight to the idea that private individuals needed to take steps to protect their privacy. In its heyday, the list discussed public policy issues related to cryptography, as well as more practical nuts-and-bolts mathematical, computational, technological, and cryptographic matters. The list had a range of viewpoints and there was probably no completely unanimous agreement on anything. The general attitude, though, definitely put personal privacy and personal liberty above all other considerations.

Early discussion of online privacy

The list was discussing questions about privacy, government monitoring, corporate control of information, and related issues in the early 1990s that did not become major topics for broader discussion until ten years or so later. Some list participants were more radical on these issues than

almost anyone else.

Those wishing to understand the context of the list might refer to the history of cryptography; in the early 1990s, the US government considered cryptography software a munition for export purposes. (PGP source code was published as a paper book to bypass these regulations and demonstrate their futility.) In 1992, a deal between NSA and SPA allowed export of cryptography based on 40-bit RC2 and RC4 which was considered relatively weak (and especially after SSL was created, there was many contests to break it). The US government had also tried to subvert cryptography through schemes such as Skipjack and key escrow. It was also not widely known that all communications were logged by government agencies (which would later be revealed during the NSA and AT&T scandals) though this was taken as an obvious axiom by list members.[14]

The original cypherpunk mailing list, and the first list spin-off, *coderpunks*, were originally hosted on John Gilmore's toad.com, but after a falling out with the sysop over moderation, the list was migrated to several cross-linked mail-servers in what was called the "distributed mailing list."[15][16] The *coderpunks* list, open by invitation only, existed for a time. *Coderpunks* took up more technical matters and had less discussion of public policy implications. There are several lists today that can trace their lineage directly to the original Cypherpunks list: the cryptography list (cryptography@metzdowd.com), the financial cryptography list (fc-announce@ifca.ai), and a small group of closed (invitation-only) lists as well.

Toad.com continued to run with the existing subscriber list, those that didn't unsubscribe, and was mirrored on the new distributed mailing list, but messages from the distributed list didn't appear on toad.com.[17] As the list faded in popularity, so too did it fade in the number of cross-linked subscription nodes.

To some extent, the cryptography list[18] acts as a successor to cypherpunks; it has many of the people and continues some of the same discussions. However, it is a moderated list, considerably less zany and somewhat more technical. A number of current systems in use trace to the mailing list, including Pretty Good Privacy, /dev/random in the Linux kernel (the actual code has been completely reimplemented several times since then) and today's anonymous remailers.

Main principles

The basic ideas can be found in *A Cypherpunk's Manifesto* (Eric Hughes, 1993): "Privacy is necessary for an open society in the electronic age. ... We cannot expect governments, corporations, or other large, faceless organizations to grant us privacy ... We must defend our own privacy if we expect to have any. ... Cypherpunks write code. We know that someone has to write software to defend privacy, and ... we're going to write it."[19]

Some are or were quite senior people at major hi-tech companies and others are well-known researchers (see list with affiliations below).

The first mass media discussion of cypherpunks was in a 1993 *Wired* article by Steven Levy titled *Crypto Rebels*:

> The people in this room hope for a world where an individual's informational footprints -- everything from an opinion on abortion to the medical record of an actual abortion -- can be traced only if the individual involved chooses to reveal them; a world where coherent messages shoot around the globe by network and microwave, but intruders and feds trying to pluck them out of the vapor find only gibberish; a world where the tools of prying are transformed into the instruments of privacy. There is only one way this vision will materialize, and that is by widespread use of cryptography. Is this technologically possible? Definitely. The obstacles are political -- some of the most powerful forces in

> government are devoted to the control of these tools. In short, there is a war going on between those who would liberate crypto and those who would suppress it. The seemingly innocuous bunch strewn around this conference room represents the vanguard of the pro-crypto forces. Though the battleground seems remote, the stakes are not: The outcome of this struggle may determine the amount of freedom our society will grant us in the 21st century. To the Cypherpunks, freedom is an issue worth some risk.[20]

The three masked men on the cover of that edition of *Wired* were prominent cypherpunks Tim May, Eric Hughes and John Gilmore.

Later, Levy wrote a book, *Crypto: How the Code Rebels Beat the Government – Saving Privacy in the Digital Age*,[21] covering the crypto wars of the 1990s in detail. "Code Rebels" in the title is almost synonymous with cypherpunks.

The term *cypherpunk* is mildly ambiguous. In most contexts it means anyone advocating cryptography as a tool for social change, social impact and expression. However, it can also be used to mean a participant in the Cypherpunks electronic mailing list described below. The two meanings obviously overlap, but they are by no means synonymous.

Documents exemplifying cypherpunk ideas include Timothy C. May's *The Crypto Anarchist Manifesto* (1992)[22] and *The Cyphernomicon* (1994),[23] *A Cypherpunk's Manifesto*.[19]

Privacy of communications

A very basic cypherpunk issue is privacy in communications and data retention. John Gilmore said he wanted "a guarantee -- with physics and mathematics, not with laws -- that we can give ourselves real privacy of personal communications."[24]

Such guarantees require strong cryptography, so cypherpunks are fundamentally opposed to government policies attempting to control the usage or export of cryptography, which remained an issue throughout the late 1990s. The *Cypherpunk Manifesto* stated "Cypherpunks deplore regulations on cryptography, for encryption is fundamentally a private act."[19]

This was a central issue for many cypherpunks. Most were passionately opposed to various government attempts to limit cryptography — export laws, promotion of limited key length ciphers, and especially escrowed encryption.

Anonymity and pseudonyms

The questions of anonymity, pseudonymity and reputation were also extensively discussed.

Arguably, the possibility of anonymous speech and publication is vital for an open society and genuine freedom of speech — this is the position of most cypherpunks.[25] That the Federalist Papers were originally published under a pseudonym is a commonly-cited example.

Censorship and monitoring

In general, cypherpunks opposed the censorship and monitoring from government and police.

In particular, the US government's Clipper chip scheme for escrowed encryption of telephone conversations (encryption supposedly secure against most attackers, but breakable by government) was seen as anathema by many on the list. This was an issue that provoked strong opposition and

brought many new recruits to the cypherpunk ranks. List participant Matt Blaze found a serious flaw[26] in the scheme, helping to hasten its demise.

Steven Schear first suggested the warrant canary in 2002 to thwart the secrecy provisions of court orders and national security letters.[27] As of 2013, warrant canaries are gaining commercial acceptance.[28]

Hiding the act of hiding

An important set of discussions concerns the use of cryptography in the presence of oppressive authorities. As a result, Cypherpunks have discussed and improved steganographic methods that hide the use of crypto itself, or that allow interrogators to believe that they have forcibly extracted hidden information from a subject. For instance, *Rubberhose* was a tool that partitioned and intermixed secret data on a drive with fake secret data, each of which accessed via a different password. Interrogators, having extracted a password, are led to believe that they have indeed unlocked the desired secrets, whereas in reality the actual data is still hidden. In other words, even its presence is hidden. Likewise, cypherpunks have also discussed under what conditions encryption may be used without being noticed by network monitoring systems installed by oppressive regimes.

Activities

As the *Manifesto* says, "Cypherpunks write code";[19] the notion that good ideas need to be implemented, not just discussed, is very much part of the culture of the mailing list. John Gilmore, whose site hosted the original cypherpunks mailing list, wrote: "We are literally in a race between our ability to build and deploy technology, and their ability to build and deploy laws and treaties. Neither side is likely to back down or wise up until it has definitively lost the race."[29]

Software projects

Anonymous remailers such as the Mixmaster Remailer were almost entirely a cypherpunk development. Among the other projects they have been involved in were PGP for email privacy, FreeS/WAN for opportunistic encryption of the whole net, Off-the-record messaging for privacy in Internet chat, and the Tor project for anonymous web surfing.

Hardware

In 1998, the Electronic Frontier Foundation, with assistance from the mailing list, built a $200,000 machine that could brute-force a Data Encryption Standard key in a few days.[30] The project demonstrated that DES was, without question, insecure and obsolete, in sharp contrast to the US government's recommendation of the algorithm.

Expert panels

Cypherpunks also participated, along with other experts, in several reports on cryptographic matters.

One such paper was "Minimal Key Lengths for Symmetric Ciphers to Provide Adequate Commercial Security".[31] It suggested 75 bits was the *minimum* key size to allow an existing cipher to be considered secure and kept in service. At the time, the Data Encryption Standard with 56-bit keys was still a US government standard, mandatory for some applications.

Other papers were critical analysis of government schemes. "The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption",[32] evaluated escrowed encryption proposals. *Comments on the Carnivore System Technical Review*.[33] looked at an FBI scheme for monitoring email.

Cypherpunks provided significant input to the 1996 National Research Council report on encryption policy, *Cryptography's Role In Securing the Information Society* (CRISIS).[34] This report, commissioned by the U.S. Congress in 1993, was developed via extensive hearings across the nation from all interested stakeholders, by a committee of talented people. It recommended a gradual relaxation of the existing U.S. government restrictions on encryption. Like many such study reports, its conclusions were largely ignored by policy-makers. Later events such as the final rulings in the cypherpunks lawsuits forced a more complete relaxation of the unconstitutional controls on encryption software.

Lawsuits

Cypherpunks have filed a number of lawsuits, mostly suits against the US government alleging that some government action is unconstitutional.

Phil Karn sued the State Department in 1994 over cryptography export controls[35] after they ruled that, while the book *Applied Cryptography*[36] could legally be exported, a floppy disk containing a verbatim copy of code printed in the book was legally a munition and required an export permit, which they refused to grant. Karn also appeared before both House and Senate committees looking at cryptography issues.

Daniel J. Bernstein, supported by the EFF, also sued over the export restrictions, arguing that preventing publication of cryptographic source code is an unconstitutional restriction on freedom of speech. He won, effectively overturning the export law. See *Bernstein v. United States* for details.

Peter Junger also sued on similar grounds, and won.

Civil disobedience

Cypherpunks encouraged civil disobedience, in particular US law on the export of cryptography. Until 1997, cryptographic code was legally a munition and fall until ITAR, and the key length restrictions in the EAR was not removed until 2000.

In 1995 Adam Back wrote a version of the RSA algorithm for public-key cryptography in three lines of Perl[37][38] and suggested people use it as an email signature file:

```
#!/bin/perl -sp0777i<X+d*lMLa^*lN%0]dsXx++lMlN/dsM0<j]dsj
$/=unpack('H*',$_);$_=`echo 16dio\U$k"SK$/SM$n\EsN0p[lN*1
lK[d2%Sa2/d0$^Ixp"|dc`;s/\W//g;$_=pack('H*',/((..)*)$/)
```

Vince Cate put up a web page that invited anyone to become an international arms trafficker; every time someone clicked on the form, an export-restricted item — originally PGP, later a copy of Back's program — would be mailed from a US server to one in Anguilla. This gained overwhelming attention. There was an option to add your name to a list of such traffickers.[39][40][41]

Cypherpunk fiction

In Neal Stephenson's novel *Cryptonomicon* many characters are on the "Secret Admirers" mailing list. This is fairly obviously based on the cypherpunks list, and several well-known cypherpunks are mentioned in the acknowledgements. Much of the plot revolves around cypherpunk ideas; the leading

characters are building a data haven which will allow anonymous financial transactions, and the book is full of cryptography. But, according to the author[42] the book's title is — in spite of its similarity — not based on the Cyphernomicon,[23] an online cypherpunk FAQ document.

Legacy

Cypherpunk achievements would later also be used on the Canadian e-wallet, the MintChip, and the creation of bitcoin. It was an inspiration for CryptoParty decades later to such an extent that the *Cypherpunk Manifesto* is quoted at the header of its Wiki,[43] and Eric Hughes delivered the keynote address at the Amsterdam CryptoParty on 27 August 2012.

Notable cypherpunks

Cypherpunks list participants included many notable computer industry figures. Most were list regulars, although not all would call themselves "cypherpunks".[44] The following is a list of noteworthy cypherpunks and their achievements:

John Gilmore is one of the founders of the Cypherpunks mailing list, the Electronic Frontier Foundation, and Cygnus Solutions. He created the alt.* hierarchy in Usenet and is a major contributor to the GNU Project.

Julian Assange, a well-known cypherpunk who advocates for the use of cryptography to ensure privacy on the Internet

- Jacob Appelbaum: Tor developer, political advocate
- Julian Assange: WikiLeaks founder, deniable cryptography inventor, journalist; co-author of *Underground*; author of *Cypherpunks: Freedom and the Future of the Internet*; member of the International Subversives. Assange has stated that he joined the list in late 1993 or early 1994.[3] An archive of his cypherpunks mailing list posts[45] is at the Mailing List Archives.
- Derek Atkins: computer scientist, computer security expert, and one of the people who factored RSA-129
- Adam Back: inventor of Hashcash and of NNTP-based Eternity networks; co-founder of Blockstream
- Jim Bell: author of *Assassination Politics'*
- Steven Bellovin: Bell Labs researcher; later Columbia professor; Chief Technologist for the US Federal Trade Commission in 2012
- Matt Blaze: Bell Labs researcher; later professor at University of Pennsylvania; found flaws in the Clipper Chip[46]
- Eric Blossom: designer of the Starium cryptographically secured mobile phone; founder of the GNU Radio project
- Jon Callas: technical lead on OpenPGP specification; co-founder and Chief Technical Officer of PGP Corporation; co-founder with Philip Zimmermann of Silent Circle
- Bram Cohen: creator of BitTorrent
- Lance Cottrell: original author of the Mixmaster Remailer software; founder of Anonymizer[46]
- Matt Curtin: founder of Interhack Corporation; first faculty advisor of the Ohio State University Open Source Club;[47] lecturer at Ohio State University
- Hugh Daniel (deceased): former Sun Microsystems employee; manager of the FreeS/WAN project (an early and important freeware IPsec implementation)
- Suelette Dreyfus: deniable cryptography co-inventor, journalist, co-author of *Underground*
- Hal Finney (deceased): cryptographer; main author of PGP 2.0 and the core crypto libraries of later versions of PGP; designer of RPOW

- Eva Galperin: malware researcher and security advocate; Electronic Frontier Foundation activist[48]
- John Gilmore*: Sun Microsystems' fifth employee; co-founder of the Cypherpunks and the Electronic Frontier Foundation; project leader for FreeS/WAN
- Mike Godwin: Electronic Frontier Foundation lawyer; electronic rights advocate
- Ian Goldberg*: professor at University of Waterloo; designer of the off-the-record messaging protocol
- Rop Gonggrijp: founder of XS4ALL; co-creator of the Cryptophone
- Sean Hastings: founding CEO of Havenco; co-author of the book *God Wants You Dead*[49]
- Johan Helsingius: creator and operator of Penet remailer
- Nadia Heninger: assistant professor at University of Pennsylvania; security researcher[50]
- Robert Hettinga: founder of the International Conference on Financial Cryptography; originator of the idea of Financial cryptography as an applied subset of cryptography[51]
- Mark Horowitz: author of the first PGP key server
- Tim Hudson: co-author of SSLeay, the precursor to OpenSSL
- Eric Hughes: founding member of Cypherpunks; author of *A Cypherpunk's Manifesto*
- Peter Junger (deceased): law professor at Case Western Reserve University
- Paul Kocher: president of Cryptography Research, Inc.; co-author of the SSL 3.0 protocol
- Ryan Lackey: co-founder of HavenCo, the world's first data haven
- Brian LaMacchia: designer of XKMS; research head at Microsoft Research
- Ben Laurie: founder of The Bunker, core OpenSSL team member, Google engineer.
- Morgan Marquis-Boire: researcher, security engineer, and privacy activist
- Matt Thomlinson (phantom): security engineer, leader of Microsoft's security efforts on Windows, Azure and Trustworthy Computing, CISO at Electronic Arts
- Timothy C. May (deceased): former Assistant Chief Scientist at Intel; author of *A Crypto Anarchist Manifesto* and the *Cyphernomicon*; a founding member of the Cypherpunks mailing list
- Jude Milhon (deceased; aka "St. Jude"): a founding member of the Cypherpunks mailing list, credited with naming the group; co-creator of *Mondo 2000* magazine
- Vincent Moscaritolo: founder of Mac Crypto Workshop;[52] Principal Cryptographic Engineer for PGP Corporation; co-founder of Silent Circle and 4th-A Technologies, LLC
- Sameer Parekh: former CEO of C2Net and co-founder of the CryptoRights Foundation human rights non-profit
- Vipul Ved Prakash: co-founder of Sense/Net; author of *Vipul's Razor*; founder of Cloudmark
- Runa Sandvik: Tor developer, political advocate
- Len Sassaman (deceased): maintainer of the Mixmaster Remailer software; researcher at Katholieke Universiteit Leuven; biopunk
- Steven Schear: creator of the warrant canary; street performer protocol; founding member of the International Financial Cryptographer's Association[53] and GNURadio; team member at Counterpane; former Director at data security company Cylink and MojoNation
- Bruce Schneier*: well-known security author; founder of Counterpane
- Nick Szabo: inventor of smart contracts; designer of bit gold, a precursor to Bitcoin
- Zooko Wilcox-O'Hearn: DigiCash and MojoNation developer; founder of Zcash; co-designer of Tahoe-LAFS
- Jillian C. York: Director of International Freedom of Expression at the Electronic Frontier Foundation (EFF)[54]
- John Young: anti-secrecy activist and co-founder of Cryptome
- Philip Zimmermann: original creator of PGP v1.0 (1991); co-founder of PGP Inc. (1996); co-founder with Jon Callas of Silent Circle
- Marc Andreessen: co-founder of Netscape which invented SSL

* indicates someone mentioned in the acknowledgements of Stephenson's *Cryptonomicon*.

References

This article incorporates material from the Citizendium article "Cypherpunk", which is licensed under the Creative Commons Attribution-ShareAlike 3.0 Unported License but not under the GFDL.

1. "A Patent Falls, and the Internet Dances" (https://archive.nytimes.com/www.nytimes.com/library/cyber/week/090697patent.html). *archive.nytimes.com*. Retrieved 2020-02-04.
2. Arvind Narayanan: What Happened to the Crypto Dream?, Part 1 (http://randomwalker.info/publications/crypto-dream-part1.pdf). IEEE Security & Privacy. Volume 11, Issue 2, March–April 2013, pages 75-76, ISSN 1540-7993
3. Robert Manne: The Cypherpunk Revolutionary - Julian Assange (https://www.themonthly.com.au/issue/2011/february/1324596189/robert-manne/cypherpunk-revolutionary). The Monthly March, 2011, No. 65
4. "ResourceBlog Article: Oxford English Dictionary Updates Some Entries & Adds New Words; Bada-Bing, Cypherpunk, and Wi-Fi Now in the OED" (https://web.archive.org/web/20110521191819/http://web.resourceshelf.com/go/resourceblog/43743). 21 May 2011. Archived from the original (http://web.resourceshelf.com/go/resourceblog/43743) on 2011-05-21. Retrieved 5 September 2020.
5. "Please title this page. (Page 2)" (http://cryptome.org/jya/cp-who.htm). *Cryptome.org*. Retrieved 5 September 2020.
6. Jim Choate: "Cypherpunks Distributed Remailer (http://cypherpunks.venona.com/date/1997/02/msg02037.html)". Cypherpunks mailing list. February 1997.
7. "Cypherpunk Mailing List Information" (https://web.archive.org/web/20160305051810/http://imchris.org/projects/cpunk.html). Archived from the original (http://imchris.org/projects/cpunk.html) on 2016-03-05.
8. "Setting up a filtering CDR node for Cypherpunks" (https://web.archive.org/web/20141205102841/https://cpunks.org/cpunk/howto.html). 5 December 2014. Archived from the original (https://cpunks.org/cpunk/howto.html) on 2014-12-05. Retrieved 5 September 2020.
9. Riad S. Wahby: "back on the airwaves (https://cpunks.org//pipermail/cypherpunks/2013-July/000001.html)". Cypherpunks mailing list. July 2013.
10. Riad S. Wahby: "domain change (https://cpunks.org//pipermail/cypherpunks/2013-July/000011.html)". Cypherpunks mailing list. July 2013.
11. "Re: POST: The Frightening Dangers of Moderation" (https://web.archive.org/web/20071030112059/http://cypherpunks.venona.com/date/1997/02/msg01681.html). 30 October 2007. Archived from the original (http://cypherpunks.venona.com/date/1997/02/msg01681.html) on 2007-10-30. Retrieved 5 September 2020.
12. "Re: Re: Add To Your Monthly Income!!" (https://web.archive.org/web/20080822071741/http://cypherpunks.venona.com/date/1997/01/msg02533.html). 22 August 2008. Archived from the original (http://cypherpunks.venona.com/date/1997/01/msg02533.html) on 2008-08-22. Retrieved 5 September 2020.
13. "Cypherpunks Date Index for 1997 04" (https://web.archive.org/web/20061021180914/http://cypherpunks.venona.com/date/1997/04/). 21 October 2006. Archived from the original (http://cypherpunks.venona.com/date/1997/04/) on 2006-10-21. Retrieved 5 September 2020.
14. "The Clipper Chip: How Once Upon a Time the Government Wanted to Put a Backdoor in Your Phone" (https://www.exabeam.com/information-security/clipper-chip/).
15. "Re: Sandy and the Doc" (http://cypherpunks.venona.com/date/1997/01/msg02001.html). *Cypherpunks.venona.com*. Retrieved 5 September 2020.
16. "Newgroup -- distributed mailing list on the way?" (http://cypherpunks.venona.com/date/1997/02/msg00627.html). *Cypherpunks.venona.com*. Retrieved 5 September 2020.

17. "Switching to full traffic mode" (http://cypherpunks.venona.com/date/1997/02/msg02277.html). *Cypherpunks.venona.com*. Retrieved 5 September 2020.
18. "Cryptography" (http://www.mail-archive.com/cryptography@metzdowd.com). *Mail-archive.com*.
19. Hughes, Eric (1993), *A Cypherpunk's Manifesto* (http://www.activism.net/cypherpunk/manifesto.html)
20. Levy, Steven (May 1993). "Crypto Rebels" (https://www.wired.com/wired/archive/1.02/crypto.rebels.html). *Wired*.
21. Levy, Steven (2001). *Crypto: How the Code Rebels Beat the Government – Saving Privacy in the Digital Age*. Penguin. ISBN 0-14-024432-8.
22. Timothy C. May (1992), *The Crypto Anarchist Manifesto* (http://www.activism.net/cypherpunk/crypto-anarchy.html)
23. May, Timothy C. (September 10, 1994). "The Cyphernomicon: Cypherpunks FAQ and More, Version 0.666" (https://web.archive.org/web/20180612074817/https://www.cypherpunks.to/faq/cyphernomicron/cyphernomicon.html). *Cypherpunks.to*. Archived from the original (https://www.cypherpunks.to/faq/cyphernomicron/cyphernomicon.html) on 2018-06-12. Retrieved June 12, 2018. as well as Hughes's
24. John Gilmore, *home page* (https://web.archive.org/web/20100427075340/http://www.toad.com/gnu/), archived from the original (http://www.toad.com/gnu/) on 2010-04-27, retrieved 2010-08-15
25. Emphasis on the word possibility; as Sarah Smith notes, even cypherpunks recognize the impossibility of absolute anonymity. For a range of discussion on the complexities of defending anonymity within maintaining security (against terrorism e.g.), see Sarah E. Smith, "Threading the First Amendment Needle: Anonymous Speech, Online Harassment, and Washington's Cyberstalking Statute", *Washington Law Review* 93/3 (Oct. 2018): 1563-1608; Julian Assange, Jacob Appelbaum, Andy Muller-Maguhn, and Jérémie Zimmermann, *Cypherpunks: Freedom and the Future of the Internet* (OR Books, 2012/2016). ISBN 978-1-939293-00-8, Ebook ISBN 978-1-939293-01-5; Dennis Bailey, *The Open Society Paradox : Why the 21st Century Calls for More Openness — Not Less* (Dulles VA: Potomac, 2004), 28-29; and Eric Hughes <hughes@soda.berkeley.edu>, "A Cypherpunk's Manifesto" (9 March 1993): https://www.activism.net/cypherpunk/manifesto.html
26. Matt Blaze (1994), *Protocol failure in the escrowed encryption standard* (http://portal.acm.org/citation.cfm?id=191193)
27. "Yahoo! Groups" (https://groups.yahoo.com/neo/groups/cypherpunks-lne-archive/conversations/messages/5869/). *groups.yahoo.com*. 2002-10-31. Retrieved 2019-02-25.
28. "Apple takes strong privacy stance in new report, publishes rare "warrant canary" " (https://arstechnica.com/tech-policy/2013/11/apple-takes-strong-privacy-stance-in-new-report-publishes-rare-warrant-canary). *Ars Technica*. 2013.
29. "Cryptography Export Restrictions" (https://www.freeswan.org/freeswan_trees/freeswan-1.5/doc/exportlaws.html). *www.freeswan.org*. Retrieved 2020-12-06.
30. Electronic Frontier Foundation (1998), *Cracking DES: Secrets of Encryption Research, Wiretap Politics, and Chip Design* (https://archive.org/details/crackingdes00elec), Electronic Frontier Foundation, ISBN 1-56592-520-3
31. Blaze; Diffie; Rivest; Schneier; Shimomura; Thompson & Wiener (1996). "Academic: Minimal Key Lengths for Symmetric Ciphers to Provide Adequate Commercial Security - Schneier on Security" (http://www.schneier.com/paper-keylength.html).
32. Hal Abelson; Ross Anderson; Steven M. Bellovin; Josh Benaloh; Matt Blaze; Whitfield Diffie; John Gilmore; Peter G. Neumann; Ronald L. Rivest; Jeffrey I. Schiller & Bruce Schneier (1998), *The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption* (http://www.schneier.com/paper-key-escrow.html)
33. Steven Bellovin; Matt Blaze; David Farber; Peter Neumann; Eugene Spafford, *Comments on the Carnivore System Technical Review* (https://web.archive.org/web/20100618062919/http://www.crypto.com/papers/carnivore_report_comments.html), archived from the original (http://www.crypto.com/papers/carnivore_report_comments.html) on 2010-06-18, retrieved 2010-08-15

34. Kenneth W. Dam; Herbert S. Lin, eds. (1996). *Cryptography's Role In Securing the Information Society* (https://web.archive.org/web/20110928184335/http://cryptome.quintessenz.at/mirror/jya/nrcindex.htm). Washington, D.C.: National Research Council. p. 688. ISBN 0-309-05475-3. LCCN 96-68943 (https://lccn.loc.gov/96-68943). Archived from the original (http://cryptome.quintessenz.at/mirror/jya/nrcindex.htm) on September 28, 2011.
35. "The Applied Cryptography Case: Only Americans Can Type!" (http://www.ka9q.net/export/).
36. Schneier, Bruce (1996). *Applied Cryptography* (2nd ed.). John Wiley & Sons. ISBN 0-471-11709-9.
37. Adam Back, *export-a-crypto-system sig, web page* (http://www.cypherspace.org/rsa/)
38. Adam Back, *post to cypherpunks list, RSA in six lines of Perl* (http://www.cypherspace.org/rsa/org-post.html)
39. Vince Cate, *ITAR Civil Disobedience (International Arms Trafficker Training Page)* (http://online.offshore.com.ai/arms-trafficker/)
40. Zurko, Marie Ellen (1998-10-07). "Crypto policy costs the US a citizen" (http://www.ieee-security.org/Cipher/PastIssues/1998/issue9810/issue9810.txt). *Electronic CIPHER: Newsletter of the IEEE Computer Society's TC on Security and Privacy* (29). Retrieved 2013-10-11.
41. Dawson, Keith (1996-05-05). "Become an international arms trafficker in one click" (https://web.archive.org/web/19970116044849/http://www.tbtf.com/archive/05-05-96.html#i-a-traf). *Tasty Bits from the Technology Front*. Archived from the original (http://tbtf.com/archive/1996-05-05.html#i-a-traf) on 1997-01-16. Retrieved 2013-10-11.
42. Neal Stephenson, *Cryptonomicon cypher-FAQ* (https://web.archive.org/web/20100528150638/http://web.mac.com/nealstephenson/Neal_Stephensons_Site/cypherFAQ.html), archived from the original (http://web.mac.com/nealstephenson/Neal_Stephensons_Site/cypherFAQ.html) on May 28, 2010
43. "cryptoparty.org - cryptoparty Resources and Information" (https://web.archive.org/web/20120912144522/https://cryptoparty.org/wiki/CryptoParty). *Cryptoparty.org*. Archived from the original (https://cryptoparty.org/wiki/CryptoParty) on 12 September 2012. Retrieved 5 September 2020.
44. "Warm Party for a Code Group" (https://web.archive.org/web/20090305092908/http://www.wired.com/culture/lifestyle/news/2002/09/55114). *Wired*. September 13, 2002. Archived from the original (https://www.wired.com/culture/lifestyle/news/2002/09/55114) on March 5, 2009.
45. "Archived copy" (https://web.archive.org/web/20160101223032/https://marc.info/?a=90366091900010). Archived from the original (https://marc.info/?a=90366091900010) on 2016-01-01. Retrieved 2015-10-04.
46. Rodger, Will (30 November 2001). "Cypherpunks RIP" (https://www.theregister.co.uk/2001/11/30/cypherpunks_rip/). *The Register*. Retrieved 13 July 2016.
47. "Officers - Open Source Club at Ohio State University" (https://web.archive.org/web/20160304205216/http://opensource.osu.edu/about/officers). Archived from the original (http://opensource.osu.edu/about/officers) on 2016-03-04. Retrieved 2011-07-01.
48. Franchesci-Bicchierai, Lorenzo (20 September 2014). "Egypt's New Internet Surveillance System Remains Shrouded in Mystery" (http://mashable.com/2014/09/19/egypts-new-internet-surveillance-system/). Retrieved 23 September 2014.
49. Hastings, Sean (2007). *God Wants You Dead* (1st ed.). Vera Verba. ISBN 978-0979601118.
50. Evans, Jon (13 January 2013). "Nadia Heninger Is Watching You" (https://techcrunch.com/2013/01/12/nadia-heninger-is-watching-you/). Retrieved 23 September 2014.
51. Grigg, Ian (2001). Frankel, Yair (ed.). "Financial Cryptography in 7 Layers" (https://link.springer.com/chapter/10.1007%2F3-540-45472-1_23). *Financial Cryptography*. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer. **1962**: 332–348. doi:10.1007/3-540-45472-1_23 (https://doi.org/10.1007%2F3-540-45472-1_23). ISBN 978-3-540-45472-4.
52. "Mac Crypto - Info" (http://www.vmeng.com/mc/). *Vmeng.com*. Retrieved 5 September 2020.
53. "IFCA" (http://www.ifca.ai/). *Ifca.ai*.
54. "Jillian York" (https://www.eff.org/about/staff/jillian-york). *Electronic Frontier Foundation*. 2011-10-07.

Further reading

- Andy Greenberg: *This Machine Kills Secrets: How WikiLeakers, Cypherpunks, and Hacktivists Aim to Free the World's Information*. Dutton Adult 2012, ISBN 978-0525953203

External links

- *A Cypherpunk's Manifesto* (http://www.activism.net/cypherpunk/manifesto.html) written by Eric Hughes
- *The Crypto Anarchist Manifesto* (http://www.activism.net/cypherpunk/crypto-anarchy.html) written by Timothy C. May
- Assange 'The World Tomorrow' — Cypherpunks uncut version (https://www.youtube.com/watch?v=i85fX9-sKYo)
- *The Cyphernomicon* (http://www.swiss.ai.mit.edu/6805/articles/crypto/cypherpunks/cyphernomicon/CP-FAQ) by Timothy C. May ("Cypherpunks FAQ and More" from 1994)
- Archives of the first eight years of the mailing list (Zipped, 83MB) (http://cryptome.org/cpunks/cpunks-92-98.zip)
- "Warm Party for a Code Group" (http://archive.wired.com/culture/lifestyle/news/2002/09/55114) - Cypherpunks 10 year anniversary (article in Wired)
- Crypto Rebels (http://archive.wired.com/wired/archive/1.02/crypto.rebels.html), Wired Magazine issue 1.02 (May/Jun 1993)
- The Crypto Project (https://crypto.is/), a revitalization of the Cypherpunk movement