

# Cypherpunk anonymous remailer

A **Cypherpunk anonymous remailer**, also known as a Type I remailer, is a type of **anonymous remailer** that receives messages encrypted with **PGP** or **GPG**, follows predetermined instructions to strip any identifying information, and forwards the messages to the desired recipient.<sup>[1]</sup>

Cypherpunk anonymous remailers are vulnerable to **traffic analysis attacks**, which take advantage of the predictable order in which messages are sent to recipients. This predictability can potentially reveal the identity of the sender. To address this weakness, Type II and Type III remailers were developed.<sup>[2]</sup> Prior to the introduction of **Mixmaster** (Type II) remailers, users attempted to mitigate this issue by sending messages in batches<sup>[3]</sup> or by using multiple remailers in sequence to further obscure the sender's identity.<sup>[4]</sup>

Mixmaster remailers were built upon the technology of Cypherpunk remailers, rendering the latter **obsolescent**.<sup>[5]</sup> However, there are still websites and systems which rely on the general ideas of layered encryption and identity obfuscation behind Type I remailers.<sup>[6]</sup>

## History

---

The **Cypherpunk** movement emerged in the late 1980s and early 1990s, consisting of activists, cryptographers, and computer scientists who believed in the use of **cryptography** as a means to safeguard **privacy** and resist government interference. They played a crucial role in the development of privacy technologies, including remailers.<sup>[7]</sup>

## Uses

---

While they are mostly considered obsolete due to the Mixmaster being the most common remailer type, Cypherpunk remailers are still applicable in niche applications for those who have no other accessible options. For example, sites that are censored or blocked by **governments** can use such remailers to circumvent this censorship. Cypherpunk remailers also require less setup and fewer resources to run, and can therefore be a suitable solution for those under time constraints or with few available assets.

## See also

---

- [Anonymity](#)
- [Anonymous P2P](#)

- Anonymous remailer
- [Mixmaster anonymous remailer](#) (Type II)
- [Mixminion](#) (Type III)
- [Onion routing](#)
- [Tor \(network\)](#)
- [Pseudonymous remailer](#) (aka. nim servers)
- [Pen net remailer](#)
- [Data privacy](#)
- [Traffic analysis](#)

## Notes

---

- The additional headers used in this context are referred to as "pseudo-headers" because they are not included in the RFC 822 headers specification for email.
- Messages sent to Cypherpunk remailers can be layered, meaning they pass through multiple Cypherpunk remailers to minimize the chances of identifying the sender.
- Some Cypherpunk remailers also function as [Mixmaster anonymous remailers](#), enabling them to divide long Cypherpunk messages into Mixmaster packets and forward them to the next remailer if it supports Mixmaster functionality.
- Many users of Cypherpunk remailers may choose to repeat steps 1–4 to add additional layers of protection to their messages, routing them through multiple remailers for enhanced privacy and security.

## Further reading

---

- *Email Security*, [Bruce Schneier](#) (ISBN 0-471-05318-X)
- *Computer Privacy Handbook*, Andre Bacardi (ISBN 1-56609-171-3)

## External links

---

- [About.com: Send Email Anonymously – Chaining Remailers with PGP](http://email.about.com/library/weekly/aa042400a.htm) (<http://email.about.com/library/weekly/aa042400a.htm>) Archived (<https://web.archive.org/web/20051024191223/http://email.about.com/library/weekly/aa042400a.htm>) 2005-10-24 at the [Wayback Machine](#)

- [Feraga.com: How to use a Type I Anonymous Remailer \(http://feraga.com/node/73\)](http://feraga.com/node/73) (link not active 12 May 2010, see [archive version \(https://web.archive.org/web/20070223110507/http://feraga.com/node/73\)](https://web.archive.org/web/20070223110507/http://feraga.com/node/73) )

## References

---

1. "Anonymous Remailers" ([https://mason.gmu.edu/~afinn/html/tele/components/anonymous\\_remailers.htm](https://mason.gmu.edu/~afinn/html/tele/components/anonymous_remailers.htm)) . *mason.gmu.edu*. Retrieved 2023-12-11.
2. Van Oorschot, Paul C. (2 March 2023). "Anonymous remailers + secure email" (<https://web.archive.org/web/20231231022203/https://people.scs.carleton.ca/~paulv/anonRemailerNotes.pdf>) (PDF). Archived from the original (<https://people.scs.carleton.ca/~paulv/anonRemailerNotes.pdf>) (PDF) on 2023-12-31.
3. Anonymous Remailers. (n.d.). Retrieved August 10, 2023, from [1] ([https://mason.gmu.edu/~afinn/html/tele/components/anonymous\\_remailers.htm](https://mason.gmu.edu/~afinn/html/tele/components/anonymous_remailers.htm)) Archived ([https://web.archive.org/web/20210924022208/http://mason.gmu.edu/~afinn/html/tele/components/anonymous\\_remailers.htm](https://web.archive.org/web/20210924022208/http://mason.gmu.edu/~afinn/html/tele/components/anonymous_remailers.htm)) 2021-09-24 at the [Wayback Machine](#)
4. Remailers: Send Emails without Registration. (n.d.). Retrieved August 10, 2023, from [2] ([http://www.whonix.org/wiki/Remailer#Cypherpunk\\_Remailer](http://www.whonix.org/wiki/Remailer#Cypherpunk_Remailer)) Archived ([https://web.archive.org/web/20230609191143/https://www.whonix.org/wiki/Remailer#Cypherpunk\\_Remailer](https://web.archive.org/web/20230609191143/https://www.whonix.org/wiki/Remailer#Cypherpunk_Remailer)) 2023-06-09 at the [Wayback Machine](#)
5. Winkler, S., & Zeadally, S. (2015). An analysis of tools for online anonymity. *International Journal of Pervasive Computing and Communications*, 11(4), 436–453. [3] (<https://doi.org/10.1108/IJPCC-08-2015-0030>) Archived (<https://web.archive.org/web/20230813203517/https://www.emerald.com/insight/content/doi/10.1108/IJPCC-08-2015-0030/full/html>) 2023-08-13 at the [Wayback Machine](#)
6. Lutkevich, Ben (April 2021). "What is Obfuscation?" (<https://www.techtarget.com/searchsecurity/definition/obfuscation>) .
7. Assange, Julian (26 November 2012). *Cypherpunks: Freedom and the Future of the Internet*. OR Books. pp. 70–90. [ISBN 978-1-939293-00-8](#).