See also 1996 overview by S. Parekh: https://firstmonday.org/ojs/index.php/fm/article/download/476/397

Anonymous remailers, Types 0-3 (rough notes)

Type 0 (simple remailers). Basic idea: strip headers & original email addr, resend using pseudonymous email-addr

- popular, largest at time (500K+ users): pseudo-anonymous remailer anon.penet.fi (J. Helsingius), 1992-96
- server admin keeps a trusted db (basic **nym server**) associating original email addrs to pseudonym addrs
- penet shut down '96 by owner due to legal issues (Church of Scientology triggered warrant served on CalTech)

Type I remailers (aka **cypherpunk remailers**)
Advantage over Type 0 or "penet": chain of remailers + PGP encryption.

- Nested set of encrypted messages, each with instructions on next hop + package itself to be forwarded.
  Each stage removes an encryption layer (also removes decrypted instructions at current layer).

  Postal mail analogy: outer envelope has address of a first mail server, inside is another envelope with instructions/address of a second, and so on, until final last envelope contains message content for recipient Bob.

  (Cf: headers in TCP message layers, but Type I remailer also uses encryption at each "envelope layer")
- Type I alternatives: PGP encrypt + mail servers or USENET bulletin boards/addrs (to anonymize recipient)
- Type I issues: traffic analysis (also: active attackers). For basic idea consider simple analogy:

  - suppose you're shipping 3 different items in wooden boxes: a rabbit, goat, elephant, by courier, rail, trucks

  - observing box sizes & loading/unloading times: alows tracking the packages, reveals which is which.

  - same idea allows: tracking email messages through a network ... by size, message flows, timing.

  - model: powerful attacker can observe size of all msgs in/out of remailers + arrival/departure time (metadata)
  As layers are unwrapped, message also shrinks in size by a predictable amount per hop (aids tracking in/out).

  Thus: messages easily traced thru a chain of remailers (esp. if no delays in forwarding). Or by using mail logs.
- Better (cf. Type II): introduce pools (delays) with message reordering (cost: latency for legit recipients).

  But many attacks known, e.g.: attacker sends large volume of recognizable msgs, to flush out storage pools.

Type I has weaknesses, but good interoperability (anyone technically skilled can send, with manual construction)

Type II remailers — motivated by weaknesses of Type I:
Mixmaster is popular Type II remailer, still active (2023): https://mixmaster.sourceforge.net/
FAQ: https://mixmaster.sourceforge.net/faq.shtml
IETF draft: https://datatracker.ietf.org/doc/html/draft-sassaman-mixmaster-03
Based on Chaum's **mix-net** concept. Beyond simply nesting of PGP msgs.
Goals: anonymity, unobservability (hides sender-recipient relation).

- Email messages are split into equal-size parts (packets).
  Parts sent on independent paths. Constraint: all same-msg parts end at a same last node, it reassembles them.
  At each node, message parts are stored in **pools**; periodically, a random subset is selected and forwarded.
  Thus parts arriving at any remailer node are reordered (different parts are delayed randomly).
  (One simple attack is: replay msg to retrace its path; remailer should prevent replays, i.e., send once only)

- Parts may go through up to 20 remailer nodes (each keeps a pool of parts). Packet header has 20 slots.
  At each forwarding step: current remailer node decrypts header using RSA decryption private key.
  One header is removed, others all move up 1 slot, newly-empty last header is replaced by random padding.
- Type II issues: trust in individual remailers; latency; number of msgs (+ reordering) relies on volume of msgs.

  General view: "Type IIs largely solved anonymous/pseudonymous email" as a practical problem.

  Disadvantage (vs. Type I): Type II mail sender (but not receiver) requires Mixmaster client (for formatting).

Type III remailer: Mixminion (Oakland 2003 paper, Danezis et al.)
`https://www.mixminion.net/minion-design.pdf` (good general background on anonymous remailers)
Improves a few items beyond Type II/Mixmaster.

Aside: an ongoing risk of plain email is that messages can be stored cheaply, forever, by many stakeholders.

Secure email products (circa 2022) — begin with a (marketing-type NordVPN) explainer:
"Top 5 free anonymous email providers in 2022" `https://www.youtube.com/watch?v=FnC5Cw51Hk8`

Anon email aim: prevent trace-back to you (hides metadata, often encrypts content). So don't include identity, device name, IPaddr info in your msg content. Preferably, provider keeps no records of msg content or metadata.

1. ProtonMail [free + premium features for a fee]

   Uses PGP before message leaves device. But doesn't encrypt metadata or Subject lines.
   Can set up account without giving any PII, can send *self-destructing* msgs (auto-deleted? at server or client?)

2. Tutanota.

   End-to-end encrypts entire inbox, Subject lines, contact lists. Can encrypt for non-users via pre-shared secret (password). Strips IP addr from email. Open-src (how do you know what's in binary unless you self-compile?)

3. Secure Email. (Uses TLS.)

   "The service doesn't log your IP addr" so it can't be warranted to pass on data that it doesn't have. (True?)

4. Guerilla Mail (a web service, per later video) — `www.gorillamail.com`

   Around for over 10 yrs. Provides disposable email addr (free). You can also receive email on that.
   And can send anonymous mail without an account (if you wish; but presumably then can't get reply email).

5. Mailfence.

   Uses OpenPGP, "the most widely used email encryption standard" (almost surely a false claim). One account can have multiple email addr aliases. Filters incoming email for trackers, spam.

Amateur 2023 video (1m) explaining Gorilla mail (above): `https://www.youtube.com/watch?v=6bWF5Z57-bo`
Summary of video: various web sites let you enter and send anonymous email.
Use a VPN to get to a web site like gorrilla mail, then paste the target email addr and body content into web form.
Send an email to yourself and you'll see it arrive with a random source address.
Issues: must trust VPN (re: your IP address), and gorilla mail site (anonymous email addr, but msg sent cleartext?), plus recipient can't respond if one-time addr (some remailers accommodate this by providing **reply blocks**).