# 2020 Crypto Talk Resources

## News

* [Solar Winds](https://www.schneier.com/crypto-gram/archives/2021/0115.html)
* [Zodiac Killer solved](https://youtu.be/-1oQLPRE21o)
* [Breaking Caesare and Vigenere by Quantum??](https://ia.cr/2021/554) (overkill!)

## Factoring Tempest in a teacup

* [Factoring paper yawn](https://ia.cr/2021/933)
* [Discussing on SE](https://crypto.stackexchange.com/questions/88582/does-schnorrs-2021-factoring-method-show-that-the-rsa-cryptosystem-is-not-secur)
* [eh no](https://www.cryptologie.net/article/515/this-destroyes-the-rsa-cryptosystem/)
* [Bruce S says no](https://www.schneier.com/blog/archives/2021/03/no-rsa-is-not-broken.html)

## PGP ? Maybe not

* [Debian alternate trust](https://lists.debian.org/debian-devel-announce/2020/09/msg00000.html) - the last unique use-case for PGP Web-of-Trust replaced due to COVID in part
* [Latacora - stop using encrypted email 2020](https://latacora.micro.blog/2020/02/19/stop-using-encrypted.html)
* [Latacora - The PGP Problem 2019](https://latacora.micro.blog/2019/07/16/the-pgp-problem.html)
* my 2019 comments [odp](http://www.blu.org/meetings/2019/09/Crypto2019.odp) [flipbook](http://www.blu.org/meetings/2019/09/Crypto2019.flipbook) \* [pdf](http://www.blu.org/meetings/2019/09/Crypto2019.pdf)
* [A history of end-to-end encryption and the death of PGP](https://www.cryptologie.net/article/487/a-history-of-end-to-end-encryption-and-the-death-of-pgp/) Jan, 2020

Alternatives - always know your threat model, as a solution against a different threat model may not be right for you!

* Divorce/Probate Lawyers and Child Welfare Dept ?
* Foreign Nation-State Intelligence / Sabotage?
* Domestic Tax or Law enforcement?
* Housemates ?
* Religious Police ?
* Advertising privacy-breaking data-hoarders ?

## Alternatives

* [Alternatives to PGP by author of Manning Real-world Cryptography](https://www.cryptologie.net/article/502/alternatives-to-pgp/) - recaps what's wrong too. May, 2020
* [2021 public Pros and Cons](https://www.slant.co/options/5270/alternatives/~email-pgp-alternatives)

### Email

PGP email plug-in provided a semi-convenient integration to do attachment of real-body as encrypted file, that used the Web of Trust PKI for public-key distribution.

Internet Email protocols are basically broken from birth re Security/Privacy/authenticity. PGP only ever did securing of bodies, not of headers, which for many threat models are problematic too. Secure attachments by encrypting the real message as a file and attaching it is possible with any file-at-rest encryptor, using either PKI or symmetric with out-of-band key or passphrase transmission.

* AxCrypt - Freemium, Windows Mac & Mobile only. Targetted to securing email attachments.

### One-time Authenticated Message (**signcryption**)

Assymetric keyed -

* [saltpack](https://saltpack.org/) (lacks forward secrecy?), implemented at [keybase.io](https://keybase.io) (now owned by Zoom, so if you're worried about China, maybe not?) and [keys.pub](https://keys.pub/)
* [age](https://github.com/FiloSottile/age) and [rage](https://github.com/str4d/rage) alas don't [provide signing](https://github.com/FiloSottile/age/issues/51) yet?

### Chat

* [Tweet](https://twitter.com/mshelton/status/1170028705378263041)
* [Signal](https://signal.org/) "is hardened" requires phone#; single device at a time plus desktop; FLOSS.
* [WhatsApp](https://www.whatsapp.com/) "is popular" but owned by FaceBook since 2014 so ...
* [Wire](https://wire.com/en/) "is beautiful"
* [Threema](https://threema.ch/) "lets you talk to Europeans" works well to EU; mobile only?
* [Matrix](https://matrix.org/) - Federated protocol ! [Element aka Riot](https://about.riot.im/)=> is lead implementation; see e.g [2019 LWN](https://lwn.net/Articles/779331/); bridges networks, Voip, decentralized.
* TextSecure
* Telegram (not fully FLOSS, requires a phone #, only some messages E2E)

### File Authentication (Signing)

* [minisign](https://jedisct1.github.io/minisign/)
* [Signify](https://github.com/aperezdc/signify) used by OpenBSD packaging
* [Debian alternate trust](https://lists.debian.org/debian-devel-announce/2020/09/msg00000.html)
* [TUF/Notary](https://duckduckgo.com/?q=+Update+Framework+(TUF)+provides+Notary+service)

### Files at rest, Files in motion; Blobs=file at rest

Blob could also be an Attachment - provided symmetric key is passed via a secure channel.

Symmetric encryption - require secure channel to agree a key, of course! \* [Encpipe](https://github.com/jedisct1/encpipe) \* [Scrypt](https://www.tarsnap.com/scrypt.html) \* [eureka](https://github.com/mimoo/eureka) \* [nacl/box](https://godoc.org/golang.org/x/crypto/nacl/box) and [nacl/secretbox](https://godoc.org/golang.org/x/crypto/nacl/secretbox) and impleemntations in the language of your choice! See Saltpack above at Signcryption.

* [Magic Wormhole](https://github.com/warner/magic-wormhole) - in motion only, Syncronous transfer E2E only. (So competes with Apple Airdrop?) Uses [PAKE: Password Authenticated Key Exchange](https://blog.cryptographyengineering.com/2018/10/19/lets-talk-about-pake/) [2](https://en.wikipedia.org/wiki/Password-authenticated_key_agreement); handles firewalls and optionally TOR. [2016 slides](https://www.lothar.com/~warner/MagicWormhole-PyCon2016.pdf)
* Encrypted backups - tneds to be a feature of your backup provider. Can of course use any file at rest encryption on a GZ file.

### Keyservers/Web-of-Trust

* Keybase.io - bought by Zoom so plausibly under control of hostile nation-state if that bothers you
* "Broadcast of Trust" - posting public key or key signatures on social media, as we did with PGP Fingerprints in .sig
* LastPass Family/Group (paid tier) to share symetric key / passphrase with frequent people you can be seen to be associated with.

## Post Quantum Future

Rerun from 2020

* [Bruce S](https://www.schneier.com/blog/archives/2020/07/update_on_nists.html)
* [More Bruce](https://www.schneier.com/blog/archives/2020/09/more_on_nists_p.html)
* Hacker Public Radio episode [HPR3147](https://archive.org/details/hpr3147) \* [eps](http://hackerpublicradio.org/eps.php?id=3147)
* [IACR 2020-455](https://eprint.iacr.org/2020/455)
* [Overview scribd](https://www.scribd.com/document/474476570/PQC-Overview-Aug-2020-NIST)
* [NIST forum](https://groups.google.com/a/list.nist.gov/g/pqc-forum/c/erUpGzb8n9M)
* [Dilitium crystals](https://pq-crystals.org/dilithium/index.shtml) yes they went for the punt
* [NIST forum 2](https://groups.google.com/a/list.nist.gov/g/pqc-forum)
* [NSA](https://www.nsa.gov/what-we-do/cybersecurity/post-quantum-cybersecurity-resources/)
* [WP: McEliece](https://en.wikipedia.org/wiki/McEliece_cryptosystem)
* [article](https://thebulletin.org/2020/02/keeping-classified-information-secret-in-a-world-of-quantum-computing)
* [LLNL report](https://cgsr.llnl.gov/content/assets/docs/QuantumComputingandCryptography-20190920.pdf)

## Declassified MILCRYPT III

* [news vis Schneier](https://www.schneier.com/blog/archives/2021/01/military-cryptanalytics-part-iii.html)
* [WP](https://en.wikipedia.org/wiki/Military_Cryptanalytics)
* [declassified file FOIA](https://www.governmentattic.org/39docs/NSAmilitaryCryptalyticsPt3_1977.pdf)

## Dermot Turing & Bletchley Park ; US National Crypto museum

* [BP](https://bletchleypark.org.uk/)
* [UK Nat'l Museum of Computing, at BP](https://www.tnmoc.org/)
* [NSA Museum about](https://www.nsa.gov/about/cryptologic-heritage/museum/) [https://cryptologicfoundation.org/visit/museum/national\_cryptologic\_museum.html](http://docs.google.com/Foundation)
* [Book X-Y-Z](https://dermotturing.com/my-recent-books/x-y-z-the-real-story-of-how-enigma-was-broken/)
* [Book The Bombe](https://www.tnmoc.org/tnmocshop/the-bombe-the-machine-that-defeated-enigma-dermot-turing)
* [The real story of how Enigma was broken - Sir Dermot Turing](https://www.youtube.com/watch?v=qn_BBQEjCxI)
* [new Collosus video](https://www.youtube.com/watch?v=g2tMcMQqSbA)
* [The Lawfare Podcast: Project VENONA, with David Hatch, senior historian NSA](https://www.lawfareblog.com/lawfare-podcast-project-venona)

# RUBICON/MINERVA Scandal Part II: "The Last Rotor Machine"

Continued from 2020 [slides](http://www.blu.org/meetings/2020/09/) [video](https://youtu.be/K6NQUHLBP3c)

Late Breaking History "The Scandalous History of the Last Rotor Cipher Machine" [IEEE Spectrum, Peter Adams](https://spectrum.ieee.org/the-scandalous-history-of-the-last-rotor-cipher-machine) Aug 2021

## Reinjecting Rotor Machines: Late Electro-Mechanical Transitional

What came after WW2 Rotor machines ( Enigma (1920s-1930), US SIGABA, and UK TYPEX ), and before Elelectronic machines, besides the WW2 and early Cold War "Pinwheel" machines?

* [image](https://en.wikipedia.org/wiki/HX-63#/media/File:Loopback-rotor.png) [PD image](https://commons.wikimedia.org/wiki/File:Loopback-rotor.png)

### Fialka M-125 (Soviet/Russian)

Doesn't appear to actually reinject but improves on Enigma otherwise.

* [CM](https://www.cryptomuseum.com/crypto/fialka/index.htm)
* [german museum](https://www.deutsches-spionagemuseum.de/en/sammlung/fialka/)
* [wp](https://en.wikipedia.org/wiki/Fialka)
* [jproc](http://www.jproc.ca/crypto/russian_m125_fialka.html)
* [W1TP](http://www.w1tp.com/enigma/mfialka.htm)
* [article](https://www.wondersandmarvels.com/2014/11/fialka-the-bigger-better-russian-enigma.html)
* [another](https://people.duke.edu/~ng46/collections/crypto-fialka.htm)
* [tech details archived](https://web.archive.org/web/20090430164219/www.xat.nl/fialka/)
* [Reflector "Magic Circuit" hack that makes non-reciprocal and allows 1/30 identity](https://web.archive.org/web/20080504122132/http://www.xat.nl/fialka/circuit/magic.htm)

### HX-63 (1963)

* [IEEE Spectrum, Peter Adams](https://spectrum.ieee.org/the-scandalous-history-of-the-last-rotor-cipher-machine) Aug 2021
* [WP DE](https://de.wikipedia.org/wiki/HX-63) [https://en.wikipedia.org/wiki/HX-63](http://docs.google.com/WP%20EN)
* [jproc](http://www.jproc.ca/crypto/hx63.html)
* [CM](https://www.cryptomuseum.com/crypto/hagelin/hx63/index.htm)

### KL-7 (1945-1985)

* [CM](https://www.cryptomuseum.com/crypto/usa/kl7/index.htm)
* [WP](https://en.wikipedia.org/wiki/KL-7)

### Other

* General Rotor tech details covering above machines inter alia [1](http://home.ecn.ab.ca/~jsavard/crypto/pp010303.htm) [2](http://home.ecn.ab.ca/~jsavard/crypto/ro020301.htm)