Boston Linux/Unix

Annual Cryptology Talk

September 15, 2021

Bill Ricker

(*Annual **Web of Trust** signing deferred*
...due to you-know-what...
and maybe forever ...)

Agenda

- 2021 Cryptology News in Review
- PGP Alternatives
- 2021 the number
- History Resources
- Part II of RUBICON/MINERVA (continued from 2020, YT)

2021 News - Cracks

- *Solar Winds* supply-chain hack *bypassed* multi-factor by forging MFA cookie using stolen integration secret key. (BS-CG)
- Final Zodiac Killer cipher cracked with computer assist. YT
- Grandson of Spectre/Meltdown abuses µOp cache

Breaking Caesar and Vigenere by quantum computers?

- ia.cr/2021/554
- Sounds like overkill **and** also beyond today.
- A prof commented dryly that his “students ran Caesar with 20 qubits and IBM HW had stability difficulty”

2021 ~~News~~ - Factoring

"Fast Factoring Integers by SVP Algorithms, corrected"

- 2021/232 withdrawn; ia.cr/2021/933
- claimed Factoring breakthrough
- Crypto/security world pauses, frantically reads, and *yawns*.
  - [StackExchange]
  - Running Commentary
  - BS-[2021.03.05]

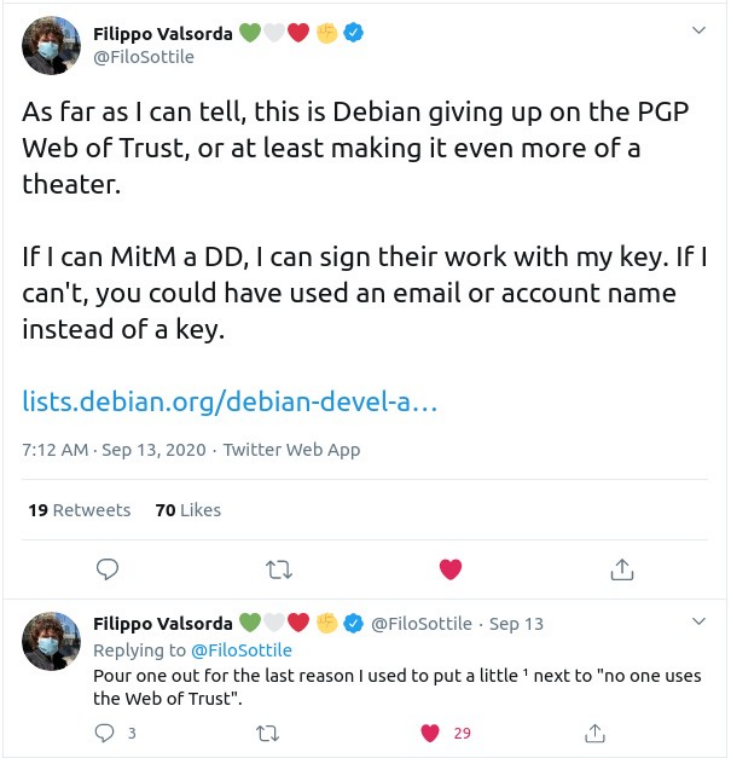
Twitter

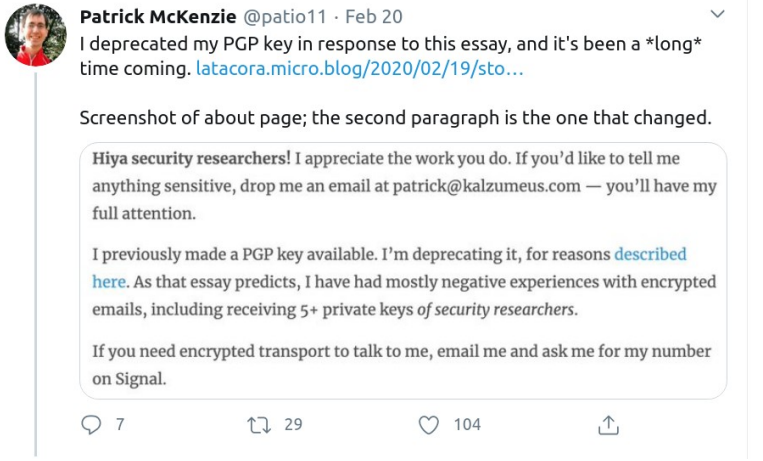
- Justin Troutman @justintroutman
  - Chosen abstracts are the new chosen plaintexts.
- Sophie, @SchmiegSophie
  - I think the paper unfortunately says more about Schnorr than it says about RSA. I'll leave it at that, it of respect for his contributions to the field.
- @EllipticKiwi
  - I have no time to look at the paper today, but he has been talking about lattice algs for factoring for more than 10 years, and making very bold claims
- Stefano Tessaro @StefanoMTessaro
  - Since the rump session at EUROCRYPT '09, where he even claimed polynomial time. It is the same paper, which has evolved over the years. (One can find several drafts of it.)
- Carsten Baum @crypto_carsten
  - Ah ok, didn't know about that. So we might classify the paper as age-induced weirdness.

PGP? Maybe not …

- DD has alternate trust root now
  - “DAM Key and identity requirements” 9/13
  - (Still need GPG to sign uploads)
- Latacora
  - “Stop Using Encrypted Email” 2020
  - “The PGP Problem” 2019

2020 rerun,
2019 rerun ...





PGP Update

- https://gist.github.com/rjhansen/67ab921ffb4084c865b3618d6955275f

2019 rerun ...

Why all the PGP h8?

- The Math is fine. (At least for now.)
- The support-all-use-cases UX is terrible.
  - Why don’t HR, Banker, Contracts office have PGP?
  - Which can result in crypto fails as well as just fail fails.
  - Normal people need fit-for-purpose tools not Legos™
- Can’t replace a flawed magic hammer with another single magic hammer

2019 rerun ...

Alternatives

- Everything depends on threat model
  - Threat Model is (partly) different per mode
  - Is your opponent
    - The auditor / avoiding data breach
    - A hostile nation-state with massive intel budget
    - A police-state with unrestained ethics
    - Nosy journalists
    - Your sister/boss/sysop

2019 rerun ...

Alternatives - Email

- Modern email supports point-to-point secure delivery
  - secures meta-data better than PGP;
  - encrypted in transit, but not at rest, may be good enough depending on threat model/regulatory
- Put sensitive content in an encrypted attachment
- Or, specialized vendor – often for Corp use, where Audit access to secured emails required and/or easy interface needed for support staff

2019 rerun ...

Alternatives – files/attachments

- Password on a ZIP
  - usually weak encryption,
  - sometimes good enough (check threat model)
  - most people have the software already
- Cloud
  - Keybase Filesystem *but Zoom/China?*
  - Or any File cryptor & any cloud
- Magic-wormhole - send file interactively (like chat)
  - Weak password + interaction = strong; live > store'n'forward
  - Uses Rendezvous, PAKE
    - Password Authenticated Key Excange => out-of-band horse-stapler passphrase
  - 2016 slide deck

2019 rerun ...

Alternatives - Chat

- Secure chat E2E easier to automate key management securely than eMail
- Stream (vs store’n’forward) avoids issues
- Choices
  - Add “keybase chat” *but Zoom/China?*

2019 rerun ...

Alternatives: Blobs, Files

- Secured Data blobs on disk or in cloud
  - nacl/box
  - nacl/secretbox.
  - Keybase saltpack (NACL usecase packaging)
- Eureka
- Magic Wormhole
  - Syncronous only

2019 rerun ...

Alternatives: Key Server

- Keybase.io
  - alas has been sold to Zoom; check your threat model!
- Put key hash in .sig and key on personal site
- Send public key via secure E2E chat
  - But still need to avoid the PGP problem of sending the private key by mistake!!
    - Will new frameworks make that confusion less likely?

2019 rerun ...

Alternatives: Signed software

- Debian packages
  - largest de facto use of PGP
  - alternative to Web of Trust for new DD/DM
  - Still using GPG signatures for uploads
- OpenBSD has `signify` & `minisign`
  - uses ED25519
- The Update Framework (TUF) provides Notary service

Eras of Cryptology?

The Eras of Cryptology – *analagous to Typography*?

- "**Classical**" - (hand-ciphers, code-books) 25BCE - 1935
  - Caesar; Vigenère; Wheatstone-Playfair; *etc*.
  - Magic Decoder Ring, Jefferson-Bazeries, *etc* (M-94, M-138-A)
  - Basically obsolete by 1900, used anyway in WW1 and even WW2 (tactical).
  - Computers just make it more obsolete.
- "**Transitional**" (*see right*) 1935-1975
  - Whatever it is, "Transitional" is *always* whatever is between Classical & Modern is *named* !
- "**Modern**" - (stored-program computers) 1975-2025
  - Software/Firmware. COTS processors. Run anywhere.
  - Block ciphers (Fiestel structure) – DES, AES, ...
  - Stream ciphers – RC4, Bluetooth, ...
  - Public-key, key negotiation, PKI Signatures (RSA, PGP,DH, EC, PKCS,
  - These are Modern but *pre-Quantum* ...
  - ⇦*You are here*
- "POST-QUANTUM" (???) 2025-????
  - Less weird name than ironic "*Post-Modern*"
  - What-ever's next
    ... just in case Quantum Computing works ...

So ... What came between **Classical** & Modern*?*

"Transitional" (e.g. in WW2 and "Cold War") 1935-1975

- (nearly) All broken during WW2, but kept classified ... so surplus resold after the war ...

- Mechanical
  - add clockwork to a decoder ring (1890s+), *junk*.
  - **Hagelin**/Crypto-AG – C-35/C-36/C-38=**M209** "Pin&Lug" mechanical adding-machine pRNG stream additive.
- Electromechanical rotors or pin-wheels
  - combine periods to get very long sequences; keys&lamps or teleprinters
  - **Enigma** – Scrambling electrical rotors, substitution, manual transcription – earliest successful, 1930-ish!
  - Tunny/Sturgeon/ABA/... - Scrambling pinwheels for 5-bit TTY current loop pulses; first on-line teleprinter !
  - **Reinjection Rotors** KL-7, HX-63, ...
- Analog Electronic Scramblers (fax, voice) – *FDR's hotline*
- **Bespoke Digital Hardware** (1965-1980?)
  - Direct precursors of Modern Stream ciphers, successors of FISH etc.
  - Still in use in much of world until mid 1990s or later due to US Export Controls on Modern cryptography.

2020 rerun ... updated

POST-QUANTUM FUTURE

"Post-Quantum Cryptography"

- Not about Quantum enciphering (mostly)
- Practical engineering of Quantum Computing remains !
  - But still concern since algorithms exist if the hardware exists.
- Goal: algorithms that resist Quantum cryptanalysis, in case that ever works.

NIST's Post-Quantum Cryptography competition continues

- July **2020**, NIST selected third-round algorithms
  "NIST initiated a competition to find and test algorithms for quantum encryption that would resist quantum decryption back in December of 2016. Two rounds of testing have been completed, and an initial group of 69 submissions have been winnowed to 15. These 15 are now in Round Three of the testing process, and it is anticipated that as many as 4 of them will be approved as standards. This news update is intended to bring you up to date on the process."
  - HPR3147 [archive audio][HPR]
  - As with prior NIST selections, public cryptanalysis by peer/competitors is culling the herd. e.g. LEDAcrypt was dropped from 3d round, because its keys are easier to recover than they should be.
  - Target proposal for public comment 2023-2024
  - [Schneier 2020.09.08]
    Daniel Apon of NIST scribd "PQC Overview August 2020" [scribd? *Really*?][*errata*]
- Candidates include Dilithium·Crystals !
- NIST PQC [forum]
  - PQCrypto 2020 virtual conference Sept. 21-23, registration is live.
  - NSA Cybersecurity Directorate guidance on NIST Round-3 PQC candidates transparently shared publicly!
- Germany already chosen Classic McElice and **FrodoKEM**

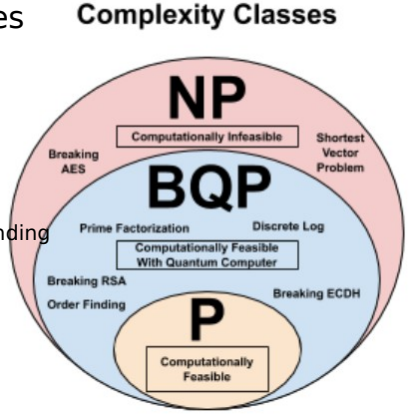
2020 rerun

Current considerations

- Non-post-quantum crypto messages can be archived today (Colorado?) for possible **VENONA**-style retro-exploitation if Quantum crack becomes a thing.
  - New desideratum beyond "Perfect Forward Secrecy"
  - Honeypots of nonsense as decoys??

"Keeping classified information secret in a world of quantum computing"
→ "Quantum Computing and Cryptography: Analysis, Risks, and Recommendations for Decisionmakers"
(1) [thebulletin] (2) [LLNL PDF]

- Theme 1: "The Race for Quantum Supremacy"
  - The Race For Quantum Supremacy Is Primarily an ***Economic*** Race
- Theme 2: "Quantum Computing Makes Current Encryption Obsolete"
  - Quantum Computing Will ***Not*** Make Encryption Obsolete
  - AES256 borderline ok … 3AES256 should be fine!
    - Since RSA keys are more at risk than AES, need PFS in session-key negotiations *now* wrto Venona II.
    - Ditch AES-128, AES-192 *now* for anything *of longterm value*.
- Theme 3: Quantum Computing Makes New Encryption More Secure Than Current Encryption
  - Quantum Computing Does ***Not*** Provide A Significantly New Encryption Capability
    - Chinese satellite entangled demo not withstanding



2021: product of primes

- 2021 = 43 * 47
- Both Hagelin Pinwheel Machines (C-52 etc) and TUNNY=Lorenz SZ42 had wheels of size 43 and 47 in co-prime wheel sequence
- TUNNY was broken on 25x23 rectangle showing diagonal of period 41.

C-52: 25,26,29,31,34,37,38,41,42,*43*,46, *47*

SZ42: **43,47**,51,53,59,37,61,41,31,29,26,23

2021: ^demo^

```
$ raku -e 'use Prime::Factor; say $_, ": ", $_.is-prime||prime-factors($_) for (25, 26, 29, 31, 34, 37, 38, 41, 42, 43, 46, 47)'
25: (5 5)
26: (2 13)
29: True
31: True
34: (2 17)
37: True
38: (2 19)
41: True
42: (2 3 7)
43: True
46: (2 23)
47: True
```

```
$ raku -e 'use Prime::Factor; say $_, ": ", $_.is-prime||prime-factors($_) for (43,47,51,53,59,37,61,41,31,29,26,23)'
43: True
47: True
51: (3 17)
53: True
59: True
37: True
61: True
41: True
31: True
29: True
26: (2 13)
23: True
```

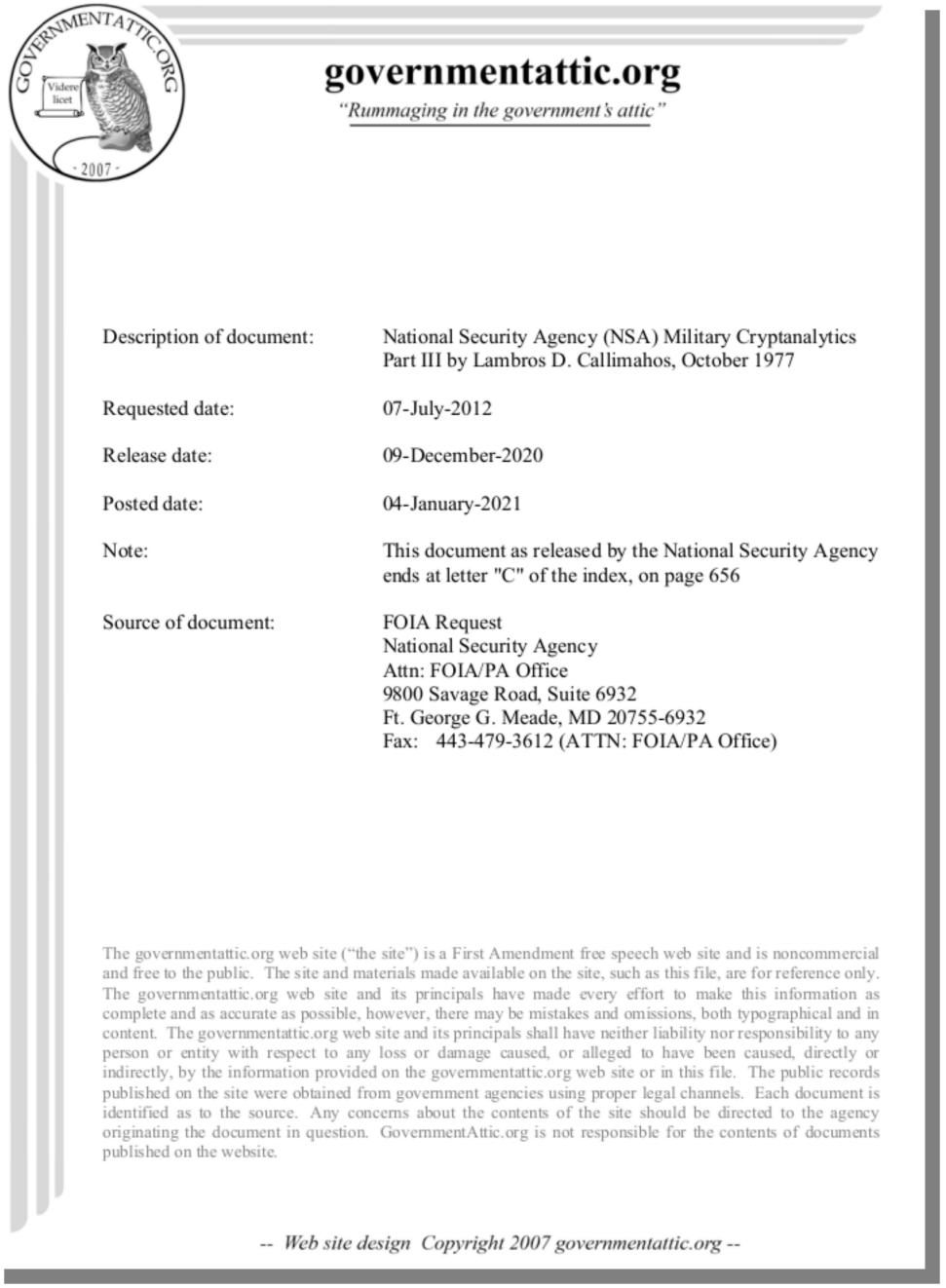
C-52: 25, 26, 29, 31, 34, 37, 38, 41, 42, *43*, 46, *47*

SZ42: **43,47**,51,53,59,37,61,41,31,29,26,23

History: Newly Declassified

NSA textbook declassified (per FOIA)

- ***Military Cryptanalytics, Part III***
  Lambros D. Callimahos, 1977. [2021.01.04]
  redacted
  - Major expansion from WFF's "Military Cryptanalysis Part III" text including LDC's monographs.
  - "Aperiodic Substitution Systems



governmentattic.org

"Rummaging in the government's attic"

Description of document:	National Security Agency (NSA) Military Cryptanalytics Part III by Lambros D. Callimahos, October 1977
Requested date:	07-July-2012
Release date:	09-December-2020
Posted date:	04-January-2021
Note:	This document as released by the National Security Agency ends at letter "C" of the index, on page 656
Source of document:	FOIA Request National Security Agency Attn: FOIA/PA Office 9800 Savage Road, Suite 6932 Ft. George G. Meade, MD 20755-6932 Fax: 443-479-3612 (ATTN: FOIA/PA Office)

Military Cryptanalytics, Part III

What's redacted?

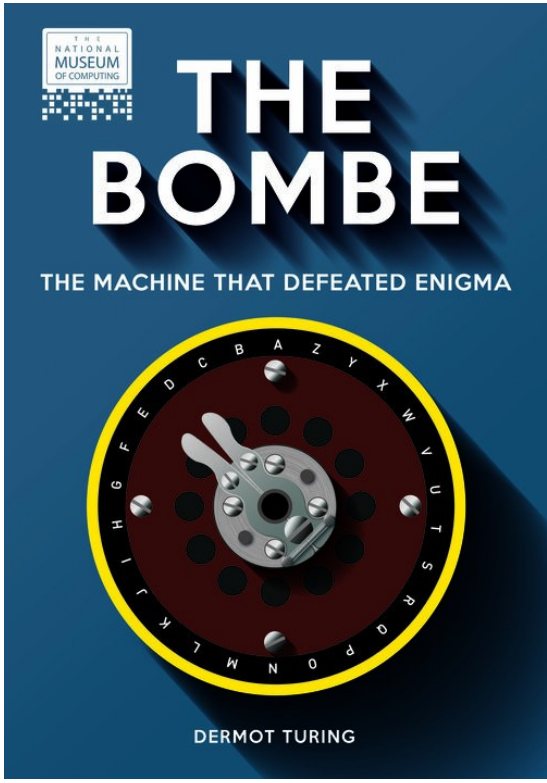
- One or more section titles are omitted from TOC under each of these headings:
  - Autokey systems
  - Long or continuous keys
  - geared disks
    - ? Kryha improvement?
  - Key analysis
  - Cryptodiagnoses
- Depth Reading

Other sections:

- Interupting key, text
- Cylindrical & strip
  - Jefferson/Bazeries/Hitt
  - incl. M-94 used in WW2
  - Cipher Device M-94 tables
- Problems (classwork)

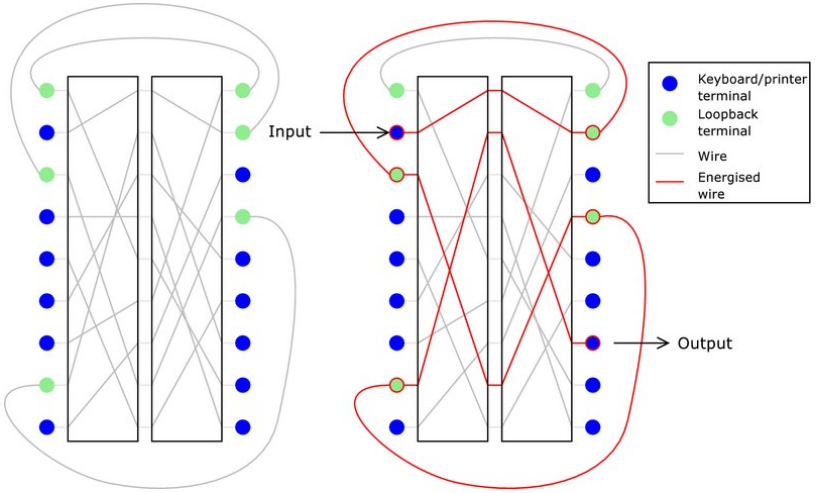
New Historical Resources

- Dermot Turing, Alan’s Nephew,2 books & videos sharing credit with Poles, boffins.
- Sr Historian at NSA, Lawfare podcast , VE NONA
- New Colossus video



Transitional: The last Rotors

- Improving on Enigma through Reinjection
  - US Army SIS discovered 1944
  - Rediscovered by industry 1953
  - Multiplies a Rotor machine's security.
  - Rather than once thru or 1+reflect, twice or more forward (& reflects)
    - Unclear to me how one assures first pass is to a looped back terminal?
    - Or is Sometimes good enough / better?



Other half of the Minerva / Rubicon Cag story from 2020 broke in 2021

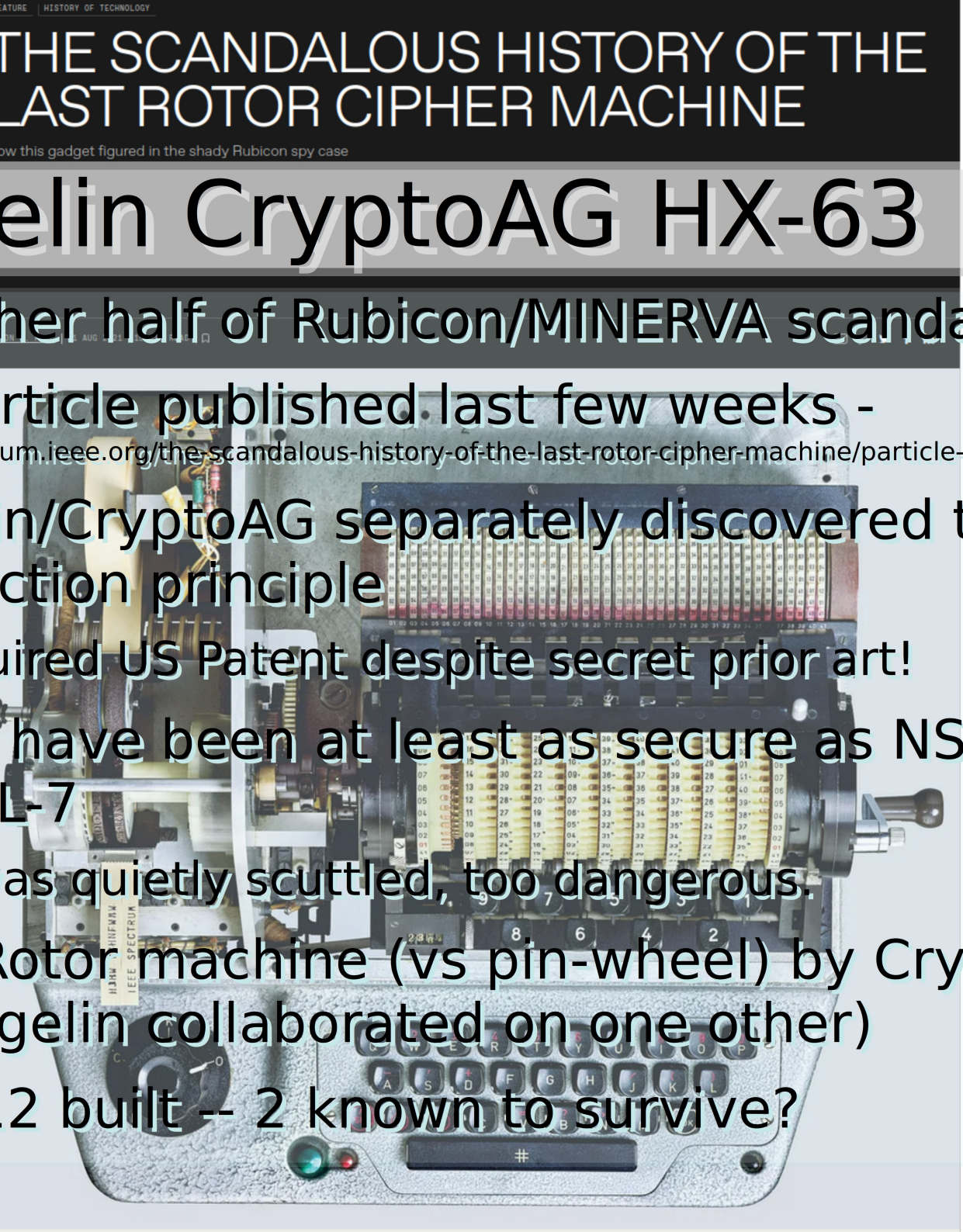
FEATURE | HISTORY OF TECHNOLOGY

THE SCANDALOUS HISTORY OF THE LAST ROTOR CIPHER MACHINE

How this gadget figured in the shady Rubicon spy case

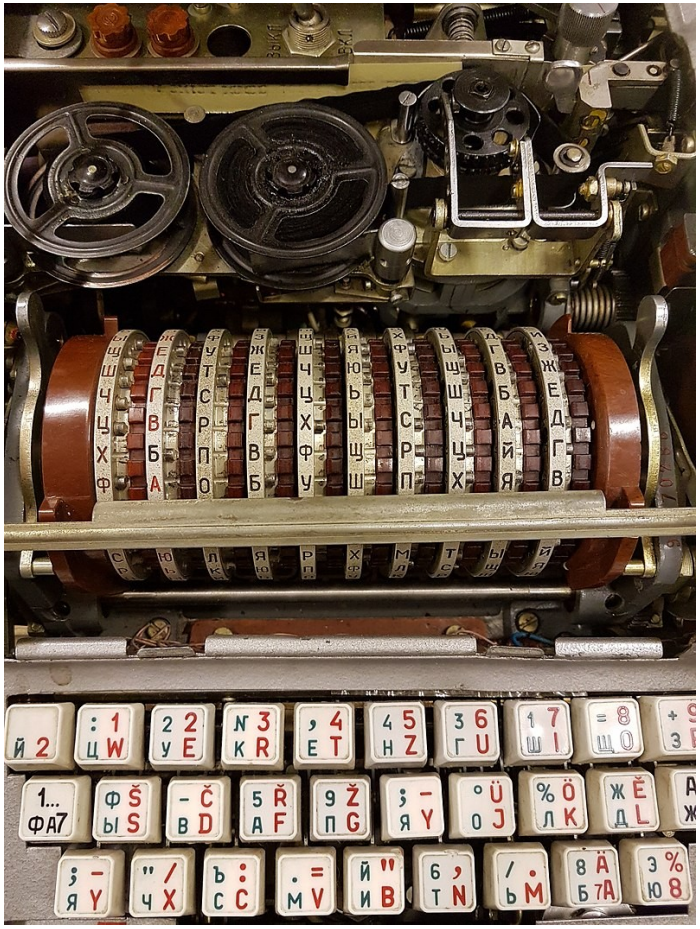
Hagelin CryptoAG HX-63

- the other half of Rubicon/MINERVA scandal !
- IEEE article published last few weeks - https://spectrum.ieee.org/the-scandalous-history-of-the-last-rotor-cipher-machine/particle-1
- Hagelin/CryptoAG separately discovered the Reinjection principle
  - Acquired US Patent despite secret prior art!
- would have been at least as secure as NSA's own KL-7
  - so was quietly scuttled, too dangerous.
- Only Rotor machine (vs pin-wheel) by CryptoAG; (Hagelin collaborated on one other)
- Only 12 built -- 2 known to survive?



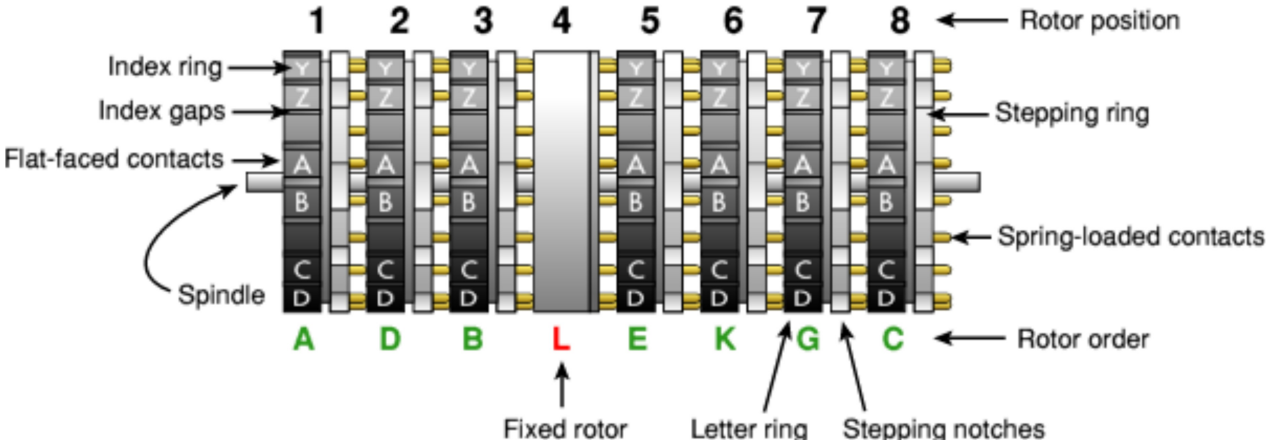
ФИАЛКА (Fialka M-125)

- 1956. 10 rotors, contra-rotating!
- Enigma Crib-Collision avoided
  - Still has reflection, mostly reciprocal, but complex reflector logic
  - total encryption can have self-encryption 1:30
    E→E (but not always E!)
    (1-elt fixed-point subcycle in permutation)
  - 3 letters rotate, so nonreciprocal
- *Said by some to have Reinjection*?
  - No? has 33 Cyrillic (and 26 Latin) letters coded on 30 pins, no extras
- TEMPEST PSU: variably powered dummy load to maintain constant mains current draw.



KL-7 aka AFSAM-7 , POLLUX/ADONIS

- 8 rotors; 26 letters + 10 reinjection = 36 contacts
- Considered unbreakable by cryptanalysis then.
- Internal rotor wiring and other keying leaked by Walker ring, and capture in fall of SVN.
- declassified in March 2021 (after accurate simulations reverse engineered)
- Synchronous timing of printer wheel
- Interoperable with 10 rotor British BID/60 Singlet by correct selection of rotors.
  - *Did Singlet have reinjection too? IDK!*



- 73 -

Q&A ?

If none, I can scroll through the HX-63 IEEE article ...

ieee