Cryptology Annual News Update and Vignette

Bill Ricker
for BLU.org (http://blu.org/cgi-bin/calendar/2022-sep)

Sept 21, 2022

Cryptology News Bulletins 2021-09 to 2022-08

Certificate Authority Root problems

Let’s Encrypt Root CA Expiration

https://community.letsencrypt.org/t/production-chain-changes/150739 (https://community.letsencrypt.org/t/production-chain-changes/150739)

```
Rich Pieri via lists.blu.org  Fri, Oct 1, 9:34 PM
to discuss
Some CA bundles like the one distributed with Sylpheed for Windows
contains several expired CA certs including the now expired
DST Root CA  X3 certificate.
This can cause problems with Let's Encrypt certificates
even though the bundle has the ISRG Root X1 CA cert.
```

Rot8000

> *ROT8000 is the Unicode equivalent of ROT13. What's clever about it is that normal English looks like Chinese, and not like ciphertext (to a typical Westerner, that is).*

-Shneier (https://www.schneier.com/blog/archives/2021/09/rot8000.html)

web app (https://github.com/rottytooth/rot8000/blob/main/readme.md)
commentary (https://pluralistic.net/2021/10/15/fargo-north-decoder#on-trusting-trust)

not as easy to do in shell or Perl/Python as Rot13 !!

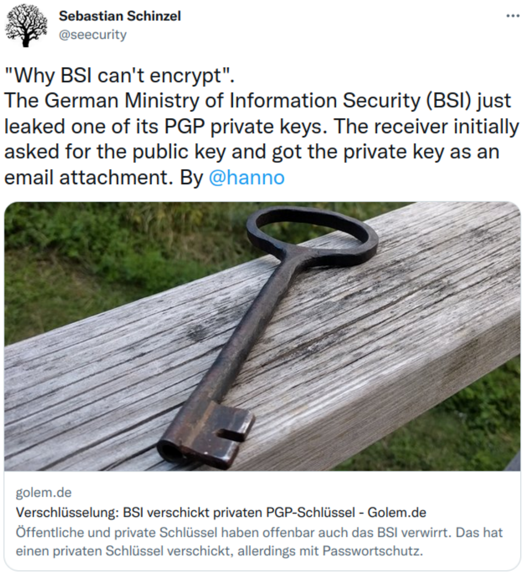
PGP Fit for purpose?

“Why BSI can’t encrypt”.

Sebastian Schinzel @seecurity (https://twitter.com/seecurity/status/1460518804690194432)

> *“Why BSI can’t encrypt”.*
> *The German Ministry of Information Security (BSI) just leaked one of its PGP private keys. The receiver initially asked for the public key and got the private key as an email attachment.*

> *Don’t treat this as a failure of BSI people. They are good people. It’s more like “PGP is so shitty that even the BSI screws it up badly”.*



Sebastian Schinzel
@seecurity

"Why BSI can't encrypt".
The German Ministry of Information Security (BSI) just leaked one of its PGP private keys. The receiver initially asked for the public key and got the private key as an email attachment. By @hanno

golem.de
Verschlüsselung: BSI verschickt privaten PGP-Schlüssel - Golem.de
Öffentliche und private Schlüssel haben offenbar auch das BSI verwirrt. Das hat einen privaten Schlüssel verschickt, allerdings mit Passwortschutz.

c/o

Stephan Neuhaus `@stephanneuhaus1` Nov 16, 2021 (https://twitter.com/stephanneuhaus1/status/1460523731139317766)

> *Cryptography is a machine for turning any problem into a key management problem.*

`deleted` *so anonymous*

> *PGP is a program which turns cryptography into an arsenal full of foot-guns*

Crypto News Feature: Post Quantum Cryptography

What’s Quantum Computing?

The only known photo of Schrodinger's cat.

Quantum Superposition (https://en.wikipedia.org/wiki/Quantum_superposition) when used for computing.

- QC measured in **“qubits”** not bits
- 30% True, 70% False.

Kinds of Quantum Hardware

- Quantum Annealing (https://en.wikipedia.org/wiki/Quantum_annealing) - big qubit counts, great for optimization problems
- Quantum Circuit/Logic (https://en.wikipedia.org/wiki/Quantum_circuit) - small numbers of qubits so far.

We’re discussing PQC before QC?

Yes !

- **Quantum Cryptography** (https://en.wikipedia.org/wiki/Quantum_cryptography)
  - theoretically using entangled quantum states
  - to create an encryption
  - or an anti-eaves-droppable connection
- Quantum Crypt**analysis**
  - Using Quantum Computing to defeat classical PKI encryption
- **Post Quantum Cryptography** (https://en.wikipedia.org/wiki/Post-quantum_cryptography)
  - new classical encryptions that can resist Quantum Cryptanalysis,
  - so read as post-**(**Quantum-Computing**)** Cryptography.

What’s the problem?

- Unbreakable ciphers aren’t always unbreakable, for always.
- QC *could theoretically* break most PKI
  - Schor’s Algorithm / Grover’s / VQF
  - discrete log as well as prime factoring, even elliptic curves

Generalization of Forward Secrecy

- Classical “Forward Secrecy” - old messages not broken by later loss of host key
- Generalized: old saved messages not broken by breakthroughs either.
- Realistic threat?
  - VENONA 1940s (http://blu.org/meetings/2018/09/)
  - NSA Utah Data farm, 2013 (https://en.wikipedia.org/wiki/Utah_Data_Center#Structure)

NIST’s Post-Quantum Cryptography Standards

> *The goal of post-quantum cryptography (also called quantum-resistant cryptography) is to develop cryptographic systems that are secure against both quantum and classical computers, and can interoperate with existing communications protocols and networks. – **NIST***

NIST PQC Competition

National Institute of Standards & Technology started a multi-round competition, similar to with AES and SHA3 competitions

- NIST ann. (https://csrc.nist.gov/projects/post-quantum-cryptography)

- NIST Q&A (https://www.nist.gov/blogs/taking-measure/post-quantum-cryptography-qa-nists-matt-scholl)
- Schneier (https://www.schneier.com/blog/archives/2022/08/nists-post-quantum-cryptography-standards.html)

NIST PQC Selections for 2022

NIST PQC 2022-08-16 (https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022)
July 5th (https://csrc.nist.gov/News/2022/pqc-candidates-to-be-standardized-and-round-4)

- PKE/KEM (PKI key exchanges)
  - CRYSTALS-KYBER (https://en.wikipedia.org/wiki/Kyber)
    "Cryptographic Suite for Algebraic Lattices"
- DSA
  - CRYSTALS-DILITHIUM
    (uses variant of SHA-3)
  - FALCON
  - SPHINCS+
- Round 4 - further research for additional PKE/KEM
  - BIKE
  - Classic McEliece
  - HQC
  - SIKE †

† and weeks later into Round 4, SIKE was broken (https://www.schneier.com/blog/archives/2022/08/sike-broken.html). Badly. 1 core-hour. (https://arstechnica.com/information-technology/2022/08/sike-once-a-post-quantum-encryption-contender-is-koed-in-nist-smackdown/)
*Well, that **was** ^further research^.*

So when can i play?

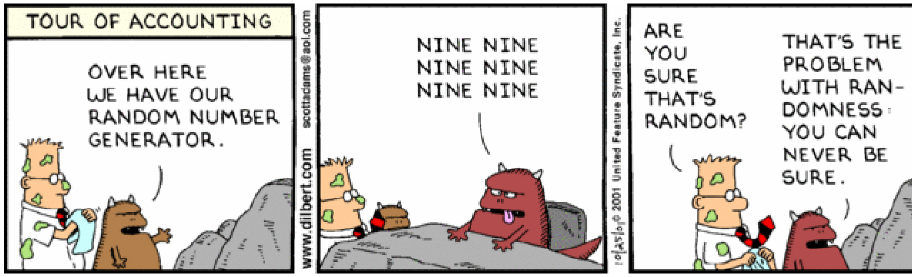
The plan is to roll out these new PQC ciphers as additional cipher options in TLS. *Soon?*

- Experiments have been tried with hybrid PKE/KEM/DSA (layered classical PKI & PQC) with TLS.
- Google is planning roll-out (https://cloud.google.com/blog/products/identity-security/how-google-is-preparing-for-a-post-quantum-world) (*with CloudFlare?*).
- MS has a PQC (https://www.microsoft.com/en-us/research/project/post-quantum-cryptography/) project including PQ TLS (https://www.microsoft.com/en-us/research/project/post-quantum-tls/) which is helping OQS OpenQuantumSafe with a PQC-enabled fork of OpenSSL (https://github.com/open-quantum-safe/openssl/tree/OQS-OpenSSL_1_1_1-stable).
- Digicert is co-backer of several candidates with Google
- Google's BoringSSL (https://en.wikipedia.org/wiki/OpenSSL#BoringSSL) support also
- German Federal OIS targeting Kyber in **Thunderbird**.

NIST PQC Schedule

- 2022 Fourth NIST conference is Nov 29 - Dec 1 (*CFP deadline Oct 1*).
- 202⅔ Draft Standards Available
- 2024 FIPS Standards; `FIPS Allowed`.
- 202⅚ FIPS certification for the PQC algorithms; `FIPS Approved`.

Known weaknesses


TOUR OF ACCOUNTING
OVER HERE WE HAVE OUR RANDOM NUMBER GENERATOR.
scottadams@aol.com
www.dilbert.com
NINE NINE NINE NINE NINE NINE
© 2001 United Feature Syndicate, Inc.
ARE YOU SURE THAT'S RANDOM?
THAT'S THE PROBLEM WITH RANDOMNESS: YOU CAN NEVER BE SURE.

- breaks have eliminated 62 of 69 entrants in Rounds 1 to 4
- including the two front-runners, Rainbow and SIKE
- 7 remain, will they survive?
- FALCON would be compromised by a lack-of-randomness in salt, or failure to salt, as repeating same key and hash again gives too much information.

Isn’t that an unlikely compromise?

No. It’s happened.

- numerous implementations have failed to salt encryption of small data despite warnings.
- DEBIAN broke system random[2] which compromised many SSH keys.
- our historical vignette will discuss danger of key reuse in WW2

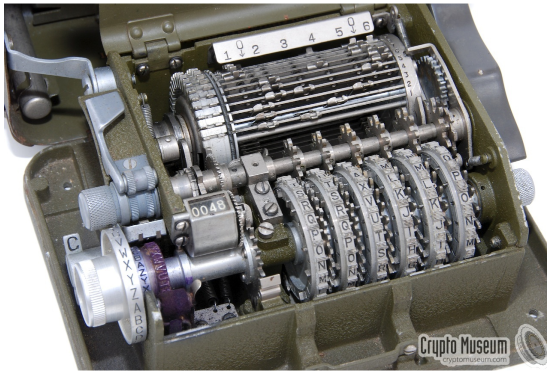
History Vignette - Pin&Lug Hagelin Cryptographs (C-3x/M209)

Bletchley Park Podcast

Bletchley Park Podcast E131: *It Happened Here: Secrets of the Supermarina* (https://audioboom.com/posts/7979946-e131-secrets-of-the-supermarina)[3] (91 min)

> *November 2021*
>
> *Many visitors to Bletchley Park are familiar with the story of breaking Enigma and reading German and even Japanese codes. But equally important work was done on Italian ciphers.*
>
> *Not only were the Code-breakers able to read Italian naval messages, before and during the war, but this information was used to decisive effect in the Battle for North Africa, and the ultimate defeat of Italy in 1943. In this It Happened Here episode, Bletchley Park's Research Historian Dr David Kenyon reveals the secrets of one of Bletchley Park's lesser-known decryption successes.*
>
> *As always, grateful thanks go to Dr Ben Thompson for voicing our archival documents.*
>
> *Featuring the following contributors from our Oral History Archive:*
> *Mavis Batey*
> *Rozanne Colchester*

Swedish Innovation, adopted by several countries



Hagelin M-209-A

- Hagelin was protegé of Nobel
- Using adding-machine mechanical-calculating techniques to combine key-wheels into additive key
    - computes a different Caesar[4] key at each position
    - summing contributions from each rotor's side-pin state, multiplied by # lugs set opposite
    - lugs move bars on a cage to make a temporary variable-toothed gear
    - which will advance the (reversed) cipher alphabet 0-27 places "natural" position for clear letter
    - before printing the enciphered letter.
- 1935 French requested Hagelin to adapt their desktop Enigma-competitor (B-series)
    - to a printing pocketable tactical (named C series)
    - model C-35 & C-36 (1936) had 5 wheels (25 × 23 × 21 × 19 × 17, different orders).
    - Z prints as Space in Plain-text, as Z in Cipher-text.
- C-38 / M-209 / C38m : 6 wheels, added a 26-position wheel (*still mutually co-prime*).
- M-209 / CSP 1500 (USA / USN) C-38 built under license by Smith-Corona
- C38m Italian Navy, K prints as space (instead of Z).

Cracking Italian Navy HQ’s Hagelin C38m pinwheel in WW2

- Legend correction: BP crack of Afrika Korps supply convoys
  - not ENIGMA ULTRA but Hagelin ZTI
  - Italian SuperMarina = Navy HQ
  - ZED like ULTRA but for RN
- HQ instructions for making up of convoys
  - wrong cipher for task
  - poorly used
- Weaknesses
  - Depths
  - Error / inexact re-transmission
  - One very long message allows purely statistical attack
  - (several medium long messages also)

How Broken

1. Manual break of a depth

    - Depths
        - caused by errors
        - subtract two aligned messages
    - Cribs PERK or PERKSUPERMARINK`
        - or codewords seen previously as covernames for ROMMEL, AFRIKACORPS, TUNIS, etc
    - complete-the-word cross-rif between 2 messages
    - which discloses fragments of both messages and their shared key

2. Infer settings from key disclosed in longest depth fragment

    - internal: wheel pin positions and lug multipliers
    - external: start position

3. Read entire message, using Settings and analog hardware
4. Use settings found to simplify break of other messages

Talent

Another Bill Tutte, Tommie Flowers & Dollis-Hill Gang at P.O.R.S. legend that is not yet fully understood!

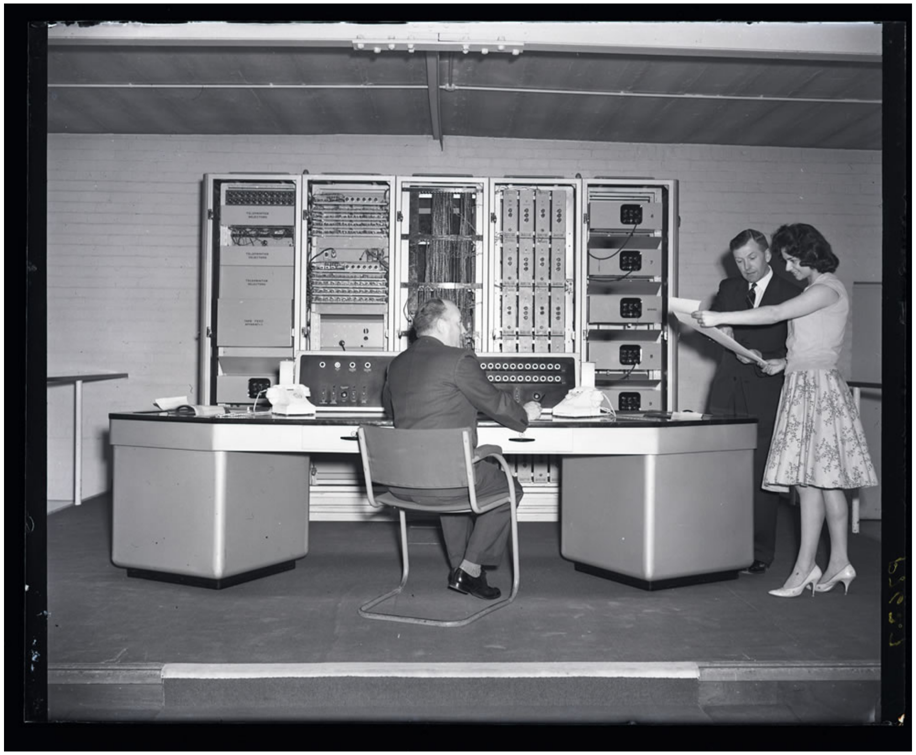
Bill Tutte of BP and the Dorris-Hill Gang for the win, before their latterly-famous “Heath Robinson” and “COLOSSUS” attack on Lorenz.

Tommie Flowers & Sidney Broadhurst of the Post Office Research Station, London (aka Dollis-Hill) were better known in the public for their post-war work on **ERNIE1**, the Post Office’s *Premium Bond Lottery* randomizer; and in the **UNCLASS** Electronics world (IEEE, ITU, etc) for the electronic telephone exchange, 3 years *before* Bell’s comparable 1ESS was installed in NJ.

ERNIE1 ⇒

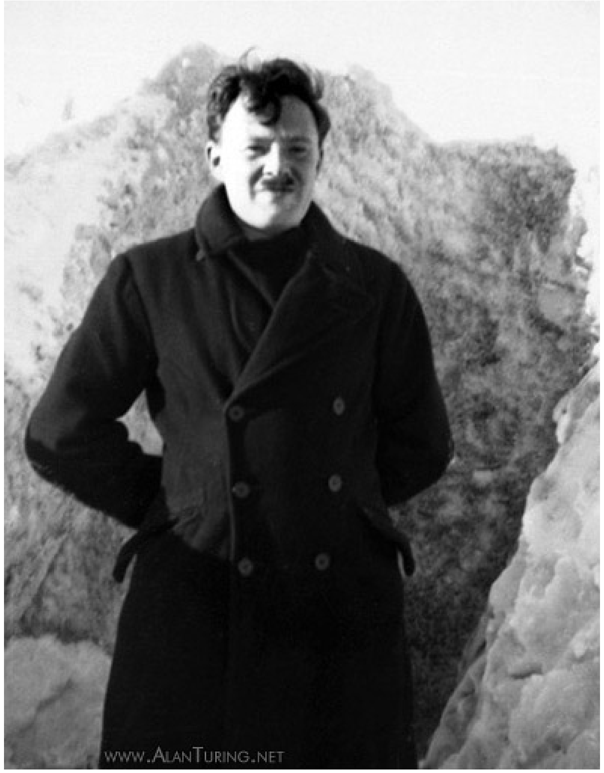
T.Flowers

(*scroll*)



S.W.Broadhurst and **Highgate Wood Electronic Exchange** racks, 1962. ⇒

Wm.T.Tutte (BP Research Section)


www.AlanTuring.net

A NIGHTINGALE in the Post Office

NIGHTINGALE codename for a machine

- Built by Flowers & Broadhurst at PORS Dollis-Hill for BP
- to decipher Hagelin messages with a given key quicker than mechanical
- and to crack monthly internal settings
- known to be used for Italian Naval HQ (Supermarin) Hagelin C38m network
- *may have been used for other Hagelin traffic?*

“It is mostly unknown how it functioned.”

“An operator remembered it was like playing a church organ.” (*implies both a keyboard and a bank of toggle switches?*)

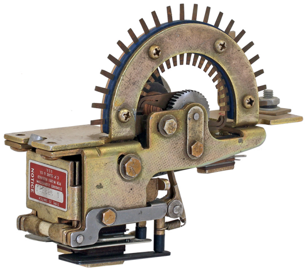
(BP say they *may* have a photo unlabeled, that has repetition of 6 units, which would be one per rotor, so plausible!)

NIGHTINGALE was the ^analog^ or emulator for Hagelin (later CryptoAG) C38/C38m/M109/CSP 1500/AM-1.

Stepper Relays aka Uniselector

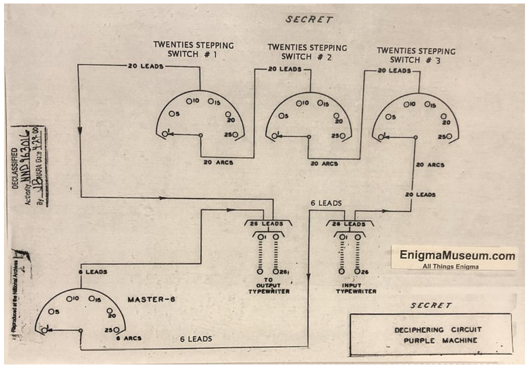
NIGHTINGALE was built with telecoms Stepper Relays aka Uniselectors, Stepper switches, Steppers.

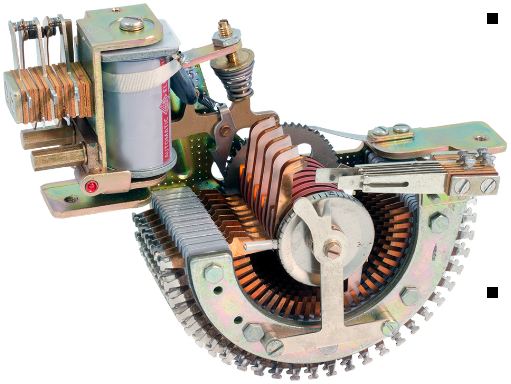
Steppers could be used as inside-out rotors, when rotors were used as **ROM**s.



Uniselector Stepper Switches / Stepper Relays were ubiquitous in pre-electronic electro-mechanical automated telephone exchanges (1927 how-to silent movie (https://archive.org/details/2190_How_to_Use_the_Dial_Phone_00_48_40_00))

- IJ Diplomatic PURPLE (https://en.wikipedia.org/wiki/Type_B_Cipher_Machine) or System 97 Type B cipher machine used Stepper relays in lieu of rotors. They were basically a semi-serial-, semi-parallel-access wired ROM.
- USA SIS officer-mathematician Leo Rosen (https://web.archive.org/web/20210402214927/https://www.nsa.gov/About-Us/Current-Leadership/Article-View/Article/1621587/leo-rosen/) recognized certain regularities in the cipher meant stepper relays instead of physical rotors, so bought American 6p25t steppers to recreate the machine!





- UK PORS Dollis-Hill used Steppers in several “analyzers” for GC&CS (BP) to make faster emulations of Enigma & Sturgeon and presumably used them on the Hagelin NIGHTINGALE also. Might have used 26-throw to emulate 26 position rotors and 26-or-less pin-wheels (different from PURPLE ROM method)?
- Uniselectors were also used in the slower portions of Dollis-Hill/BP Colossus (TUNNY), and in the Lorenz/TUNNY emulator (for reading the rest of a broken message).
- GPO Uniselectors were even used in the Enigma-solving Bombes, in the “machine gun” circuit to test a “stop”’s validity, by running through combinations quickly.

Bibliography & Footnotes

YouTube of this presentation will be linked here (http://blu.org/cgi-bin/calendar/2022-sep)

Prior talks in this series (http://blu.org/cgi-bin/calendar/speakers/b-ricker1) - most talks have slides &/or YouTube attached, sometimes extras. *Alas the YouTube audio pre-pandemic wasn't great, BLU needs a donation of a wireless clip-on mike if we ever return to Hybrid/In-Person meetings. Or we all need to wear a wired or BT headset while presenting in person? if i can get a stealth stage headset that would be better visuals!*

News and **Focus** sections have embedded links.

Good security news streams are https://www.schneier.com/crypto-gram/ (https://www.schneier.com/crypto-gram/) and https://isc.sans.edu/ (https://isc.sans.edu/), the latter being less cryptologic focus.

History section general references

- ***Bletchley Park Podcast*** E131: *It Happened Here: Secrets of the Supermarina* (https://audioboom.com/posts/7979946-e131-secrets-of-the-supermarina)[11] (91 min)
- **Books**
  - *The Code Breakers*, revised & updated; Kahn, David; 1996: NY S&S. Pp. 422-455, Corp history, M-209 operations.
  - *Decrypted Secrets*; Bauer, F.L.; 1997: Heidelberg, Springer. p 129 ■8.5.1, pic p.130, plates G&H, earlier designs p.157; history&usage p.75-76, 106, 116, 119, 169, 192, 197. p.204, 1957 rumors related to MINERVA RUBICON. P.342, quotation. p.191-192 pure decryption of M-209.
  - *Colossus: The secrets of Bletchley Park's code-breaking computers Colossus: The secrets of Bletchley Park's code-breaking computers*; B. Jack Copeland et al; 2010: OUP. ISBN 0-19-284055-X (HC), ISBN 0-19-957814-X (https://isbun.nu/0-19-957814-X) (PB). *homepage* (http://www.colossus-computer.com/)
    - this is mostly on TUNNY but has a chapter on Hagelin.
  - *Codes and Ciphers*; Churchhouse, Robert; 2002: Cambridge: CUP.

        - general coverage, Caesar to Elliptic Curves
        - Ch.10 is Hagelin cryptanalysis. Discusses recovering cage lugs and wheel pins from key-stream.
        - Supplemental Maths segregated in short appendices.
    - *Cryptanalysis Of The Hagelin Cryptograph*; Barker, Wayne G.; 1977: Aegean Park Press. archive (https://archive.org/details/hagelin/page/n2/mode/1up)
        - The most complete worked examples in open literature.

- **Websites**
    - https://cipherhistory.com/pinandlug.html (https://cipherhistory.com/pinandlug.html)
    - https://cryptomuseum.com/crypto/hagelin/index.htm (https://cryptomuseum.com/crypto/hagelin/index.htm)

- Declassified **TICOM** reports
    - http://www.jfbouch.fr/crypto/m209/ticom.html (http://www.jfbouch.fr/crypto/m209/ticom.html) summary of M-209 related TICOM
      aka C-38 or “AM 1”=American Small Machine.
        - Most of the key reports are in https://archive.org/details/ticom/ (https://archive.org/details/ticom/) bundle;
        - see also http://www.ticomarchive.com/ (http://www.ticomarchive.com/) .
        - ✓ TICOM Enemy Successes (https://archive.org/details/ticom/EnemySuccesses/mode/1up)
        - ✓ TICOM v1 Synopsis (https://archive.org/details/ticom/EuropeanAxisSignalIntelligenceVol.1Synopsis) - M-209 read 10-20% of intercepts
        - ✓ TICOM v4 High Command (https://archive.org/details/ticom/EuropeanAxisSignalIntelligenceVol.4SignalIntelligenceServiceOfTheArmyHighCommand/mode/1up)
        - ✓ TICOM I-175 (https://archive.org/details/ticom/TicomI-175) “Report by Alfred Pokorn of OKH/Chi on M.209.”
        - ✓ TICOM DF-105 (https://archive.org/details/ticom/TicomDf-105) DETERMINATION OF THE ABSOLUTE SETTING OF THE AM-1 (M 209) BY USING TWO MESSAGES WITH DIFFERENT INDICATORS. Trans, from T 2795 by AS-14 (EC) 10 pp
        - ✓ TICOM DF-114 (https://archive.org/details/ticom/Df-114CryptanalyticDeviceForSolutionOfM-209Traffic) GERMAN CRYPTANALYTIC DEVICE FOR SOLUTION OF M-209 TRAFFIC. Trans from T 2785.
        - ✓ TICOM DF-120 (https://archive.org/details/ticom/Df-120m-209) REPORT ON THE SOLUTION OF MESSAGES IN DEPTH OF THE AMERICAN CIPHER DEVICE M-209, Trans from T 2794 by AS-14 (EC) 17 ppo wfrth 11 plates

- ? TICOM DF-137 MATHEMATICAL AND MACHINE METHODS IN CRYPTOLOGY (trans from IF-380)
    - NSA released to NARA April 2011 (https://media.defense.gov/2021/Jul/15/2002769644/-1/-1/1/NARA_RELEASE_LISTING_MAY2011.PDF), NARA accession # 6332, RG not known, not seen on NSarchive etc yet?

1. See our prior discussions (http://blu.org/meetings/2018/09/) of GEE, VENONA for breaks of One Time Pad↩
2. `DSA-1571-1 openssl` predictable random number generator (https://www.debian.org/security/2008/dsa-1571) (CVE-2008-0166) (https://security-tracker.debian.org/tracker/CVE-2008-0166) (Schneier (https://www.schneier.com/blog/archives/2008/05/random_number_b.html))↩
3. *Supermarina* = Navy HQ; ^Super^ as in Superior, Above, Supervisory over the Navy.↩
4. Not actually Caesar; Self-reciprocal Beaufort (https://en.wikipedia.org/wiki/Beaufort_cipher), C=K-P & P=K-C, reversed standard alphabet↩
5. Regia Marina Italiana 1940-1943 (http://www.regiamarina.net/detail_text.asp?nid=296&lid=1) Naval situation and impact.↩
6. CryptoMuseum M-209/C-38 page (https://cryptomuseum.com/crypto/hagelin/m209/index.htm)↩
7. More information on Indicators as used by Allies and Italian Navy: Hagelin serie C: Indicators (http://www.jfbouch.fr/crypto/m209/indicator.html) (*these m209 pages cover all C-38 users and variants including M209 and C38m, looking at national Indicator Systems, including C38m Supermarina.*)↩
8. See our prior discussion of CryptoAG RUBICON/MINERVA in 2020 (http://blu.org/meetings/2020/09/) (and minor mention 2021 (http://blu.org/meetings/2021/09/))↩
9. Bauer, *op.cit.*, p.191-192↩

10. TICOM (Target Intelligence Committee) was like PAPERCLIP (collecting science/weapons papers and scientists) but for Intelligence/crypto/maths. (wikipedia (https://en.wikipedia.org/wiki/TICOM), declass archive (http://www.ticomarchive.com/the-targets/okw-chi/related-reports), archived I-45 inter alia (https://archive.org/details/ticom/I-45OkwchiCryptanalyticResearchOnEnigmaHagelinAndCipherTeleprinterMachines/page/4/mode/1up))↩

11. See above footnote on SuperMarina.↩