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".

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?

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

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

> Such bits are in quantum superposition of True and False, which is a *bug* in classical computing but a *feature* in QC.

> This allows non-deterministic algorithms (https://en.wikipedia.org/wiki/Nondeterministic_algorithm).

Kinds of Quantum Hardware

- Quantum Annealing (https://en.wikipedia.org/wiki/Quantum_annealing) - big qubit counts, great for optimization problems

  but not cryptology. (?yet?) *Not general purpose.*

- Quantum Circuit/Logic (https://en.wikipedia.org/wiki/Quantum_circuit) - small numbers of qubits so far.

> In theory, algorithms for these hardware types can use non-deterministic parallelism to evade classical performance limits, and in particular, could allow factoring fast enough to be dangerous, provided big enough quantum circuits can be made to work.

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

> (***Chinese Space Agency claimed to have demonstrated?***)

- 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

---

Every unbreakable cipher has been broken eventually (at least partially[1]).

20thC RSA and other PKI not guaranteed proof against either of:

- major breakthrough in number theory (factoring &/or discrete log), or
- quantum hardware + algorithms (practical fast factoring)

Schor’s Algorithm (https://quantum-computing.ibm.com/composer/docs/iqx/guide/shors-algorithm) in theory would factor fast on enough quantum circuits but 21 is not a large number yet. (see also Wikipedia (https://en.wikipedia.org/wiki/Shor%27s_algorithm).)

Other probabilistic quantum algorithms (Grover (https://en.wikipedia.org/wiki/Grover%27s_algorithm), GEECM (https://en.wikipedia.org/wiki/Lenstra_elliptic-curve_factorization#Quantum_version_(GEECM)), Variational Quantum Factoring (VQF) (https://arxiv.org/abs/2012.07825)) can do *some* much bigger numbers (*which may just define new class of unsafe primes??*), and with classical pre-processing, can use a much smaller number of qubits than the ^*obvious*^ $\log_2 N$.

not clear this will ever be able to generally break RSA4096, but it's not impossible, so prudent to plan for that day.

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)

```
* VENONA: It worked Once!
* We now have a Vacuum Cleaner of Holding (_Greenpeace photo c/o Wikimedia_)
```

So yes, it can happen again.

Normal Forward Secrecy requires that if e.g. the Host Key is compromised later, any retained cryptograms sent with nonce keys negotiated with the compromised Host Key aren't also compromised.

This is nice, but we'd also like to protect against advances of technology, e.g. fast factoring or solutions of discrete logs.

This may not be within *your* threat model, yet, but in dystopian plausible futures, things you've already discussed/downloaded might be retroactively illegal/disloyal and oops.

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**

… and have it ready for use not only before quantum breakthrough but early enough (roughly now) that anyone who wishes to avoid save-intercepts-now-to-break later; although it may already be too late WRTO NSA archive?

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, the Bureaucracy formerly known as NBS.

This competition was "more brutal" than prior; of 69 candidates, peer cryptanalysis has broken 62. So far.

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

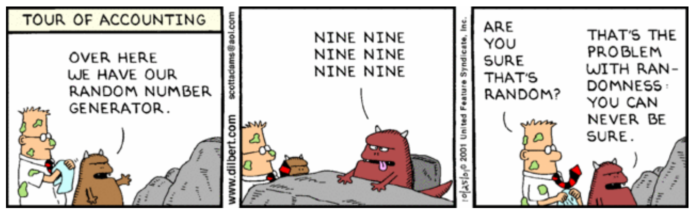
fork of OpenSSL (https://github.com/open-quantum-safe/openssl/tree/OQS-OpenSSL_1_1_1-stable).
- Digicert is co-backer of several candidates with Google
- Google's BoringSSL (https://en.wikipedia.org/wiki/OpenSSL#BoringSSL) support also
- German Federal OIS targeting Kyber in **Thunderbird**.

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

- 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

Lack of randomness failure isn't just hypothetical, lots of SSH keys got invalidated in 2008 because they were well-known-primes.

(WTF? Yep. Debian packagers applying *normal best practices* where they shouldn't even touch had *removed* the entropy-harvesting because Valgrind and Purify gave "accessing uninitialized memory" warnings. Well yeah, that's how we harvest entropy! Another problem (mostly solved?) is host key generation at VM start - the VM's entropy is rather deterministic at that point. Similarly, optimizing compilers removing zeroing memory prior to releasing it can allow keys to leak into the memory pool. Cryptographic software is an ongoing a battle against computer ^science^ that ^knows better^.)

And failure to salt wouldn't surprise me when non-specialists (applications developers, database programmers, protocol developers) who should stick to packaged PKI use-case libraries (e.g. NaCl (https://en.wikipedia.org/wiki/NaCl_(software))) try to use cryptographic primitive routines directly to avoid dependencies.)

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

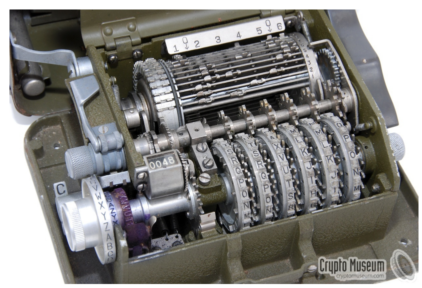
Bletchley Park Podcast

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).

Hagelin was put into an existing firm by investor Nobel, and worked synergistically with prior designer.

- Effectively choosing Caesar (or rather, Self-reciprocal Beaufort (https://en.wikipedia.org/wiki/Beaufort_cipher)) encryptions +0..27 for each letter enciphered
- via 2^{64} combinations of 6 wheel-kicks (mostly straight addition but minus overlaps!)
- chosen by a key of long period from a (hopefully) unknown starting position.
- wheel-kicks assigned by cage lug settings, triggered by wheel pin settings

- large number of internal settings for technician to get right monthly or more often, 27*2 lugs in 2 of 8 positions on each cage bar, and 131 pins in 1 of 2 positions each (sum of wheel sizes).

```
  perl --MList::Util=reduce -MNumber::Format=:subs -E '
    $n = reduce {$a+$b} (26 , 25 , 23 , 21 , 19 , 17);
    say format_number($n);'
131
  perl -MList::Util=reduce -MNumber::Format=:subs -E '
    $n = reduce {$a*$b} (26 , 25 , 23 , 21 , 19 , 17);
    say format_number($n);'
101,405,850
```

Besides mechanically implementing **addition** and **multiplication** with the rotor-cage lugs and variable gear, the pin-wheel actuators interacting with the lugs through the actuator bar were effectively mechanical **AND** gates; and if the two lugs on an **overlapped** cage bar were both operative, they were a mechanical **OR** gate.

Post-war Hagelin/CryptoAG pin-wheel models had further refinements (before going digital) -

- a so-called “slide” mechanism to offset the Beaufort ciphertext alphabet from standard position, which slide amount must be included in the indicator somehow;
- the ciphertext alphabet was mixed, not merely reversed. (*IDK if those retained reciprocal nature or if they had to have a Encipher/Decipher lever?*)

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)

Convoy instructions
- should never have been on radio! *Did they not have teleprinters from HQ to harbor HQs like a modern military??* - should have been in Enigma or stronger, not Hagelin

BP’s cracking of Italian Navy ENIGMA is well known wrto Afrika Korps supply-chain, but the Navy HQ Hagelin network was also vulnerable and exploited.[5] Contrary to ENIGMA-ULTRA legend, this and not other ULTRA sources (e.g. ENIGMA) was the one tracking the Italian convoys to NAF - SuperMarina instructions to ports for which ships were to go in what convoys! (Royal Naval traffic mostly sent as “ZED” not Ultra; ZTG or ZTI: Zed traffic, Teleprinted, German/Italian. So this would be ZTI, ULTRA equivalent but Naval.) *Some books get this right, others didn’t.*

The Hagelin C-38[6] is the pin-wheel additive system whose CX-52 successor and digital successor H-460 we discussed in the last two (http://blu.org/cgi-bin/calendar/2020-sep) years (http://blu.org/cgi-bin/calendar/2021-sep) as CryptoAG RUBICON scandal.

The **C38m** is the Italian Marina=Navy variant with spacing K instead of Z.

USA/USN and France used C-38/M-209/CSP-1500 for *tactical* messages. USA expected crackable in 4 hours.

Italian Navy HQ used it for messages whose value lasted longer and were thus exploitable and worth cracking. They may not have thought of it as *strategic* but it was longer than truly *tactical*.

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

A mix of techniques was used

One very or several merely long messages could be attacked statistically to determine internal settings: first cage lugs, and then pins. Italians wisely limited message size. But strategic use meant long message split into several max-sized parts, sent with same internal settings, so still possible.

Simplest crib, messages starts with equivalent of `to: (harborname) HQ` or, since Italian has no use for the letter *k*, **`K`** instead of `Z` is hardwired for plain-text space on C38m, so `PERK`. For messages replying to Naval HQ, crib is `PERKSUPERMARINAK`, a nice long crib!

(Unlike Enigma, a letter can represent itself, so cribs not draggable on a single message, only on depths.)

The Italian Navy indicator system if properly used *would* have been secure.[7]

French original commission for Hagelin C series was for tactical use, low level on battlefield, short-lived message value, so depths somewhat irrelevant. Italians used it for strategic high command - higher value messages with longer-lasting value, worth depth-cracking; anti-reuse instructions in theory should have been adequate, had they been practical. US used C-38 aka M-209 in tactical use; they saw how much work Brits took to break it in Italian Navy even with poor praxis, and figured it was good enough.

(This touches on previously discussed CryptoAG / CIA-BND RUBICON/MINERVA ^*scandal*^.[8])

Inference: the *regular* fixed spacing of initial positions - intended to prevent partial depths, since messages were limited to length equal to spacing - reduced the number of possible start positions that needed to be tried to read messages sent with same internal settings as had been found from a depth. This is roughly is reducing entropy of start position from 6 wheels to 4 wheels. Search with fast analogs might be practical, while still too slow if done manually, so thought safe by those without Dollis-Hill?

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 ⇒

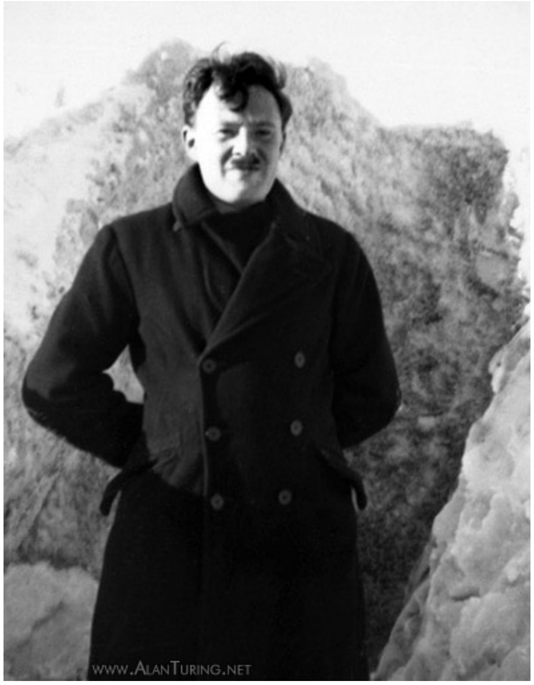
T.Flowers

(*scroll*)

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

Wm.T.Tutte *(BP Research Section)*

William "Bill" Tutte, who was their chief collaborator in GC&CS Bletchley Park, is now recognized as one of the great minds of Bletchley Park, in the Research Section, the solvers of unsolved problems. He was the first at and master of breaking Hagelin C38m messages in depths of 2, via the cross-riff method, which was necessary to find a stretch of key from which to deduce both the starting position and the internal key of the day.



Within Cryptology circles, they are remembered for **Heath Robinson** and **COLOSSUS** that *solved* TUNNY (Lorenz SZ40,SZ42) using valve (tube) electronics for higher operating speed. Before that, they developed relay-logic & stepper analogs for Enigma, STURGEON (Siemens T52), TUNNY, and Hagelin C-38 machines, that would at a minimum decipher a message whose key was known.

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.

It reportedly had some cryptanalytic features beyond merely being a faster analog, which is partly substantiated by it’s still classified some 75-80 years later.

(*US reports on decrypting Hagelin machines are mostly still classified also. Possibly because of RUBICON exploitation of follow-on systems until very recently? Or perhaps (!swag!) possibly too similar to techniques that worked on Linear-feedback 1970s-1990s key generators?*)

Extra cryptanalytic support functions may have included crib-dragging or statistics collection.

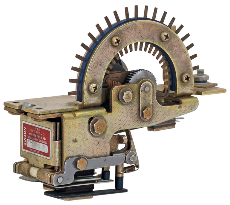
Hypothesis: Given one valid starting position from the current set of (indicator → starting position) on Net’s monthly codesheet, search through starting positions offset by n×500 from there for trial decrypt, checking for statistics suggesting natural language instead of gibberish? Is NIGHTINGALE even enough faster than manual C-38 that it could do on average 100k (=N/500) starting positions multiplied by *enough steps to get statistics? That's not near USA's 4 hours unless steppers are faster than i think! Maybe they were wired to detect a very short crib e.g. "PERK" in first 4 positions?*

Bauer states "Messages of 1000 characters are in any case at risk, since automatically decryption techniques for the M-209, for example, work well with messages of about 800 characters or more (pure cryptanalysis ...)" and that thus US had max length 500 allowed [9]

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.



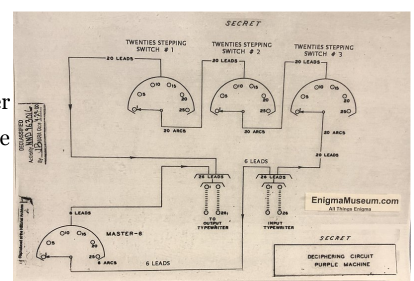
Enigma's custom-wired rotors were effectively dynamic **ROM**s, mechanically rotated like an odometer to scramble the contents and effectively multiply the size of the ROM.

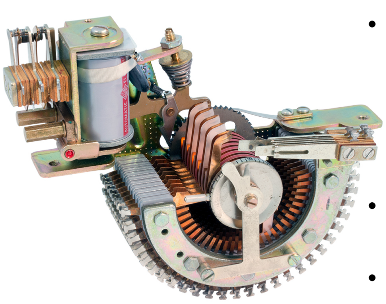
Eventually someone at pretty much each great-power cryptology bureau figured out that telephony Uniselectors could be wired on the *outside* (instead of rotors wired on the inside), more simply, and operate faster and more reliably. (Although that makes *swapping* wiring harder.)

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))

(and are why the old dial phones *dialed*, generating a pulse-train to step an activated stepper N steps).

- 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.

As noted previously, how NIGHTINGALE was built has not been declassified. Yet. We *infer* that it used Uniselectors as the other machines of its class and origin did. We are told it had some cryptanalytic functions beyond fast emulation, but know not whether related to breaking or setting.

(From TICOM[10], we know that the Germans were capable of breaking US C-38 traffic as well. It was thought that they should be able to break in 4 hours, so US relegated it to tactical use. In reality, German exploitation was much slower and only when keys captured or messages were sent "in depth", in error. They had some custom breaking machinery but mostly used IBM Hollerith punch-card electric accounting machines (https://en.wikipedia.org/wiki/Unit_record_equipment) / tabulating machines (https://en.wikipedia.org/wiki/Tabulating_machine), which were also used at USN Station HYPO (https://en.wikipedia.org/wiki/Station_HYPO) and USA/NSA VENONA. General purpose, reprogramable, but not as fast as BP's special-purpose analyzers. German statements in TICOM suggest their fast-analog of M-209 (equivalent to NIGHTINGALE) would be useful for *detecting* depths also, and they had a device that could solve settings given 5 messages in depth with cribs (stylized beginning etc)DF 114, TICOM # 2785 (https://archive.org/details/ticom/Df-114CryptanalyticDeviceForSolutionOfM-209Traffic/mode/1up); USA had a separate machine for finding coincidences, the Index of Coincidence (https://en.wikipedia.org/wiki/Index_of_coincidence) (IC) machine.)

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/1
    - ✓ 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.↩