Boston Linux/Unix

Annual Cryptology Talk

September 16, 2020

Bill Ricker

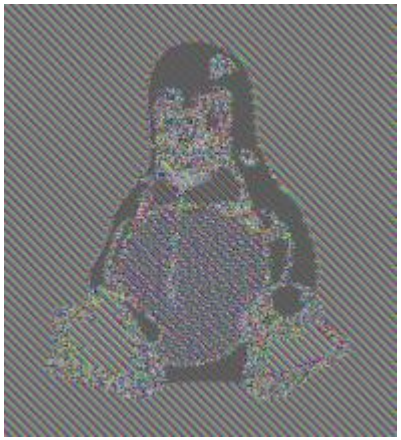
(*Annual Web of Trust signing deferred*
...due to you-know-what...
and maybe forever ...)

Agenda

- 2020 Cryptology News in Review
  - Cracks, CVE, Factoring, PGP?, PQC?
- New Insights in Transitional Cryptology
  - From recent declassifications
  - Case study of a Shift Register crypto
  - Time-line of rise and fall of a crypto empire
    - Interleaved ...

2020 News - Cracks

- Sept 2020 – Racoon Attack – practical timing oracle, extracts sequential bits of a static DH key. (Real but already was being retired.)
- Zoom Meeting claimed “E2E”
  - !wrong! *server was assigning session keys.*
  - *Also many privacy problems.*
  - *Use of AES-128 in ECB mode dubious*
    - *How much safer with video, audio ?*

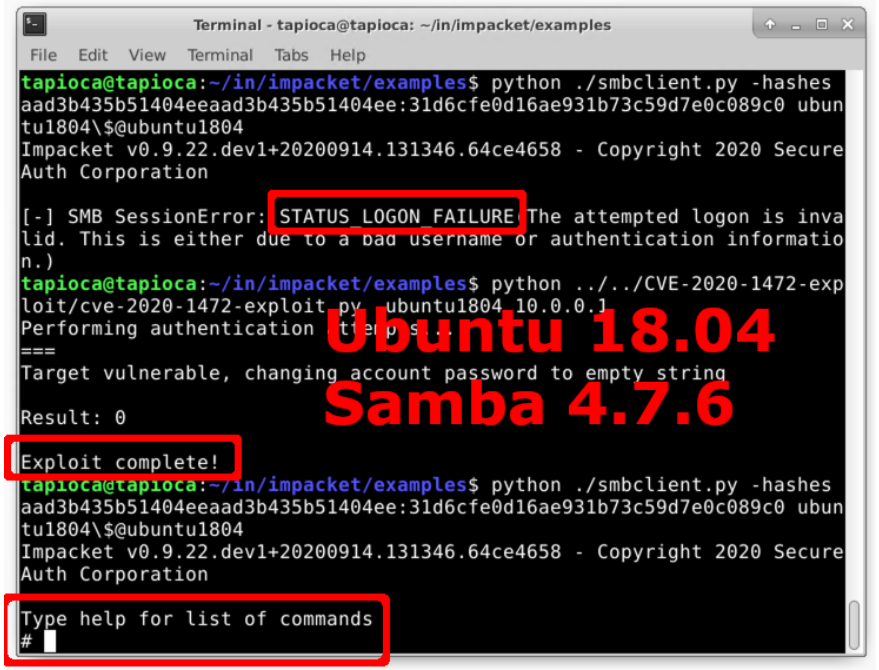


We interrupt this netcast

This Just In To the Newsroom …

- CVE-2020-1472 MS August NetLogon
  - Blank password works! ?? WTF ??
  - MS Patch scheduled for Feb 2021, *so ugh.*
  - Initially marked as "*not our problem*" by Linux.
- 9/15: Affects Linux too.
  Now.
  SAMBA/CIFS is vulnerable because bug-for-bug compatible.
  [LWN 9/15]
- @wdormann [Twitter]

  Interestingly, Samba appears to be affected by this vulnerability as well!
  The exploit works as-is against my Samba **4.7.6** instance.
  With **4.11.6**, it tests as vulnerable but the public password-blanking exploit doesn't appear to work as-is.
  12:36 PM · Sep 15, 2020



....Oopsie

Steven Bellovin @SteveBellovin · 7h
Oh, look—a flaw in the spec. It's not just the code…

> **Will Dormann** @wdormann · 9h
> Replying to @wvuuuuuuuuuuuu
> Well, the Microsoft specification mandates that a zero IV is used. So I suppose that I'm not terribly surprised at this.
> docs.microsoft.com/en-us/openspec…
>
> **3.1.4.4.1 AES Credential**
>
> If AES support is negotiated between the client and the serv using the AES-128 encryption algorithm in 8-bit CFB mode v
>
> ```
> ComputeNetlogonCredential(Input, Sk,
>                 Output)
>
>         SET IV = 0
>         CALL AesEncrypt(Input, Sk, IV, Output)
> ```
>
> AesEncrypt is the AES-128 encryption algorithm in 8-bit CFB [FIPS197].

2 3 10

Anthony de Boer @devbeard · 7h
There's an even older specification that says that IV = 4.

1 2

william ricker @n1vux · 5h
4 has more entropy than 0 but ...

1

Anthony de Boer
@devbeard

Replying to @n1vux and @SteveBellovin

The spec that IV is the number between III and V is many centuries older than

Random Number
xkcd.com

10:07 PM · Sep 15, 2020 · Twitter for iPhone

1 Like

ARCHIVE
WHAT IF?
BLAG
HOW TO
STORE
ABOUT
FEED · EMAIL
TW · FB · IG

xkcd

A WEBCOMIC OF ROMANCE, SARCASM, MATH, AND LANGUAGE.

RANDOM NUMBER

|< < PREV RANDOM NEXT > >|

```
int getRandomNumber()
{
    return 4;  // chosen by fair dice roll.
               // guaranteed to be random.
}
```

|< < PREV RANDOM NEXT > >|

PERMANENT LINK TO THIS COMIC: HTTPS://XKCD.COM/221/
IMAGE URL (FOR HOTLINKING/EMBEDDING): HTTPS://IMGS.XKCD.COM/COMICS/RANDOM_NUMBER.PNG

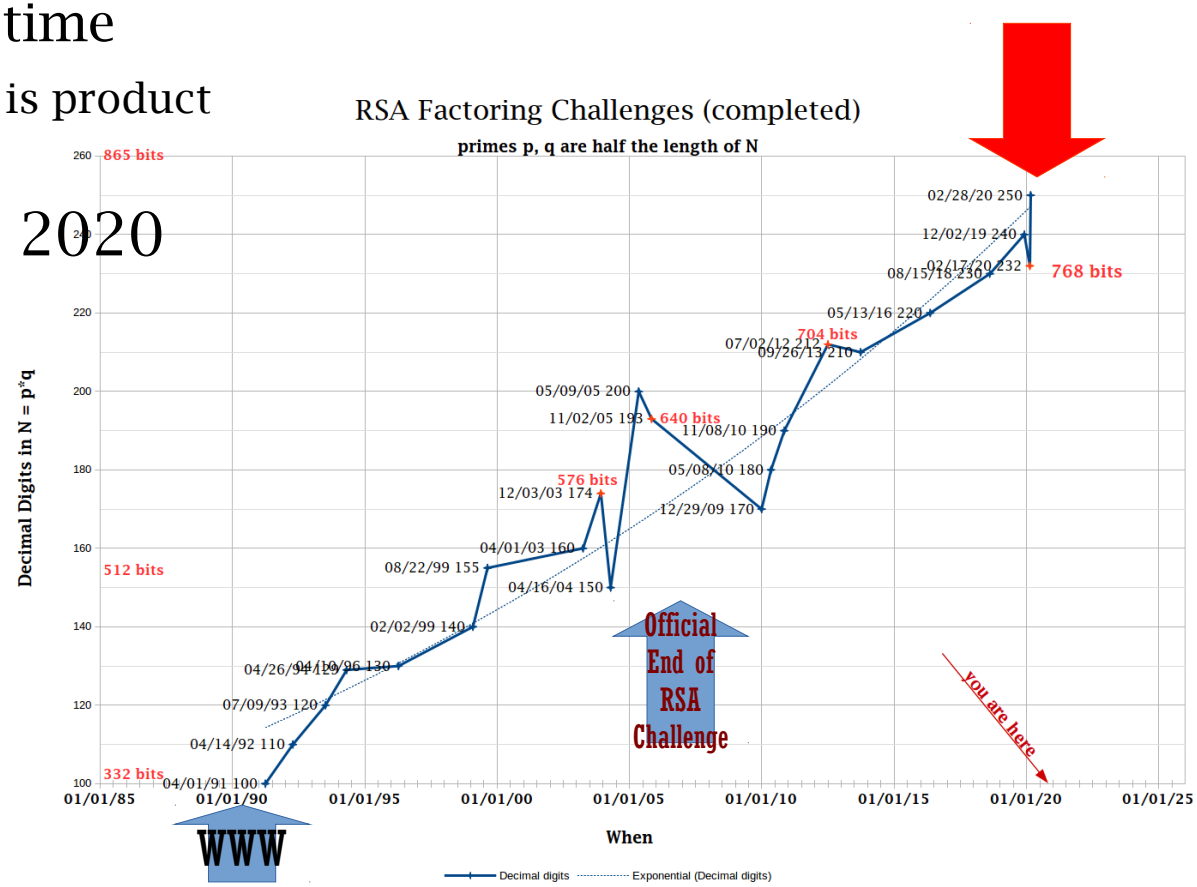
https://www.explainxkcd.com/wiki/index.php/221:_Random_Number

https://en.wikipedia.org/wiki/Initialization_vector

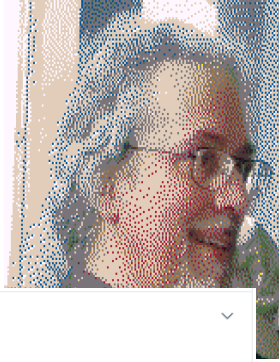
We now return you to our regular programming.

2020 News - Factoring

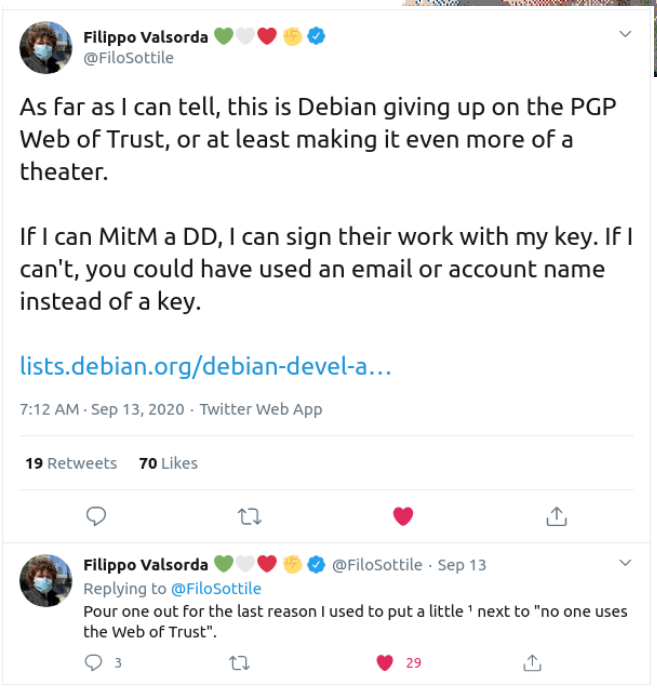
- RSA-250 factored
  - Feb 2020
  - 2,700 core-years, clusters
  - “a few months” calendar time
  - 829 bit = 250 digit composite N is product of two 125 digit primes p,q
- RSA-232 (768b) also Feb 2020
- RSA-240 Dec. 2019
  - Same team/plan.
- RSA-230 Aug 2018
- All using free software!

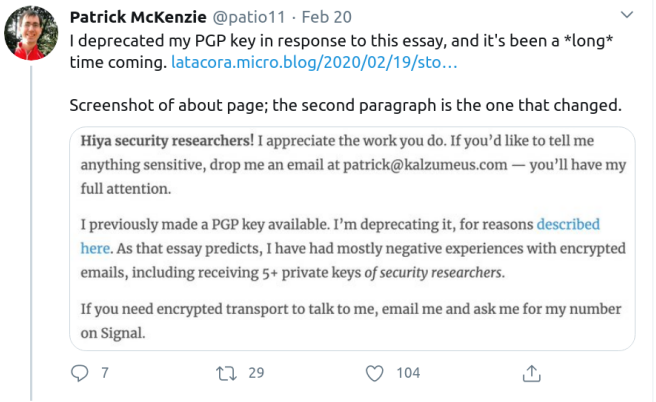


PGP? Maybe not ...



- DD has alternate trust root now
  - "DAM Key and identity requirements" 9/13
- Latacora
  - "Stop Using Encrypted Email" 2020
  - "The PGP Problem" 2019
- List of Alternatives in my 2019 BLU talk notes
  odp :: flipbook :: pdf





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**" (????) 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 …

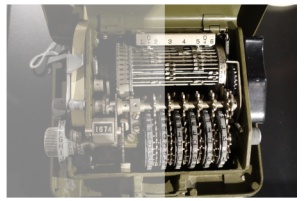
Eras of Cryptology?

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**" (????) 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
  - 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 rotors for 5-bit TTY current loop pulses; first on-line teleprinter !
- 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.

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.

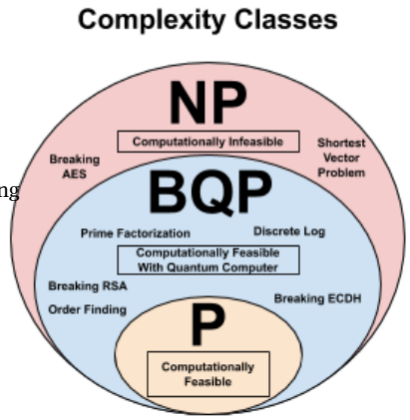
NIST's Post-Quantum Cryptography competition continues

- July, 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**

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



Transitional Cryptology

- *New Insights in Transitional Cryptology*
  - From “recent” declassifications
    - And recent on-going news
  - Case study of a Shift-Register crypto
  - Time-line of rise and fall of a crypto empire
    - Interleaved ...

THESAURUS/RUBICON MINERVA

- The intelligence coup of the century
  - Greg Miller &al Feb. 11, 2020 WAPO Working with Crypto Museum (NED).
  - "For decades, the CIA read the encrypted communications of allies and adversaries."

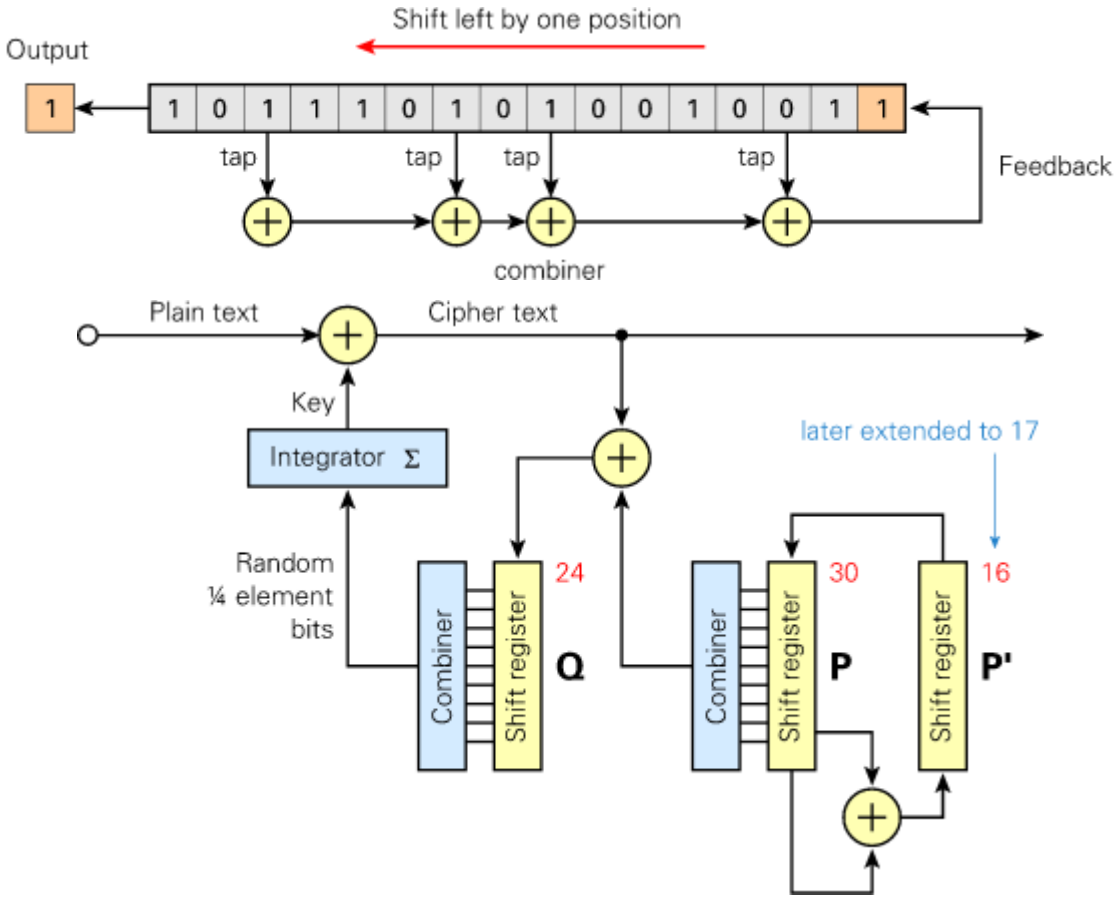
"*What's new is the scale. This wasn't a few targeted customers. It was basically everything. Crypto AG was the retail branch of NSA.*"-Matt Blaze

- WFF=William F Friedman
  BH=Boris Hagelin
- WFF&BH contacts 1937,..1950.
  First proposed deal ('50-51)
  declined by US Govt committees.
- 1951 Cosmos Club meeting
  - BH (CAG), WFF (ASA/AFSA)
  - '51 beginning Gentlemen's agreement, reviewed '53 '55
  - '53 ROFR for retirement sale
- 1952 CAG begins CX-52 pin&lug design
  - successor to C-52, M-209, etc
  - *Mechanical Adding machine analog*
- 1957 WFF-Boris meeting
  - handshake deal w/ WFF of NSA
  - Rotor secrets shared,
  - CX-52
    - Unbreakable if set up properly
    - Customer Instructions customized
      - for short cycles
    - CX-52M upgrade offered with long cycle,
      - but predictable by NSA
- 1960 "Licensing Agreement"
  - tiers of products for tiers of nations
  - retainer; CIA contact
  - Formal contract

THESAURUS/SPARTAN

1960s

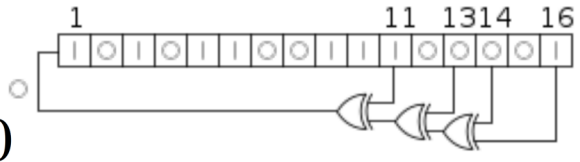
- Mechanical CX-52M
  - NSA contributes readable rotor sequence with long period
  - Appears improved but
- Shift Registers
  - LFSR
  - NLFSR
  - PseudoRandom number stream

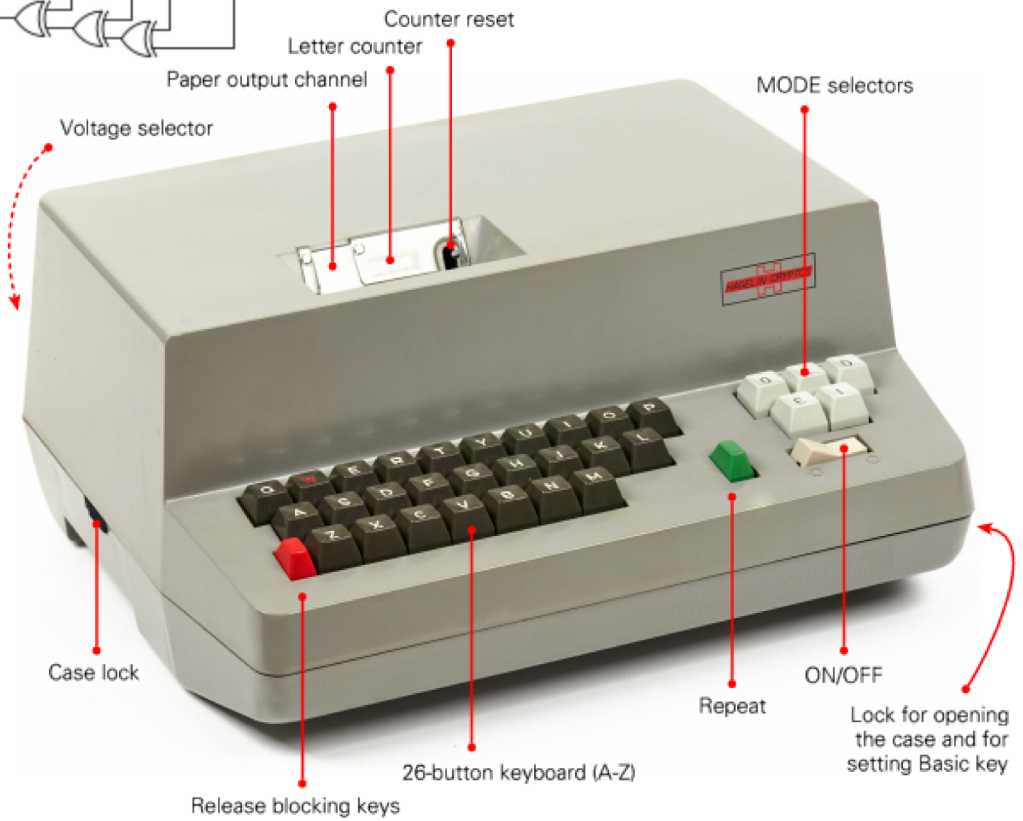


Images from CryptoMuseum.com

Hagelin/C.a.g H-460
a **Transitional** design

- 1965 design
- CMOS MSI 7400/4000
- NSA cryptologic
  - Presumed shift-register
- 1970 shipped, buggy
- 1972 re-shipped
- 1976 IT,EG complain
- 1977 reissued as H-460x
  - 5=Italy
  - Stronger but still backdoored
  - https://www.cryptomuseum.com/crypto/hagelin/h460





MODE selectors

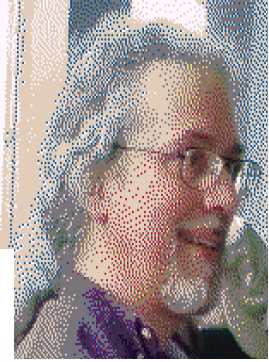
- **O** Plaintext
- **C** Cipher (encrypt)
- **D** Decipher (decrypt)
- **I** Internal key input (basic key) — 25 letters.
- **E** External key input (message key) — 5 letters

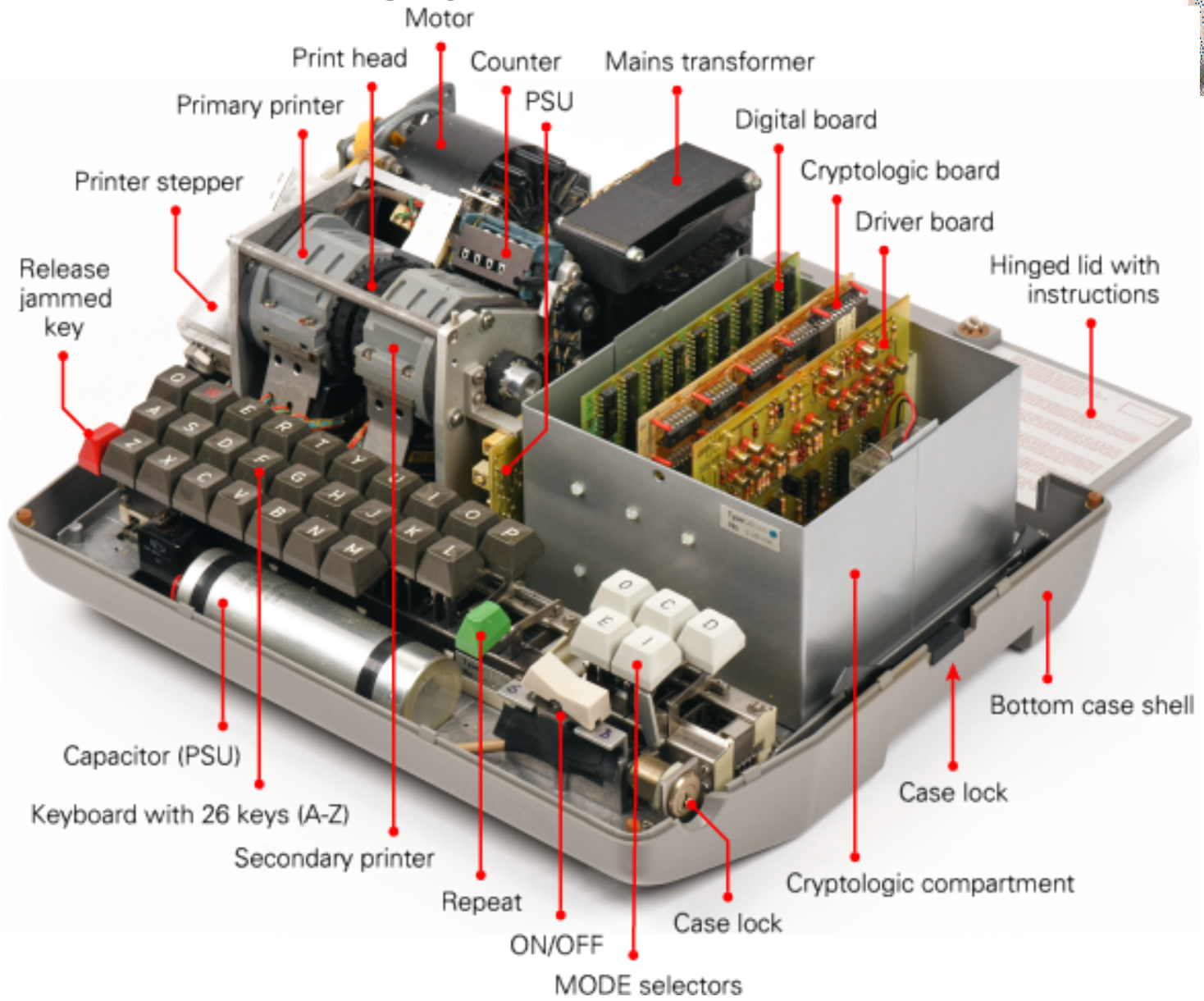
image from CryptoMuseum.com

H-460 Tour

https://www.cryptomuseum.com/crypto/hagelin/h460

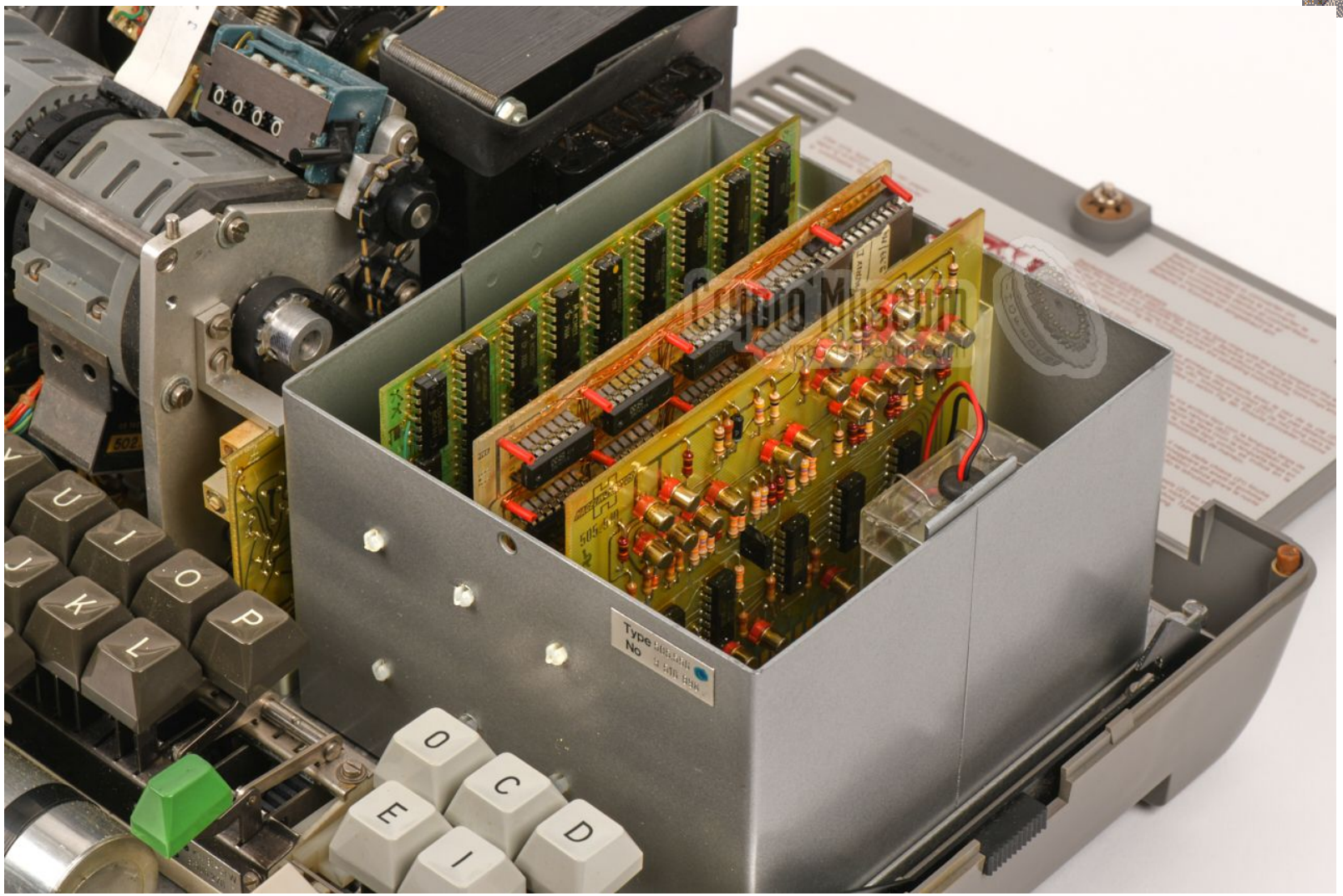
H-460 Tour





https://www.cryptomuseum.com/crypto/hagelin/h460

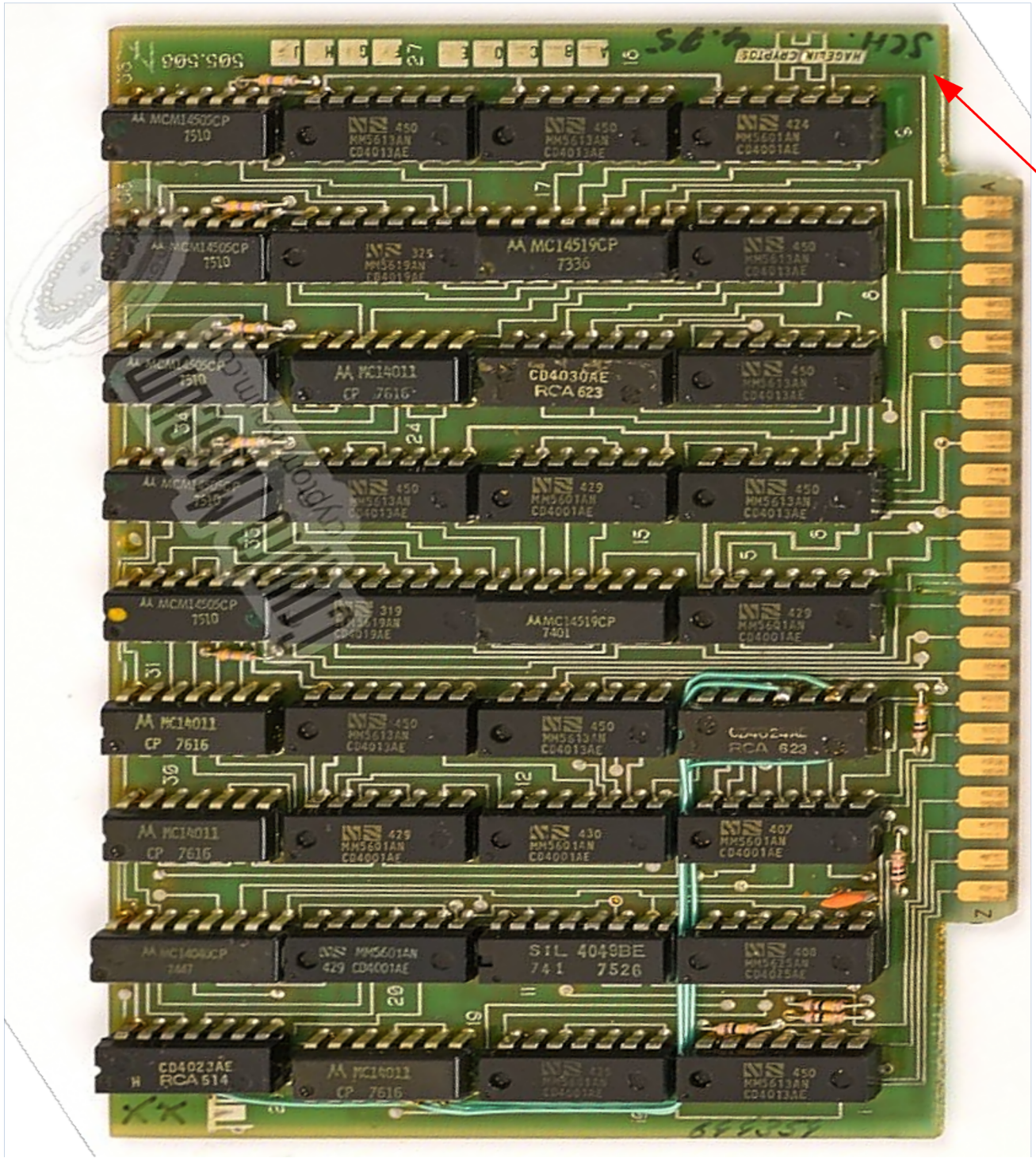
H-460 Tour



https://www.cryptomuseum.com/crypto/hagelin/h460

H-4605 Digital Board

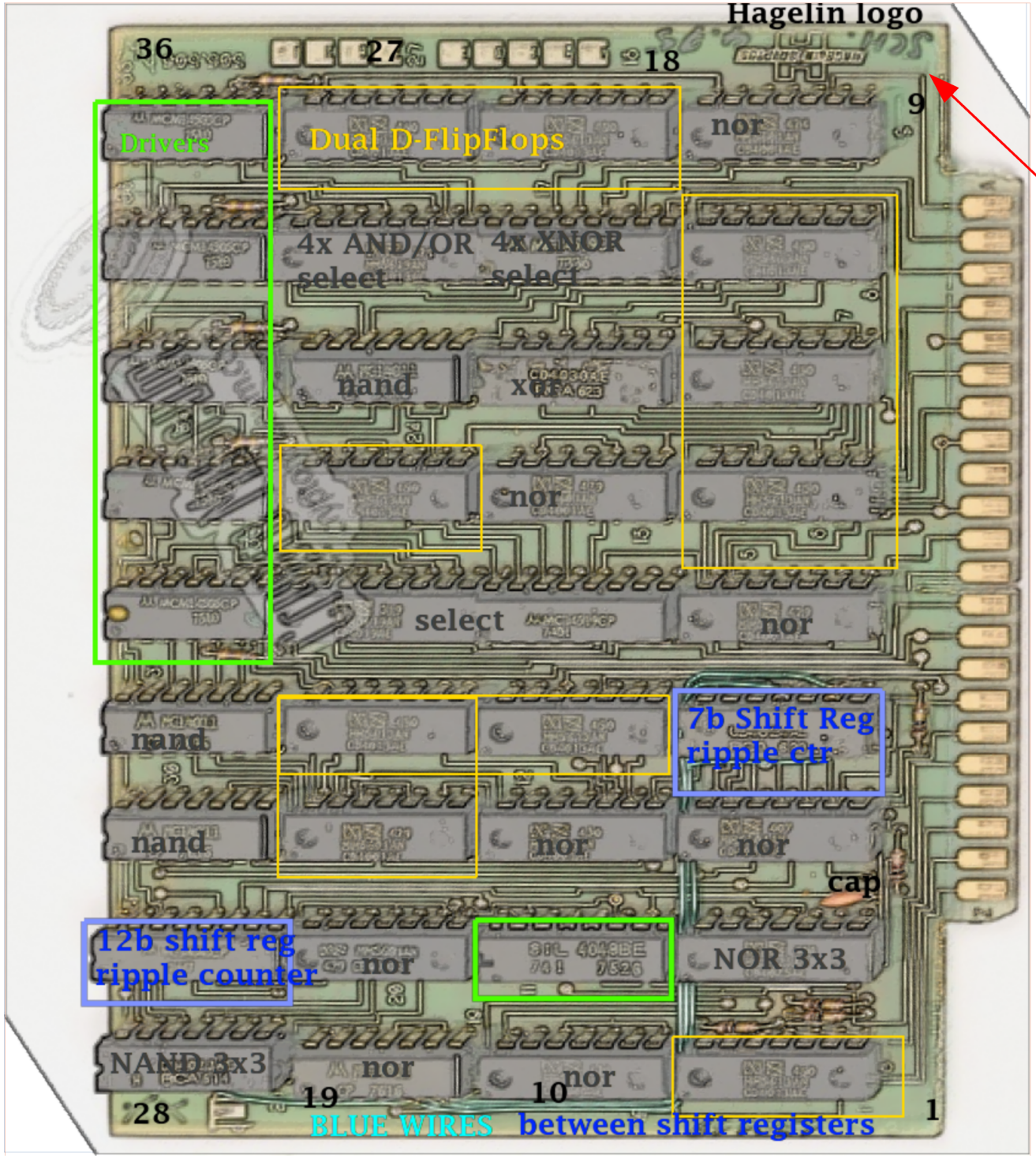
CryptoMuseum specimen photo, annotated by W.Ricker



SCH 4.75
Not updated for ’77 H-460x ?

H-4605 Digital Board

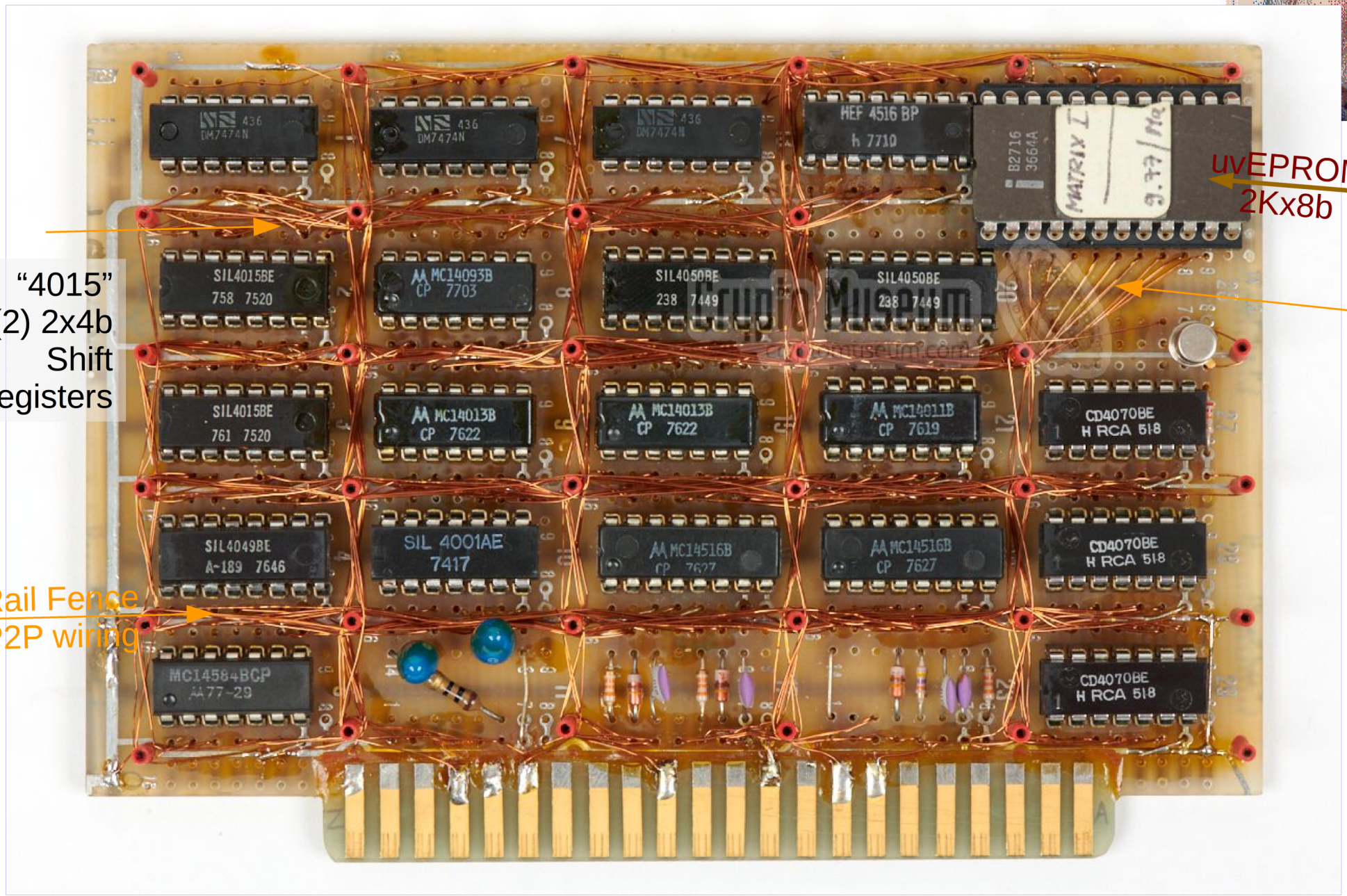
CryptoMuseum specimen photo, annotated by W.Ricker



SCH 4.75
Not updated for '77 H-460x ?

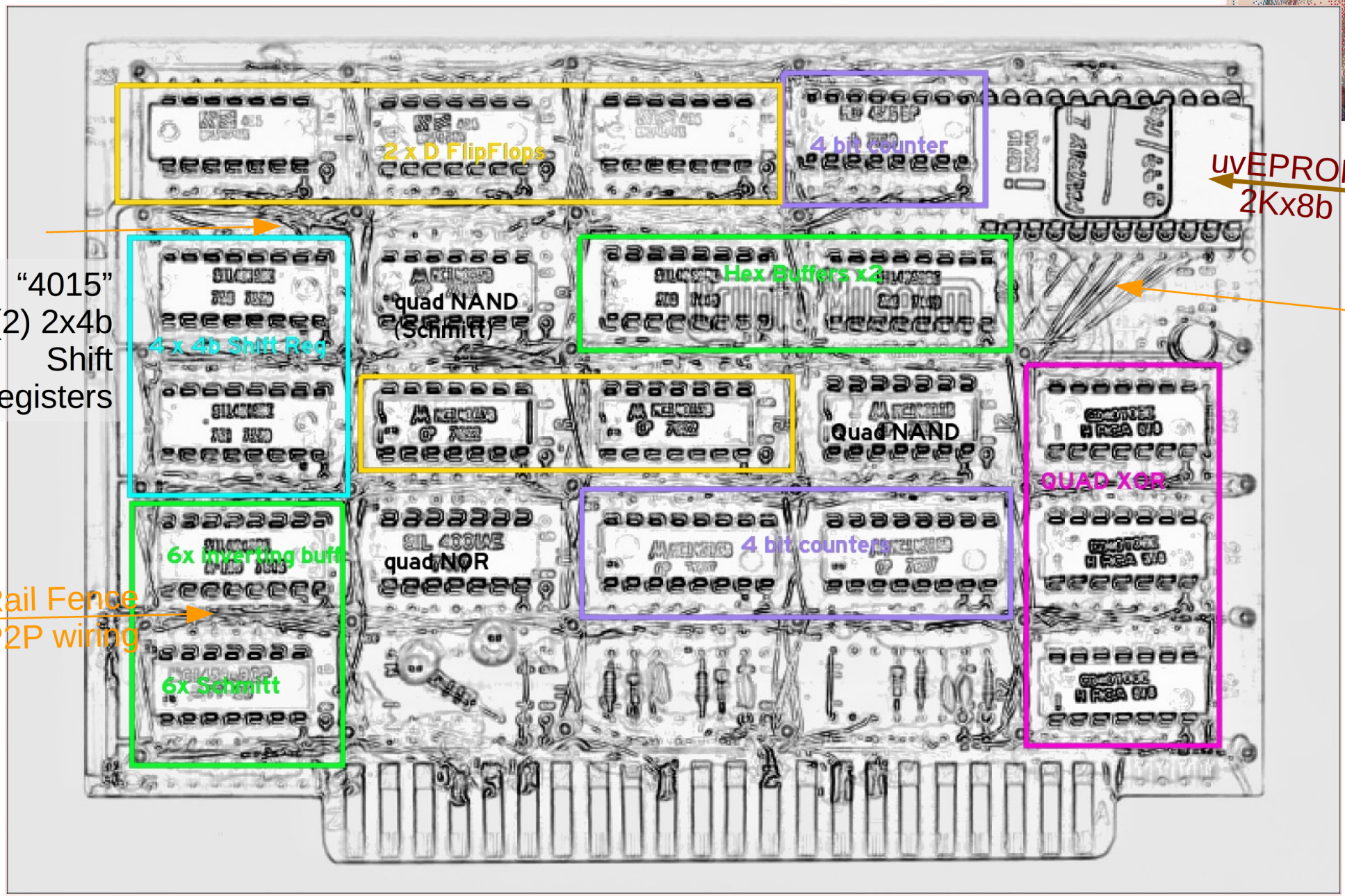
H-4605 CryptoLogicBoard

CryptoMuseum specimen photo, annotated by W.Ricker



H-4605 CryptoLogicBoard

CryptoMuseum specimen photo, annotated by W.Ricker



H-4605 Observations

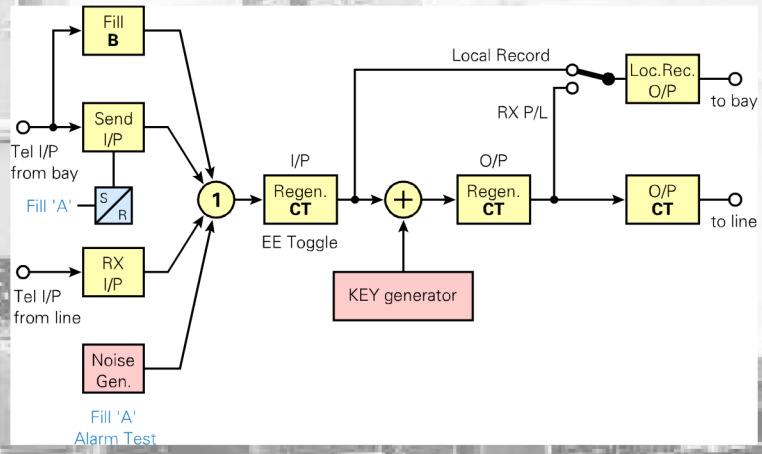
- Cryptologic board
  - Railfence wiring
    - circuit not discernible by photograph or Xray
  - 16b of MSI FSR
  - 10b of D-FlipFlop
  - 12b (3x4b) counters
  - 24b buffers
- Digital board
  - 12b& 7b CTR/FSRs
  - 20b D-FF
  - 36b Buffers
  - SCH 4.75 suggests not mod'ed
    - Unless blue-wires are 1977?
      - Should have markings for version if so!

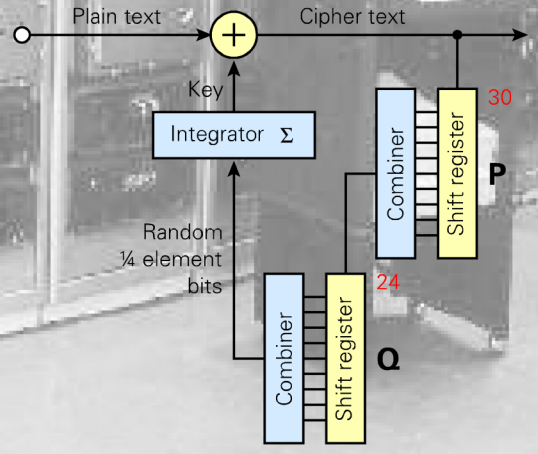
- Q. What is on ROM?
  - Microcode?
  - Constants=Variables per client
  - Which letter swapped for space
  - uvEPROM so not field re-writable, not key storage
- Q. How are E and I keys combined & used?
- Q. Where is key storage?
  - 25x5=125 bits of Internal=Basic Key
    - stored for reuse? Battery?
    - Bigger than any buffer, FF, Register!
  - 5x5=25 bits of Message/External Key
    - Bigger than any buffer except Digital board buffers?
  - Clocking for load, use?
  - Char-size 5bits assumed since Upper Case & TELEX unit co-evolved
  - Key Entropy: $\text{Log}_2(26)$=4.7bits/char
    - 117.5b message key entropy
    - 587.6b internal key entropy
    - *Not bad compared to later systems!*
    - (*Natural language message entropy much lower of course* !)

ALVIS BID/610 = TROL
a fuller **Transitional** design

- **T**apeless **R**otorless **O**n-**L**ine
- British built (Plessey)
- 1962-1965 Design,
  used to mid 1980s
- Approved for NATO Top Secret
  - ∴ *trusted by NSA*
  - ∴ *not compromised by NSA*
- OFB: Output Feed Back
  - Diffusion, but garble diffusion too
  - ¼ bit chips for error recovery/sync?
- Ganged FSRs
  - Final form used co-prime 24, 47 lengths
  - to avoid B-M *Before publication!*
- 7/7.5bits
  - @ 45.5, 50, or 75 baud
  - only 5 bits enciphered
    - *Exposing control chars' high bits seems lax and potentially an wedge point?*

Contemporaneous H-4605 doesn't have enough chips to build something this complicated.





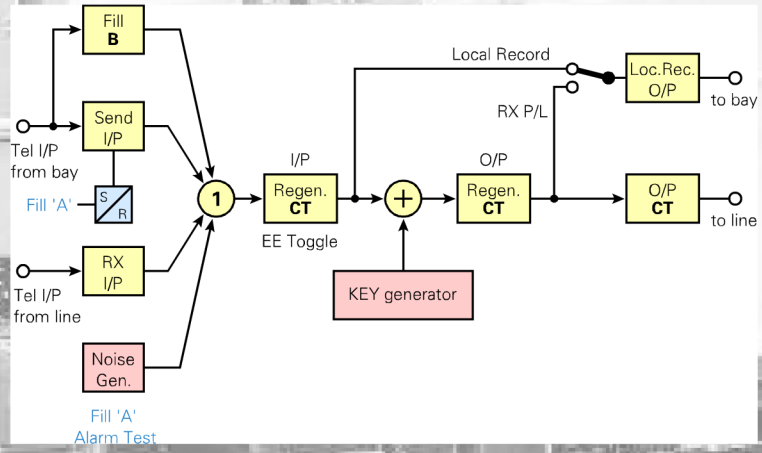
https://www.cryptomuseum.com/crypto/uk/bid610/index.htm

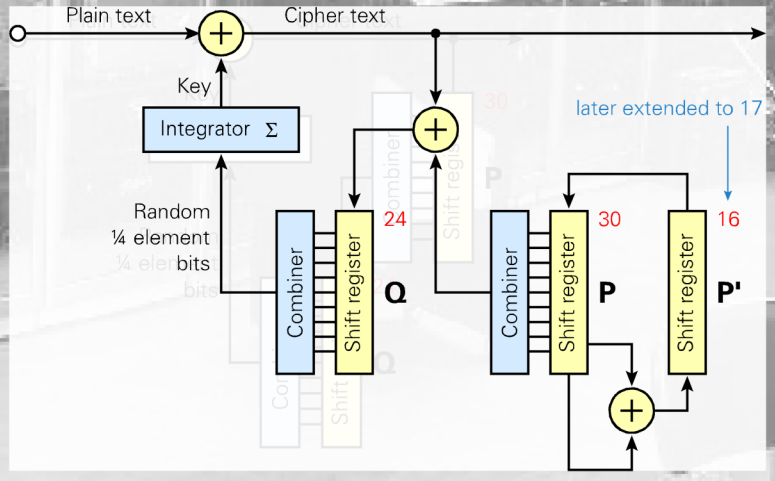
Canadian Foreign Office telex room, c. 1960's

ALVIS BID/610 = TROL
a fuller **Transitional** design

- **T**apeless **R**otorless **O**n-**L**ine
- British built (Plessey)
- 1962-1965 Design, used to mid 1980s
- Approved for NATO Top Secret
  - ∴ *trusted by NSA*
  - ∴ *not compromised by NSA*
- OFB: Output Feed Back
  - Diffusion, but garble diffusion too
  - ¼ bit chips for error recovery/sync?
- Ganged FSRs
  - Final form used co-prime 24, 47 lengths
  - to avoid B-M *Before publication!*
- 7/7.5bits
  - @ 45.5, 50, or 75 baud
  - only 5 bits enciphered
    - *Exposing control chars' high bits seems lax and potentially an wedge point?*

Contemporaneous H-4605 doesn't have enough chips to build something this complicated.





https://www.cryptomuseum.com/crypto/uk/bid610/index.htm

Canadian Foreign Office telex room, c. 1960's

H-4605 Timeline

- 1965 NSA 1st Crypto design
- 1969 Berlekamp-Massey algorithm Published (obsoletes single Linear FSR as crypto pRNG)
- 1972 effective ship (1970*)
- 1976 ITA,EGY complain it's too easy (*discovered B-M application to cryptanalysis*?)
- 1977 reissued as H-460x
  - 5=Italy
  - Stronger but still back-doored
  - https://www.cryptomuseum.com/crypto/hagelin/h460
- 1984 Cuba had broken some H-460 traffic too
  - per DDR Stasi files, in context that suggests Stasi had too
    - *with 1969 pub of B-M algo, anyone who wasn't reading a plain LFSR crypto wasn't trying*!

Inferences

- H-460: pRNG sequence XOR'd with plain text
  - Key sequence simple LFSR sequence
    - 12 or 16 bits
  - So B-M allowed reverse engineering of internal settings from deduced key seq
  - E-key, I-Key, Message text are all limited to 26-of-31chars,
    and likely same key encoding since same keyboard.
    Correlation / entropy attacks likely?
  - Further, B-M allows comparing presumed messages w/o key phase depth
    - Compare B-M implied internal keys from several messages with assumed plain-texts
      - Same internal key setting? Got it!
      - Different? One of the cribs is not aligned.
  - NSA may have reused CX-52 trick of non-maximal sequences in H-460
    – or CX-52M trick of making long sequence readable.
- H-460x: "repaired" but still readable somehow
  - Longer/Maximal sequence so that client doesn't see problem?
  - Perhaps Diffusion added?
  - Added non-linear feedback or collapsing output to block B-M?
  - 16 bits of CMOS MSI FSR available, presume M-sequence period 65,535
    - But could be 12bit FSR, with a 4-bit register unused or used for control data
  - Could have S-tables in ROM?
  - Extend FSR with D-FF's?
    - (if D-FF's not used for FSM state, could be XOR input taps in GLFSR!? Unlikely.)

H-460 Weaknesses?
(guesses!)

- Byte-stream: Substitution only, no Diffusion
  - Char streams don't diffuse beyond character
    - (*unless plain-text is in FSR feedback …*
      which means transmission corruption propagates too,
      tradeoff!)
  - *If* low-entropy text was just XOR'd bit-wise with pRNG key sequence (as TUNNY SZ-40/42) without bit-swapping (as STURGEON T-52), subject to depth attack.
  - "Crib" will expose pure key sequence
    (partial known plain text attack)
  - Probabilistic/correlation attacks in literature too.
- B-M algorithm reverses any pure key sequence to initial settings of LFSR (Taps and IV, which likely exposes I and E key).
- 1965 concept of "*large*" sequence-length not so large by 1977 digital computing capabilities. *And NSA had "large" before anyone else.*
- *If* CX-52M had covert-channel leaking keys, phase, H-460x could do same?

THESAURUS/MINERVA timeline *vs* H-460x

-
- 1969 FRG offers US partnership to buy; US freezes out French.
- 1970 “Retirement Sale” CIA+BND(FRD)**purchase** CryptoAG through shill shells; introduced Siemens and Motorolla coordination.
-
- 1975 NSA cryptographer signs into C.a.g. design meeting with own name,
  - collab w/ Motorola, w/ TI parts
  - HC-4700/4800 are Cryptofax updates
- 1977 Clark's biography of WFF mentions the 1957 meeting, against NSA advice
-
- 1979 backdoors improved
  - deniable, less obvious
  - inserting Mathematicians in the know in Crypto,a.g.

- 1965 H-460 co-design started
- 1969 T-450 online TELEX encryption launched
- 1970 CAG announces all-electronic H-460; shiped, has problems
- 1972 H-460 fixed, shipped
- 1976 Italy and Egpyt independently find weakness in H-460
- 1977 H-460x reissued in national variants, closing the customer-found weaknesses.
- 1978 Egypt wants T-450 strengthened too.

THESAURUS/MINERVA timeline *vs* H-460x

-
- 1969 FRG offers US partnership to buy; US freezes out French.
- 1970 “Retirement Sale” CIA+BND(FRD)**purchase** CryptoAG through shill shells; introduced Siemens and Motorolla coordination.
-
- 1975 NSA cryptographer signs into C.a.g. design meeting with own name,
  - collab w/ Motorola, w/ TI parts
  - HC-4700/4800 are Cryptofax updates
- 1977 Clark's biog
  the 1957 meetin
-
- 1979 backdoors
  - deniable, less ob
  - inserting Mather
    Crypto,a.g.

1990s HC-4220, inline successor in CRYPTOFAX line.

CAG/IA/Motorola Meeting - August 19-20, 1975

COMPILATION OF MINUTES

ATTENDEES: Sture Nyberg (CAG)
Oskar Sturzinger (CAG)
Peter Frutiger (CAG)
Herb Frank (IA)
Nora Mackabee (Motorola)
Jim Kirch (Motorola)
Keith Warble (Motorola)
Bob Pfeifer (Motorola)

1. There is a potential problem of procurement of printer mechanisms from TI by CAG.
   a. CAG has been unable to obtain TI commitment.
   b. Approximate qty required is 25/month.
   c. Keith will investigate and try to get TI commitment by 8/20.
2. 4700 Prototype 1 was demonstrated. Delivery of prototypes 1 and 2 is expected in about 3 weeks.
3. On-line (4800) requirements were discussed. Motorola will propose the development of an on-line teleprinter based upon the following requirements:
   a. Direct utilization of 4700 peripherals and interface electronics will be the basis for the 4800. (Same Cipher as 460)
   b. 4700 mechanical design philosophy and implementation is acceptable for the 4800.
   c. 4800 shall have temp range of 0° to 50°C.
   d. Baud rates shall be 50, 75, 100 and 200 baud.
   e. The cypher text format shall be switch selectable as 5 letter group or continuous text as in the 4700.
   f. The 4800 shall have capability of 4700 off-line capability as well as on-line capability.
   g. The 4800 shall have 2 key generators, one used for transmit and the other for receive. Direct utilization of 2 4700 KG's is acceptable with a modification of the 4700 implementation to reduce hardware as an option.

MINERVA/RUBICON denouement

- **1982** Bamford "*The Puzzle Palace*" mentions “the Boris Project”
- 1987-88 Washington claims knowledge of Iranian cables
- **1991** Swiss news leaks that US decrypted Iranian assassination cable
- 1992-1993 Iran arrests, holds CAG sales exec. Hans Buehler
- 1993 **CIA** buys out BND shares for $17M
- 1995 **“Swiss firm disputes allegations of rigging**
  Maker of code machines labels link with NSA 'hearsay' and 'invention'; NO SUCH AGENCY”
  Scott Shane in [Balt.Sun] (4 part series)
  - His 2020 retrospective twitter comments on old article [ThreadReader]
  - Included the 1975 Design meeting minutes with NSA cryptologist name
- 1994-1997 Swiss Federal Prosecutors reportedly found allegations "without foundation"
- 1997 Grabbe – Crypto AG and dirty secrets of Iran/Iraq war [archive]
- 1998 Summary of issues to date [archives]
- **2004** Schneier on Iranian codes [schneier] references Grabbe 1997 ^
- 2007-12 … and [schneir] references [archive] and 10 year old European articles, well-known in Germany for some time.
- **2014** Friedman Collection - Gentleman's agreement revealed in letters redacted [nsa][MarshallLib][memo][1970 NSA BH Bio] !
- 2015 Confirmed compromise [BBC]

At this point, anyone paying attention presumes C-a.g. was compromised by NSA, but no public, official recognition aside from Iranians. Officially dismissed as “rumors”.

Different versions of the report:

~~TOP SECRET~~

~~TOP SECRET~~

e. Hagelin Senior thanked me but said he did not need time to think the matter over; he was prepared to [redacted]

Redacted text

Full text of redacted version

~~TOP SECRET~~

~~TOP SECRET~~

EO 3.3(h)(2)
PL 86-36/50 USC 3605

e. Hagelin Senior thanked me but said he did not need time to think the matter over; he was prepared to make an answer then and there to our proposal: He accepted it without any reservations or desire for modifications. But he would like to have some more details; he wanted to know, for example, [redacted] I told him I was not authorized nor able to give him more information on this score at this time but I had no doubt that such details would be forthcoming at the proper time.

Differently redacted text

BBC 2015 story illustration, using the 2014 redaction

MINERVA/RUBICON denouement

- **1982** Bamford "*The Puzzle Palace*" mentions “the Boris Project”
- 1987-88 Washington claims knowledge of Iranian cables
- **1991** Swiss news leaks that US decrypted Iranian assassination cable
- 1992-1993 Iran arrests, holds CAG sales exec. Hans Buehler
- 1993 **CIA** buys out BND shares for $17M
- 1995 **“Swiss firm disputes allegations of rigging**
  Maker of code machines labels link with NSA 'hearsay' and 'invention'; NO SUCH AGENCY”
  Scott Shane in [Balt.Sun] (4 part series)
  - His 2020 retrospective twitter comments on old article [ThreadReader]
  - Included the 1975 Design meeting minutes with NSA cryptologist name
- 1994-1997 Swiss Federal Prosecutors reportedly found allegations "without foundation"
- 1997 Grabbe – Crypto AG and dirty secrets of Iran/Iraq war [archive]
- 1998 Summary of issues to date [archives]
- **2004** Schneier on Iranian codes [schneier] references Grabbe 1997 ^
- 2007-12 … and [schneir] references [archive] and 10 year old European articles, well-known in Germany for some time.
- **2014** Friedman Collection - Gentleman's agreement revealed in letters redacted [nsa][MarshallLib][memo][1970 NSA BH Bio] !
- 2015 Confirmed compromise [BBC]

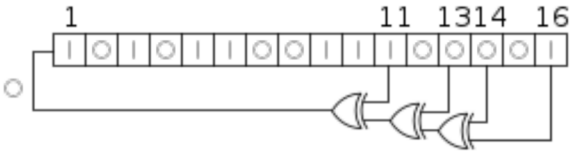
At this point, anyone paying attention presumes C-a.g. was compromised by NSA, but no public, official recognition aside from Iranians. Officially dismissed as “rumors”.

- **2018 CryptoAG liquidated** into 2 new firms, new owners -
  - CyOne Security (Swiss Gov equipment) and
  - Crypto Int'l AG. (C.I.ag) for export
    - Swedish buyers claim not to have noticed or to have discounted German & BBC reports …
- **2019** Swiss Public TV [rts.ch] **Exposé**
  - FR: [rts.ch video] 18.11.2019, 17h01
  - **La Suisse sous couverture - Agents infiltrés** (1/5)
    - **Switzerland undercover - Undercover agents (1/5)**
    - “In 1955, the American intelligence services and the Swiss company Crypto AG concluded a confidential agreement which will allow the espionage of the communications of 130 countries. For decades, a section of Swiss industry will be involved in these activities, despite the country's "neutrality" and with the blessing of the Federal Council.” [Translate.Google]
- 2019-**12** Swiss Econ Ministry suspends C.I.ag’s export license
- **2020-02**-11 [WaPo] **“Intelligence Coup of the Century”**
  - `[http://wapo.st/crypto] + [CryptoMuseum.com: RUBICON]`
  - CIA was bagman for ownership
    (but original connection and expertise was always NSA)
  - Video [YT] Marc Simons of cryptomuseum.com demonstrates use of CX-52 (one of the compromised machines), companion video to WaPo story ^^
  - Comment [Schneir]; [NSaGWU] “CIA’s MINVERVA Secret”
- 2020-**03**-01 Swiss Prosecutors file Criminal Complaint, open inquiry.
- 2020-?spring? C.I.ag denied review on Swiss export permits.
- 2020-**07**-04 Mass Layoffs at Crypto Int’l AG
- 2020-**08-27** - Crypto Intl AG files bankruptcy [CryptoMuseum]
  - Winding-up, ala US Ch.7
  - After another denial of export permit appeal.
  - Swedish owners’ Asperiq may pick up some work in Switzerland ?

- 73 -

Q&A ?

If time permits
<u>and</u> there's interest,
I could demonstrate a LFSR in
software
(*again*?)



or I can save it for Boston.PM.