Crypto News 2017

Bill Ricker
for BLU.org annual keysigning
Sept 20, 2017

0. Agenda

1. Crypto News Review
2. Annual Historical Vignette
3. How To Reminder for GPG/PGP Key-signing
4. GPG/PGP Key-signing

2016 not mentioned last year

- https://www.eff.org/deeplinks/2016/12/what-happened-crypto-2016
  - “TLS 1.3 design finalized” (includes newer faster curves)
  - “The quest for post-quantum cryptography continues”
  - *kleptography*
    - “New thinking on how to backdoor cryptographic algorithms”
    - Snowden revelations; DualEC backdoor
    - D-H Key Exchange has unsafe primes (October SN#581 ars iacr 961)
    - RFC 5114 suspected (BBN crafted DH groups, in OpenSSH and Bouncy Castle)
  - Pwns: “Attacks only get better”
    - HEIST improved on compression-oracles
    - Sweet32 – 64bit block in CBC mode: Birthday meet-in-middle (3DES, Blowfish)
      - Irrespective of key-size.
- Check https://www.eff.org/deeplinks in January to see what I left out today

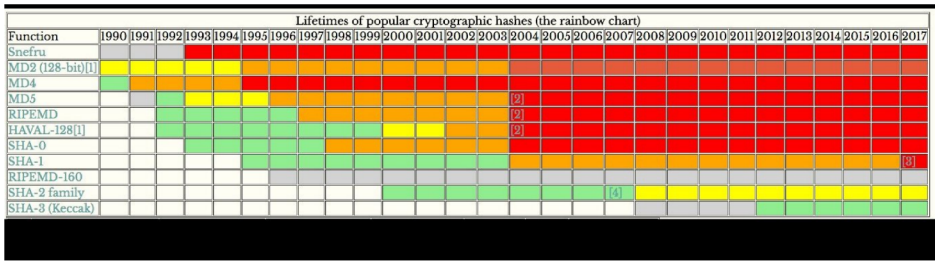
News since 2016.ix

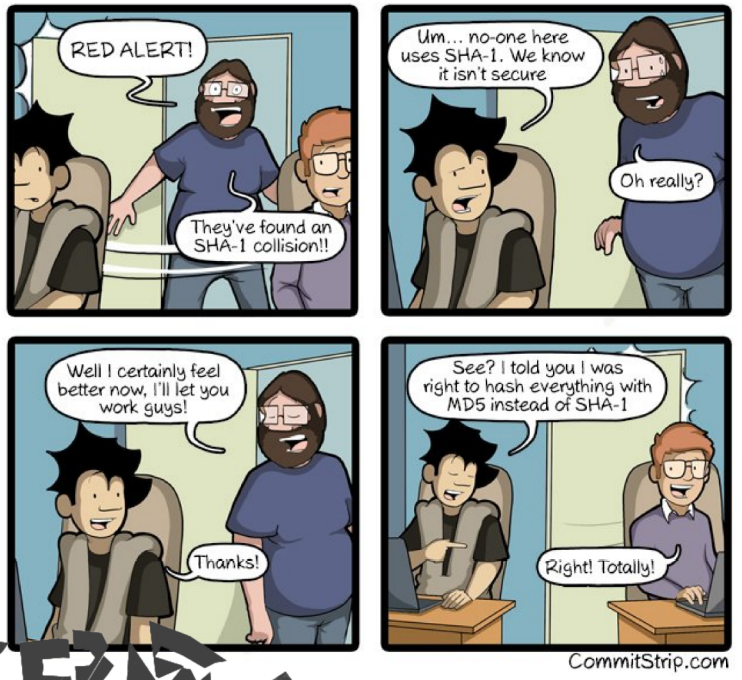
- Upgrade SSH keys
  - DSA & RSA 1024b keys deprecated & 2048 short-life.
  - ssh-keygen -a 100 -t ed25519 # EdDSA Twisted Edward curves
  - https://blog.g3rt.nl/upgrade-your-ssh-keys.html
    - Alas ED still “experimental” in PGP/GPG, not standardized yet :-(
- Is it time to adopt post-Quantum algorithms?
  - Betteridge's Law: No. Don’t panic. Not yet, anyway.
- Ubiquitous HTTPS encryption
  - LetsEncrypt https://letsencrypt.org/
    - May require automation to renew regularly
    - https://metacpan.org/pod/Crypt::LE Can help
- Dirty Cow may leak keys – covered April BLU on IOT
- WannaCry left its P & Q primes in RAM.
  - WannaKey tries to recover them.
  - Alas mostly blocked by improved OS security on mostly targeted versions of WIN
- SHA1TTERED – next slide

SHA-1 SHA1TERED

- First *practical* Sha-1 collision generation.
  - **Migrate Immediately if not sooner**.
  - Unsurprising considering results on MD5 and SHA-0.
  - NIST had recommended transition to SHA-2 by **2010**
    - https://shattered.io/
    - https://security.googleblog.com/2017/02/announcing-first-sha1-collision.html
  - Blake2 is alternative to SHA-2, SHA-3 for Floss
    - https://blake2.net/acns/slides.html
- Impacts
  - PDF pun using this @angealbertini (next slide)
    - https://twitter.com/marcan42/status/835175023425966080
    - https://alf.nu/SHA1 **make your own**
    - https://news.ycombinator.com/item?id=13715761 …
  - SVN broken with two files with same SHA-1 !
  - BitErrant ... Bit-torrent runs on SHA1 block-id
    - BitTorrent Poisoning
    - @SkelSec #biterrant a practical example of backdooring binaries using #SHA1 #SHAttered collision using the #bittorrent proto.
    - https://biterrant.io/

@vaurorapub "rainbow chart" of cryptographic hash function lifetimes http://valerieaurora.org/hash.html





SHATTERED

SHA1TERED (2) – PDF/JPEG

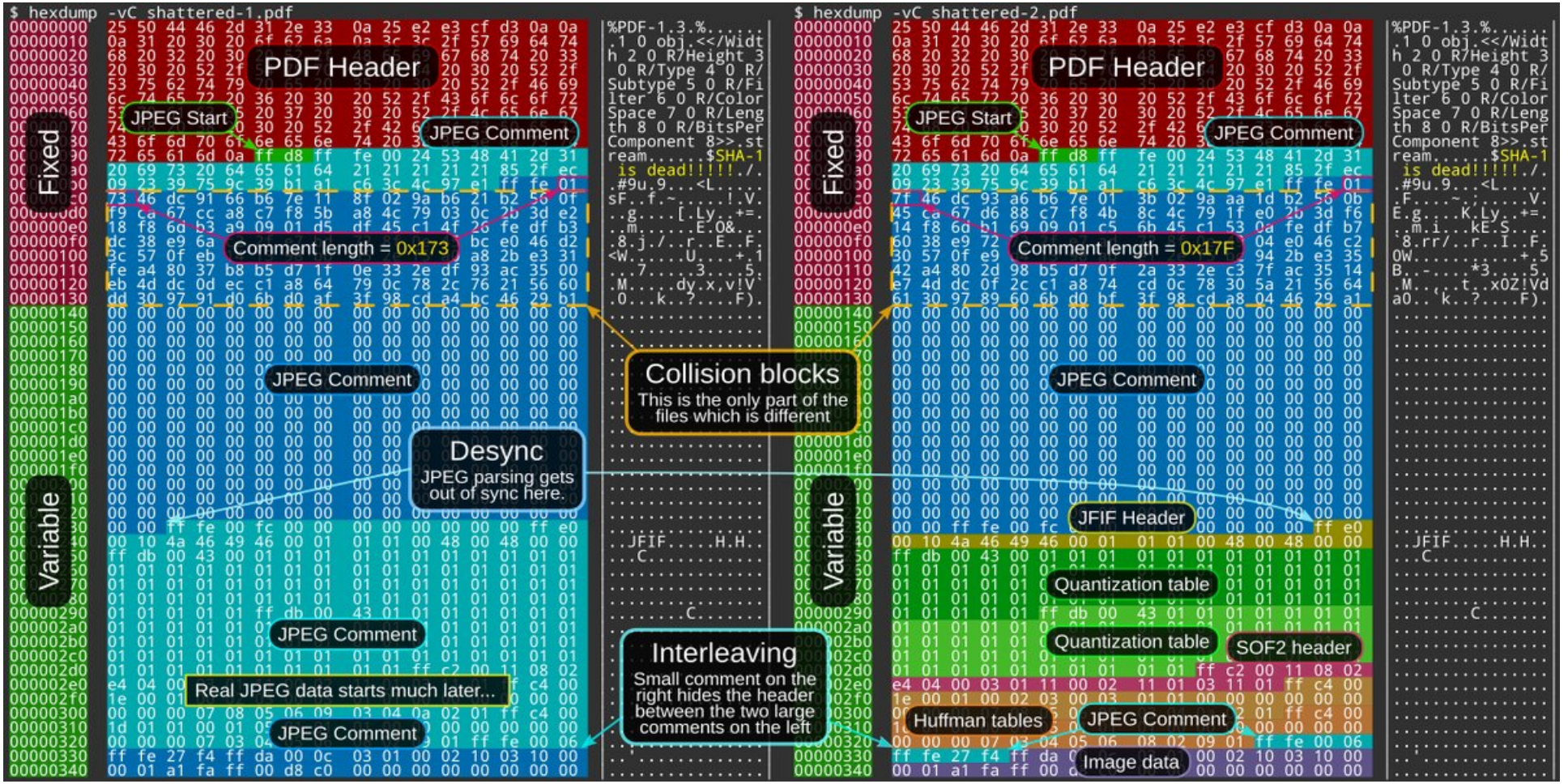
Leveraging one collision to whatever:

```
$ sha1sum ?.pdf
0666a097252b88af21c760745248840c636be9e8  a.pdf
0666a097252b88af21c760745248840c636be9e8  b.pdf
```

a.pdf
18.7 kB

b.pdf
18.7 kB

SHA1TERED (3)



SHATTERED

How about Git with SHA-1 compromised?

Answer from Linus re Git & SHA1 -

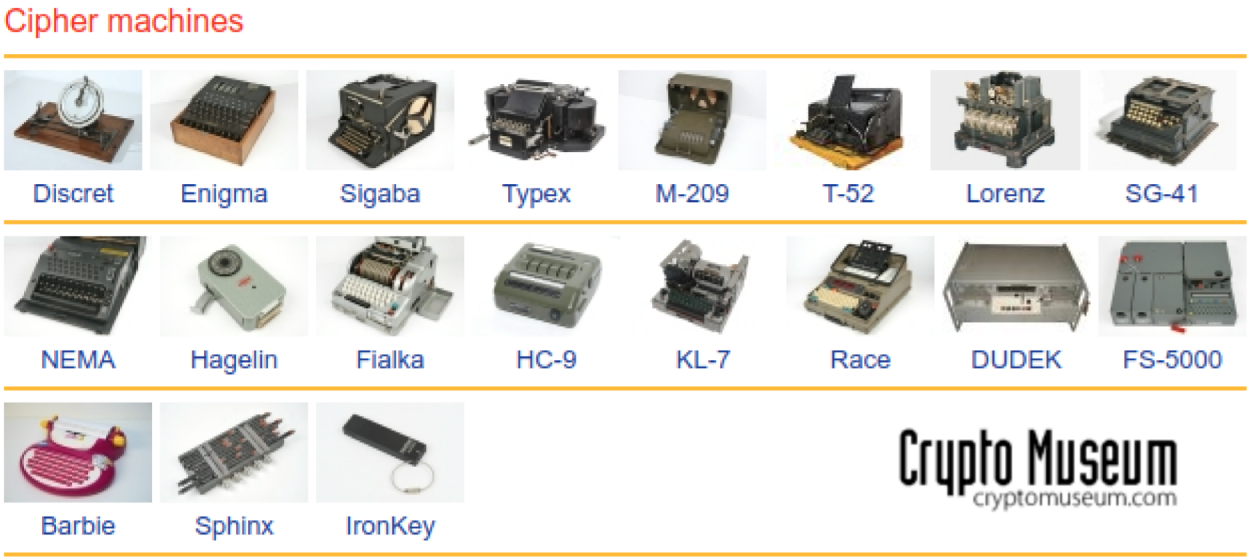
- git is less affected than SVN.
- The free-collision-generator for PDF(JPG) that reuses the one found collision does NOT affect git tree objects directly,
- so cost to find prefix collision is reduced by this but not to $0 .
  - Attacker must control both "good" and "bad" files.
  - Mitigation code to detect this sort of attack already available.
- But git will migrate from SHA1 to something else
  - without breaking existing repos,
  - eventually.
  - but not at panic speed.
- https://plus.google.com/+LinusTorvalds/posts/7tp2gYWQugL

2. Annual Historical Vignette

Of Enigmas and Fishes

Or,

Of Wheels and Rotors and Drums



Wheels, Rotors, and Drums

Drum/Pin&Lug

- Early Adding machines !
- Damm/Hagelin/Crypto.ag
- M-209
- SG 41
- … many more !

Rotors

- Enigma 3½X26 (4½)
- RED (½ x lcm(20,6)=60)
- PURPLE / CORAL / JADE
  - Actually telephone steppers not rotors!
  - Purple maintained 20+6 split
- SIGABA 5x26
- TypeX 5x26
- Fialka (M-125) 10x30
- M-325 SIGFOY 3½x26
- M-228 SIGCUM 5x26

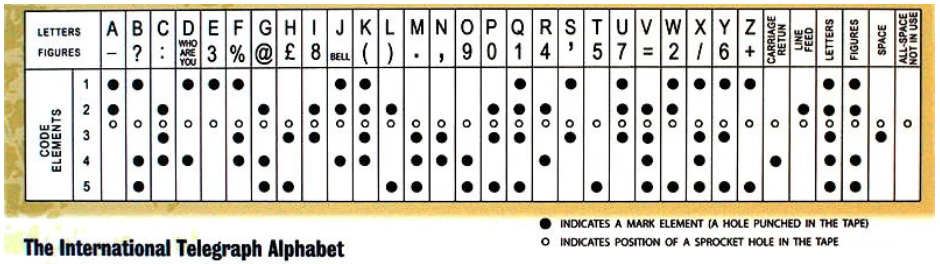
Wheels

- Parker Hitt 10x {96 97 98 99 100 101 102 103 104 105} !!
- SZ40,SZ42 Lorentz Tunny 12 x {41 31 29 26 23; 43 47 51 53 59; 61 37}
- T52 Siemens Sturgeon 10 x {47 53 59 61 64 65 67 69 71 73}

Tape Mixers

- Vernam / Maughborne / Telekrypton
- Rockex
- 5-UCO = BID/30 (OTT, ULTRA dist.)
- T-43 Thrasher OTT
  - TEMPEST-like problem in relay logic.
- SIGTOT SSM-33 (OTT; relay logic; 19??-1959; Rotor KW-2 key avail also.)
  - The original for US TEMPEST !

Baudot Code

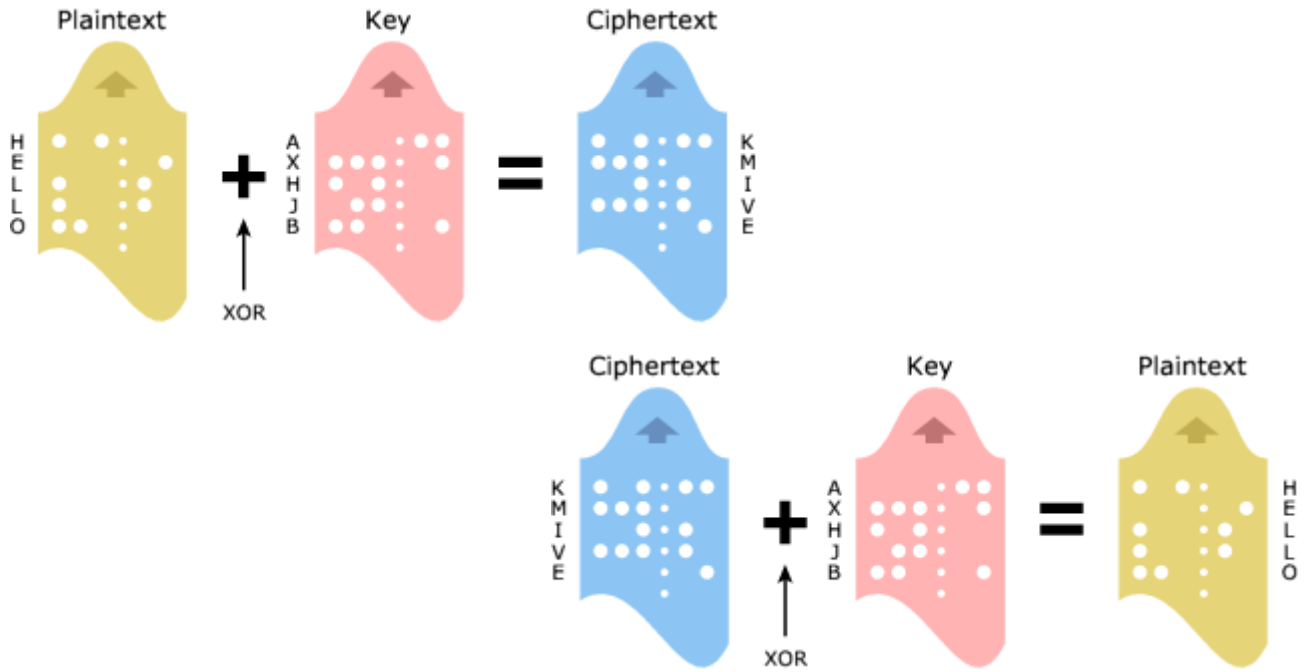


The International Telegraph Alphabet

- 5 Channels
  - Standardized as CCITT Alphabet 2
- Coding chosen to **<u>minimize mechanical wear</u>** on operating solenoids etc.
  - Most likely letters have fewest “ON” bits, & vice-versa.
  - **1: `E T space CR LF`**
  - **2**: **`A D H I L N O R S`**
  - Hence 0 bit is more common in all 5 channels in plain text
    - (8-bit ASCII has different structures but still has structures)
- Shift Letters ↔ Figures/punc.
  - Shifts repeated to mostly correct radio errors
    - PERIOD = `++M--`
    - Punctuation Is very heavy in 1 bits, unlike normal text

Image: Hackaday
https://hackaday.com/2015/09/27/demonstrating-baudot-code/

Vernam Arithmetic (1918)



XOR, aka Modulo-Two Addition. Before Transistors (or even Vacuum Valve Flip-Flops)

Key Distribution problem worse than Code books or Book codes !
Perfect security **IF** One-Time-Tape is one-time; destroyed; random; no TEMPEST.
Each has been violated ...

http://www.cryptomuseum.com/crypto/vernam.htm

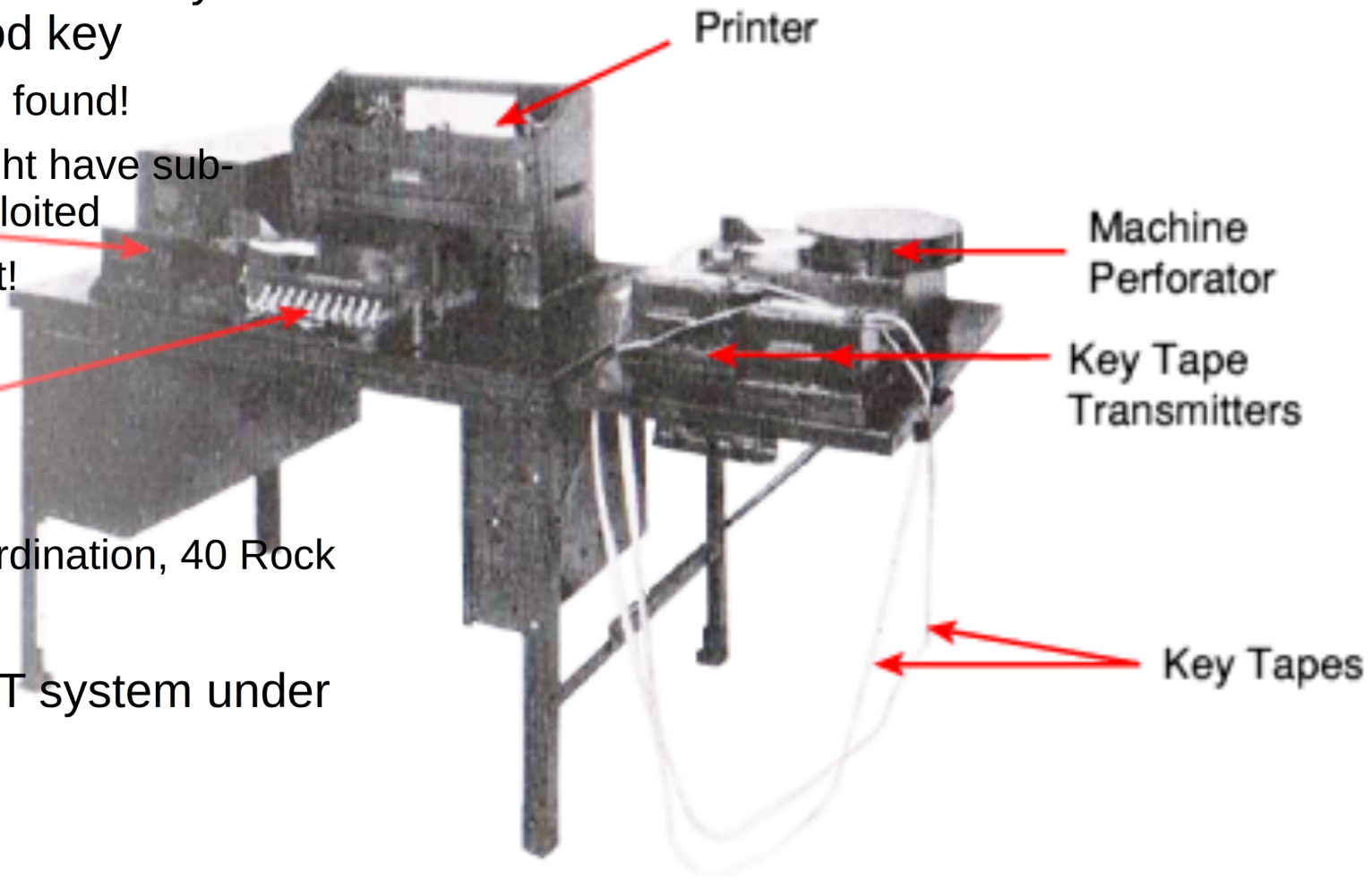
Telekrypton (1933)

- Vernam Cipher, 1918
- Western Union (prototypes 1925?)
- Designed for OTT but actually did 999*1000 long period key

  Weakness if depths found!

  Long messages might have sub-periods found & exploited

  periods in the patent!
- Modified to Rockex
  - for real OTT !
- Used transatlantic
  - British Security Coordination, 40 Rock
  - Camp X
- Evolves into SIGTOT system under Signal Corps

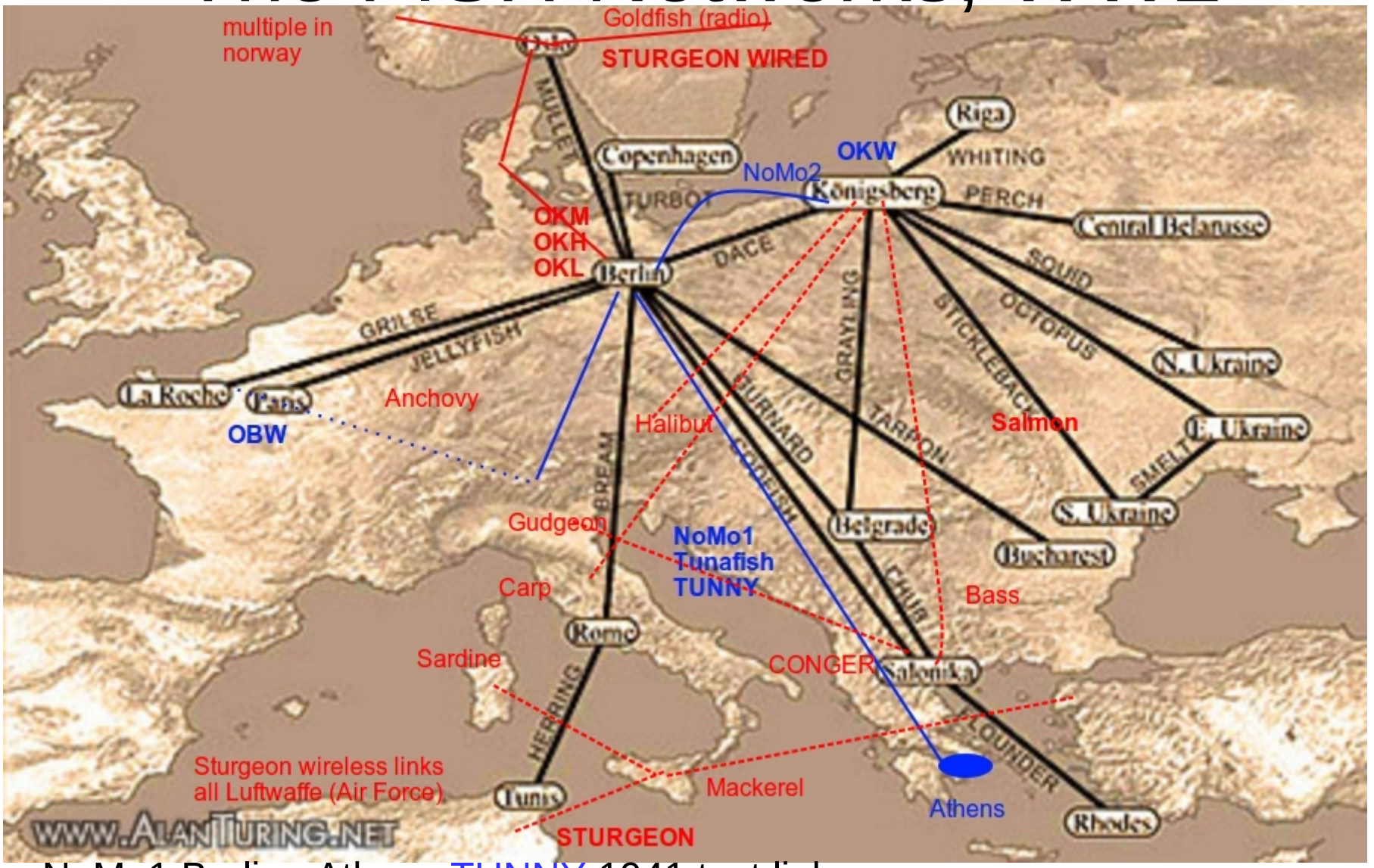


Enigma broken, what next?

- Enigma
  - enciphered offline, transmitted by hand Morse modulation.
  - unbroken at times
  - Issued at Division, Corps, and *Panzergruppe* levels
- More strategic command levels had different intel, but strictly wireline, inaccessible.

Guderian in his half-track, PzKorps mobile CP, with Enigma machine, radio ops. France 1940

The FISH Networks, WW2



- NoMo1 Berlin - Athens TUNNY 1941 test link
- NoMo2 Berlin (OKL) - Konigsberg (Luftw.) test link
- Germans call it TTY-via-HF-radio "Sägefisch" (sawfish) [*Oscilloscope joke*!]

Lorenz SZ 40/42 “Tunny”

- 5-channel Baudot TTY in-line cipher unit
  - Add-on to a TTY, either wireline or radio
    - Intended for wireline use, thought untappable
  - Each channel separately encoded $Z_i = P_i + K_i$
  - Rotors “replace” key-tape(s) in a Vernam design
    - Von Neuman’s “State of Sin”
    - Engineering compromise
    - Invented separately at least 4 times
- SZ 40 (old/original model = prototype)
  - roughly identical to Hitt’s 10 wheel machine which was known insecure
    - Lorenz subsidiary of ITT, parent of Hitt’s assignee!
    - Hitt’s had wheels that were not co-prime ! Fixed that!
    - Fixed pins on each wheel
  - K= $\chi + \psi$, uniform motion
  - *OKW/chi* : 1000 character single message was breakable.
    - Channels separable and superimpose by rectangles; P mostly 0; deduce wheel pattern and key.

- SZ 40 / SZ 42 iteratively fixed
  - Pins made Movable cams
  - “each link had its own set of wheel patterns”
  - Change χ pins monthly, ψ quarterly (then monthly), motor M wheels Mu37, Mu61 daily.
    - Later, all change daily.
  - 11th & 12th “Motor” Mu wheels make Psi wheels motion irregular
    - But the Psi still move together if they move – or don’t
    - Complication Illusoir !

TUNNY Cryptanalysis

- Sub-periods still remain!
- Delta Transform
  - $\Delta Z = \Delta P + \Delta K$
  - $\Delta K = \Delta X + \Delta \Psi$
  - ΔP mostly 0's (Baudot)
  - $\Delta \Psi$= 00000 if Psi didn't move;
  - So $p(\Delta Z_i \cong \Delta X_i) > 50\%$
  - And $\Delta \Psi_i = 0 \leftrightarrow \Delta \Psi_j = 0$

- *OKW/chi* was aware of these problems, and planned SZ 42C which would have non-uniform motion of wheels. [TICOM]
- Bletchley Park deduced the full internal structure from one long message in depth with self.

https://en.wikipedia.org/wiki/Cryptanalysis_of_the_Lorenz_cipher
& more pix
https://en.wikipedia.org/wiki/Cryptanalysis_of_the_Lorenz_cipher#/media/File:SZ42-6-wheels-lightened.jpg

TICOM team has POWs pack OBW JELLYFISH for transport to UK.
Photo 1LT Paul K. Whitaker, AUS.
via Wikimedia

Siemens Sturgeon SFM T-52

- 5 channel Teleprinter, not an attachment
  - Originally for wired use
  - Presume Radio links were initially backups?
- 10 wheels, fixed pegs
  - Should have issued new wheels periodically
  - May have intended 6 month swap per intel, but logistics not provided for?
  - Personnel, Diplomatic, Police wired nets in occupied Scandinavia did have different wheels from Air Force radio nets
- Wheel to Key map is sole inner key
  - Message Key scrambled wheel assignments as outer key in later models too!
- 5 key streams XOR the 5 Baudot bits
- 5 key streams swap adjacent bits
  - 30 of 120 possible permutations; 2 overused

- First bit permutation operation implemented !
  - *W.F.Friedman of US ASA had patent first*
- T-52a/b assigned each wheel to one key stream
  - Similar to Tunny, but permutation reduced per-channel attack
- T-52c combined (4 of 10) wheels to produce each of 10 key streams
  - Actually reduced complexity to break!
  - Noticed by Ger. Sig.Sec
  - T-52ca undid some of the damage
  - T-52d, T-52e considered secure by Brits and US as well as Germans

Siemens SFM T-52 “Sturgeon”

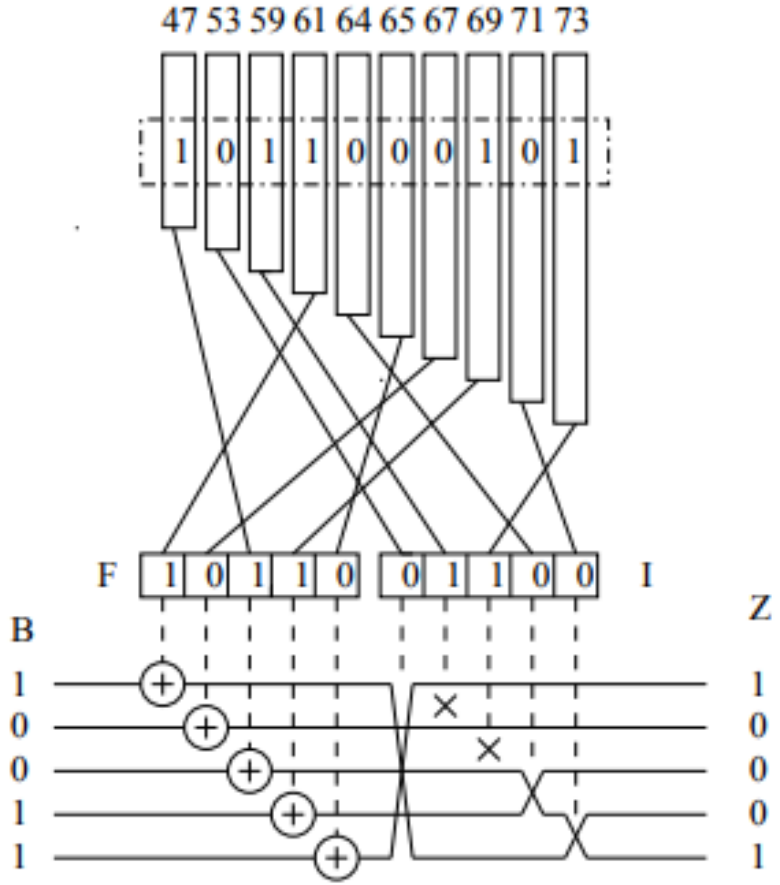


Figure1. SFM T52's functional diagram.

T-52a/b functional diagram

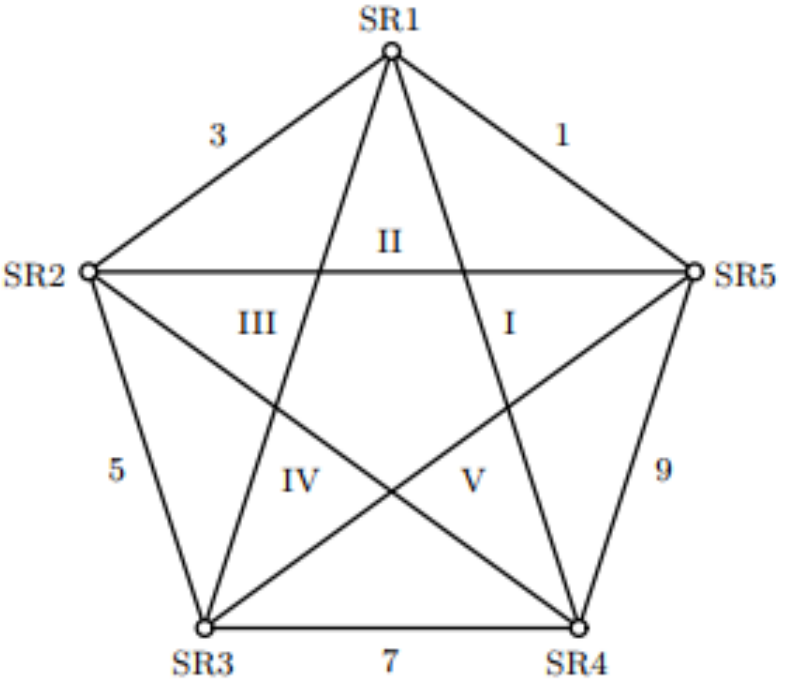


Figure3. The Pentagon

T-52c wheel combining for Permutor registers

(Substitutors similar) – attempt to mask short sub-periods

Too much structure: 60/1024 possible alphabets used; is now parity preserving! OOPSIE. OKW/chi noticed, and ‘ca’, ‘d’, ‘e’ followed.

Sturgeon Cryptanalysis

- Insecure T-52c broken by BP (radio), Swedes (wire tap) and OKW/chi (inspection).
- Entry kept with T-52a/b, T-52c(a).
- Breaking never automated at BP. (OKW/chi used IBM tabulating machines.)
- T-52d/e considered secure by both BP & OKW/chi
  - But even so a long T-52d message on Hallibut was broken by hand at BP
    - without KTF*, but with irregular cross-motor'ed wheel motion, fully solved.
    - required depth of 4, received 4½ , from a single message.
    - 5-part message sent with same starting position for each part! *Lazy scofflaws.*
  - *Not cost effective to wait for rarer depths as discipline improved.*
    And KTF would block depths if used routinely.
- Germans inconsistent whether wheels were"key" .
- Impact
  - Swedish intercepts were strategic gold.
  - Sturgeon on Radio mostly routine AF HQ stuff, useful during Enigma outage during El Alamein but boring later, not worth the cost to break.
  - Enigma & Tunny given priority at BP for automation and hand-breaking.

Klartextfunction

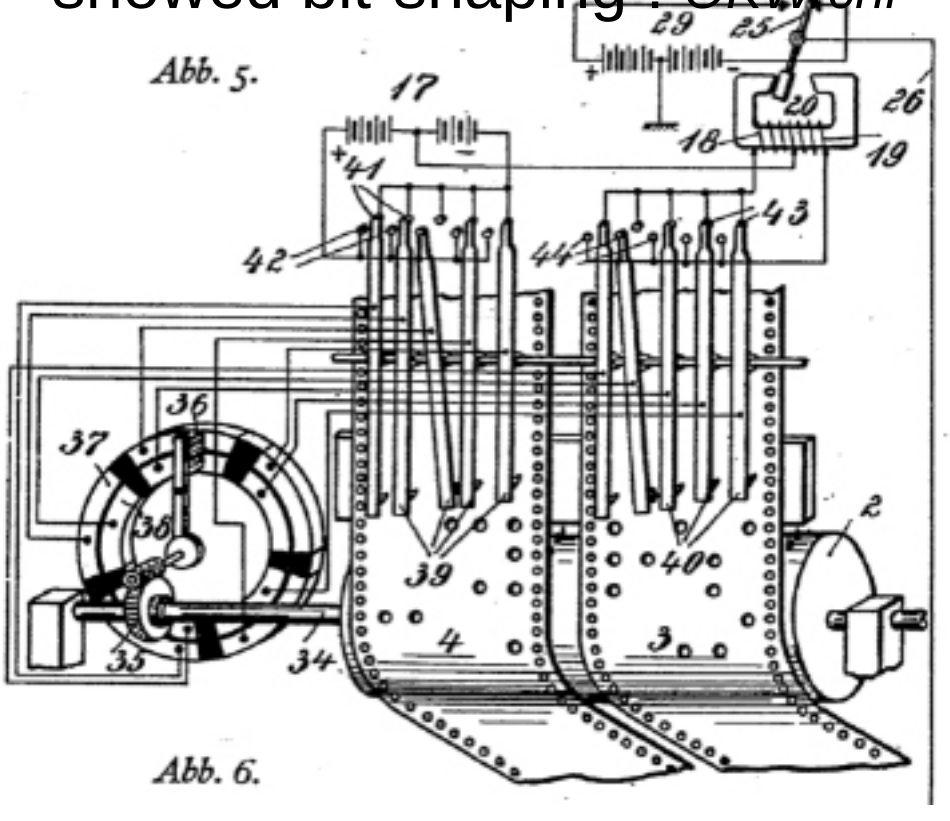
- For both SZ 42 and SFM T-52, OKW/chi was rightly concerned that depths would lead to compromise.
- Injecting a small amount of feedback from Plain, the KTF, would prevent same / near setting resulting in a depth
  - But Errors propagate w/o limit
  - Very bad for HF Radio!
  - So Least useful on longest messages where most needed!
  - So largely turned off in the field.

- Several KTF variations were used in both SZ-42 & T-52 machines
- OKW/chi did not have monitoring & enforcement authority to keep KTF on (and reset to start off).
  - *USA ASA did !*

Thrasher T-43

- Siemens SFM T-43
  - 1943/1944
- “Mixer”
  - could be OTT
  - Was assumed to be by BP
- Mostly wireline
  - Response to T-52 wireline tapping by French Resistance ?
  - Some radio as tests, and later in war of maneuver (retreat)
- Presaged by Vernam/Bell
  - Likely read the patents!

- Keytape produced by two T-52e in series
  - Von Neumann’s State of sin!
- Slow relays = oscilloscope showed bit-shaping ! *OKW/chi*



Recurring Themes

- Cribs from stereotype, verbosity, lack of abbreviation = known partial plaintext
- Limited alphabets force shift or spelling of numbers, punc
- Redundancy for error correction helps cryptanalyst too.
- Strengthening a weak system presumes not yet broken.
- Depths & near Depths
- Ignore Automation, Divide and Conquer, Guess & Confirm

- Human Error
  - Laziness. (Never reuse nonce.)
  - Poor training
  - no monitoring
  - On air test/training
- Forget Kerkoffs
- Imperfect Implementation
  - Unforeseen engineering
  - Sidechannels/TEMPEST
  - Data left behind
  - Random 7 7 7 7 7
- *Complications illusoire*

3. GPG/PGP Key Signing

- A quick HOW TO