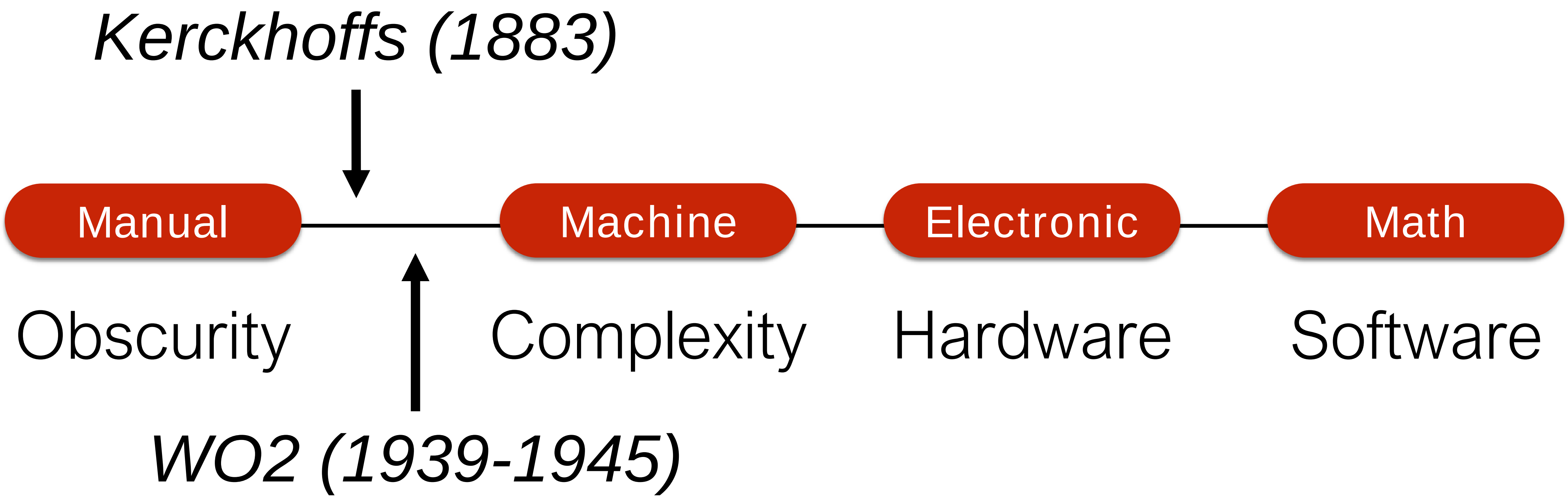
PvIB event

17 April 2018

Crypto Museum

cryptomuseum.com

Cryptography



Kerckhoffs (1883)

Manual — Machine — Electronic — Math

Obscurity

Complexity

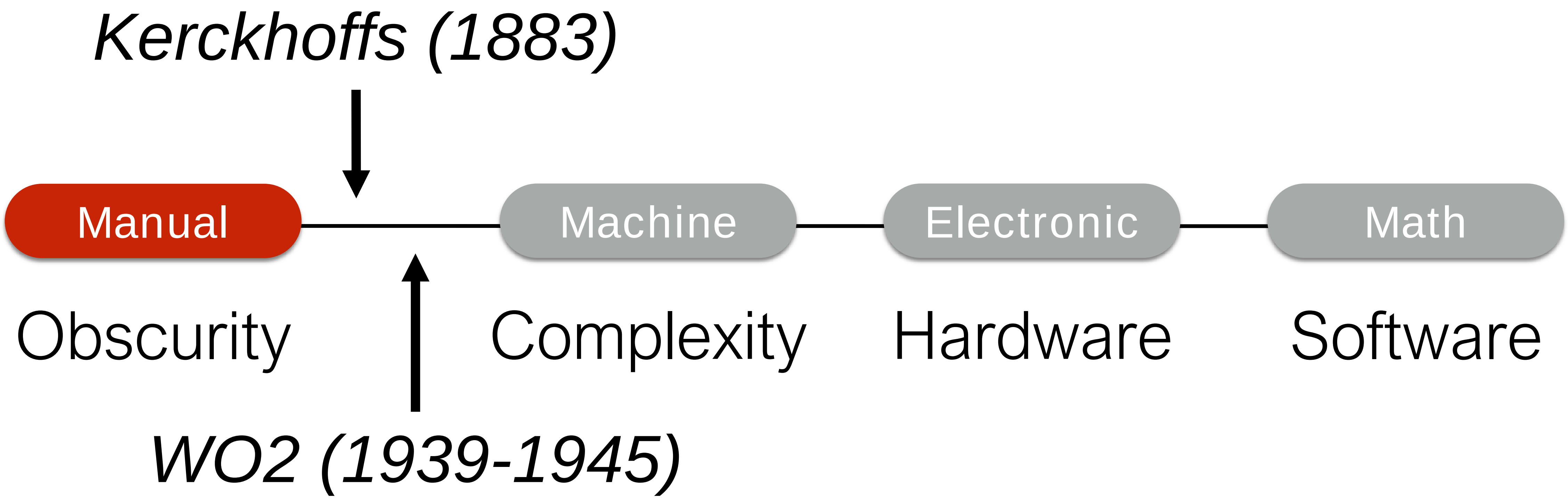
Hardware

Software

WO2 (1939-1945)

Crypto Museum
cryptomuseum.com

Cryptography



Kerckhoffs (1883)

Manual

Machine

Electronic

Math

Obscurity

Complexity

Hardware

Software

WO2 (1939-1945)

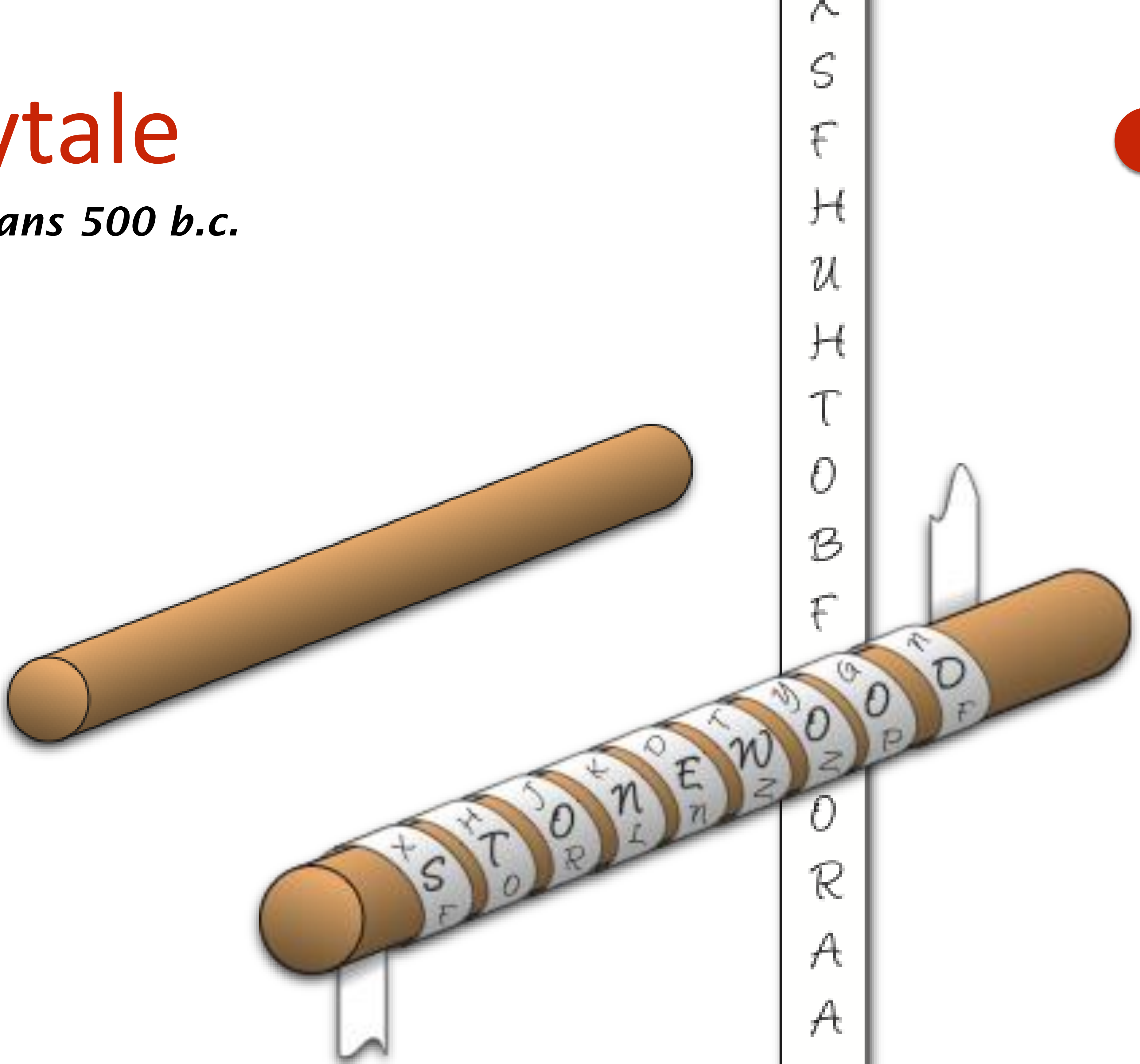
Crypto Museum
cryptomuseum.com

Security by Obscurity

Skytale

Spartans 500 b.c.

Manual

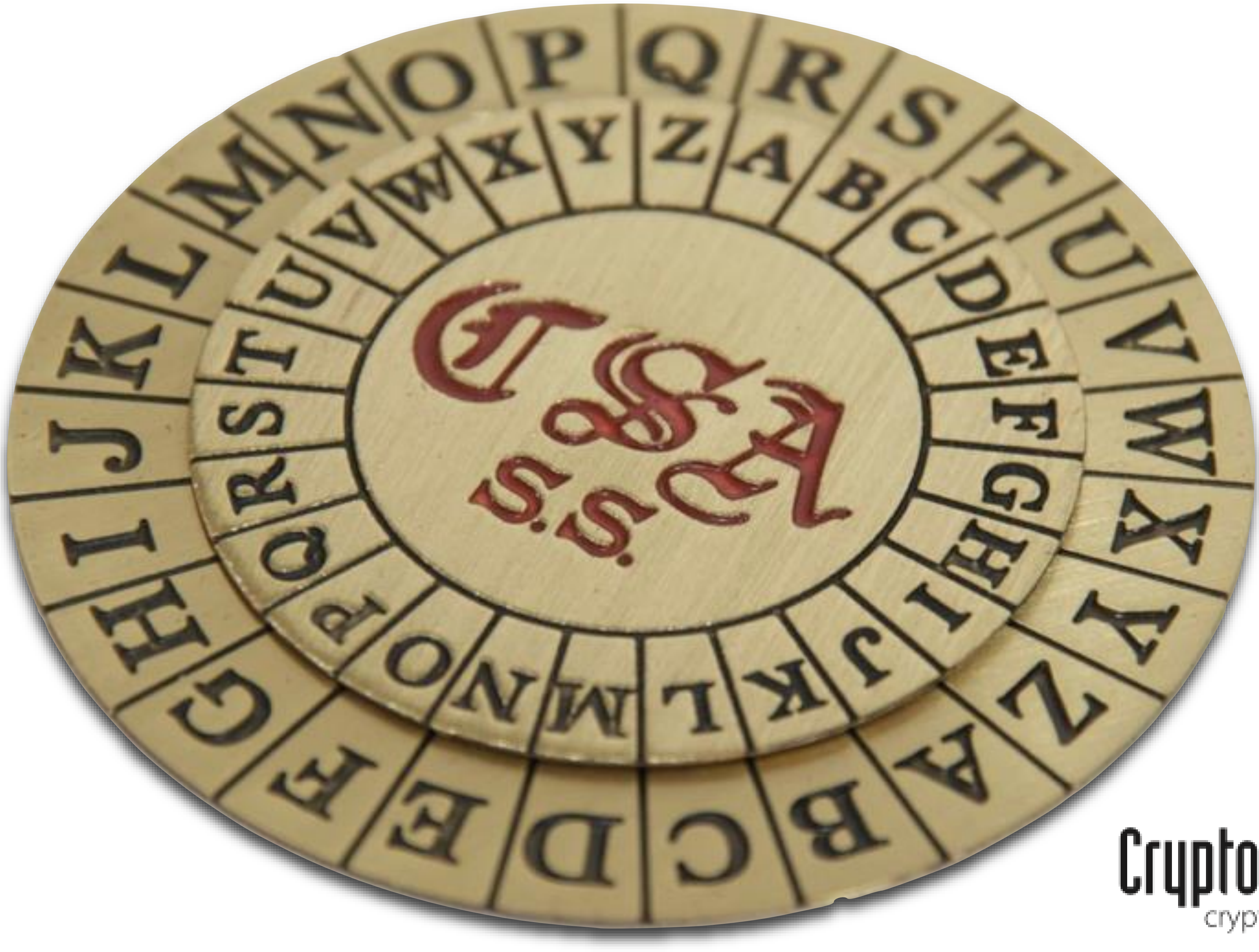


Crypto Museum
cryptomuseum.com

Caesar Cipher

Manual

Caesar, Alberti, Vigenere, American Civil War

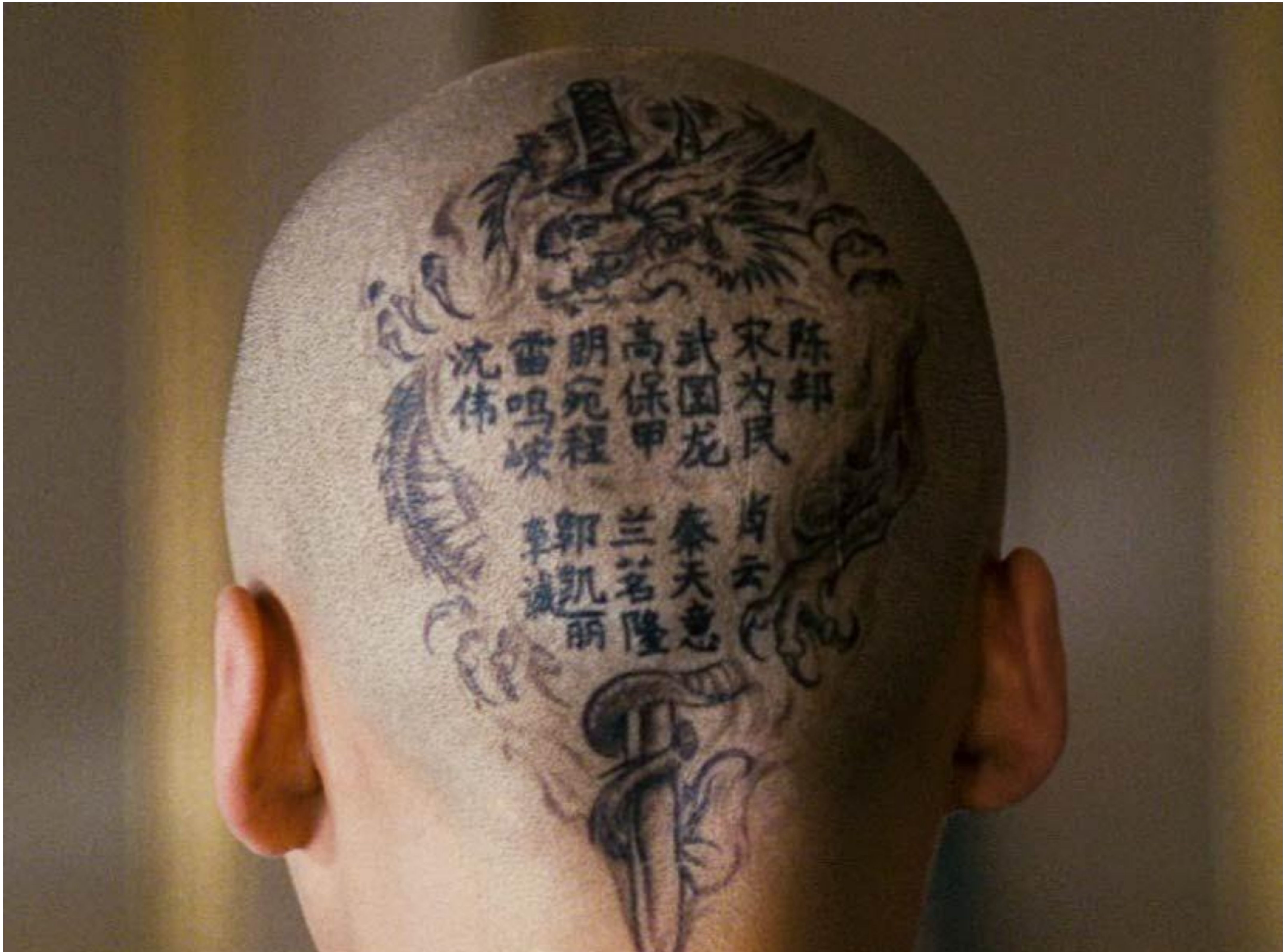


Crypto Museum
cryptomuseum.com

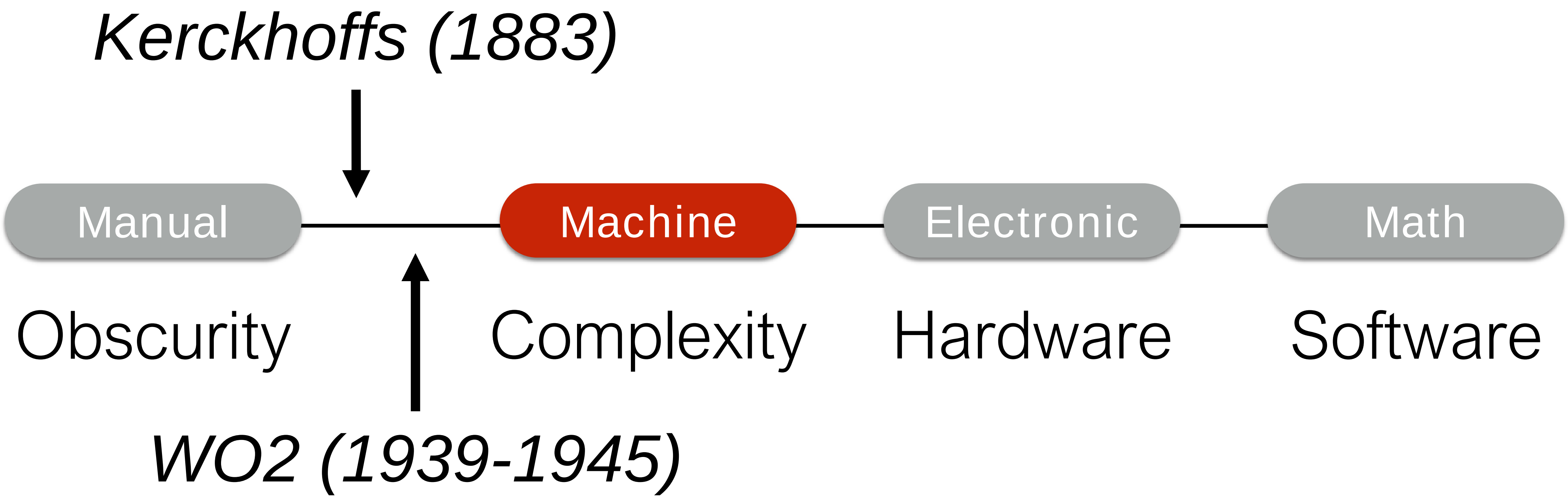
Tattoo

Manual

Hidden messages



Cryptography



Kerckhoffs (1883)

Manual

Obscurity

Machine

Complexity

Electronic

Hardware

Math

Software

WO2 (1939-1945)

Machine ciphers

- Security by complexity
- Kerckhoffs' principle(s)
- Rotor-based cipher machines
- Mechanical
- Electromechanical

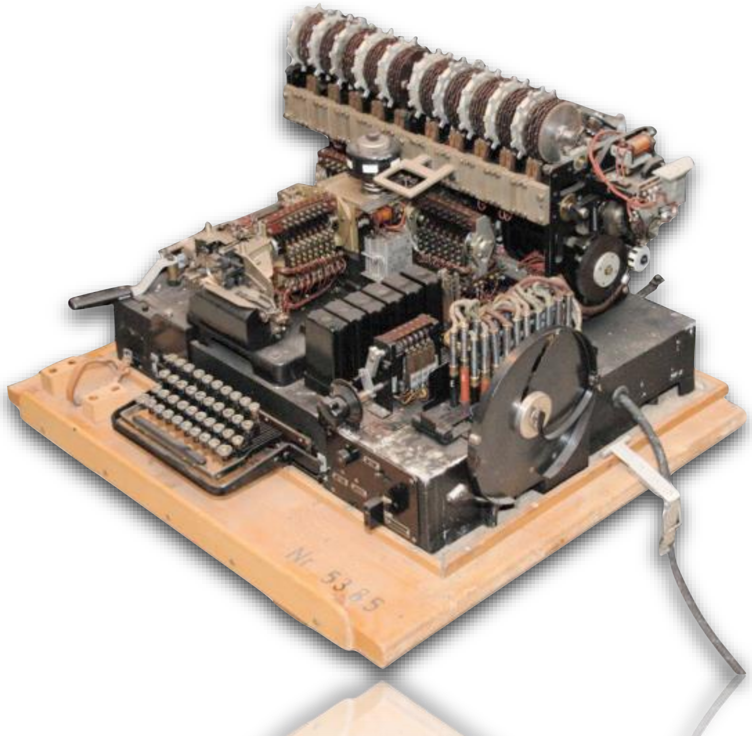
WWII

Machine

German Army

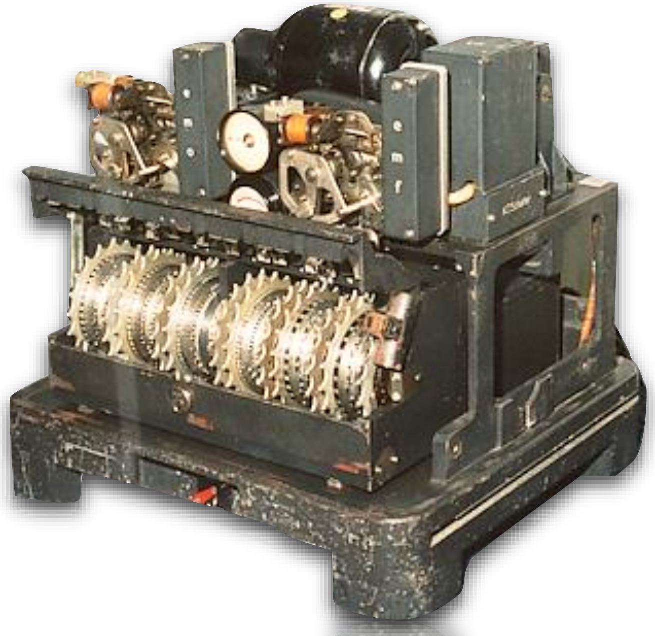
Enigma

20,000 units
Used over radio



Geheimschreiber
Siemens und Halse T52

1000 units
Mainly used over land lines



Lorenz
SZ-42

50 units
Used over land lines and radio

Crypto Museum
cryptomuseum.com

Enigma

Machine

1923 - 1975

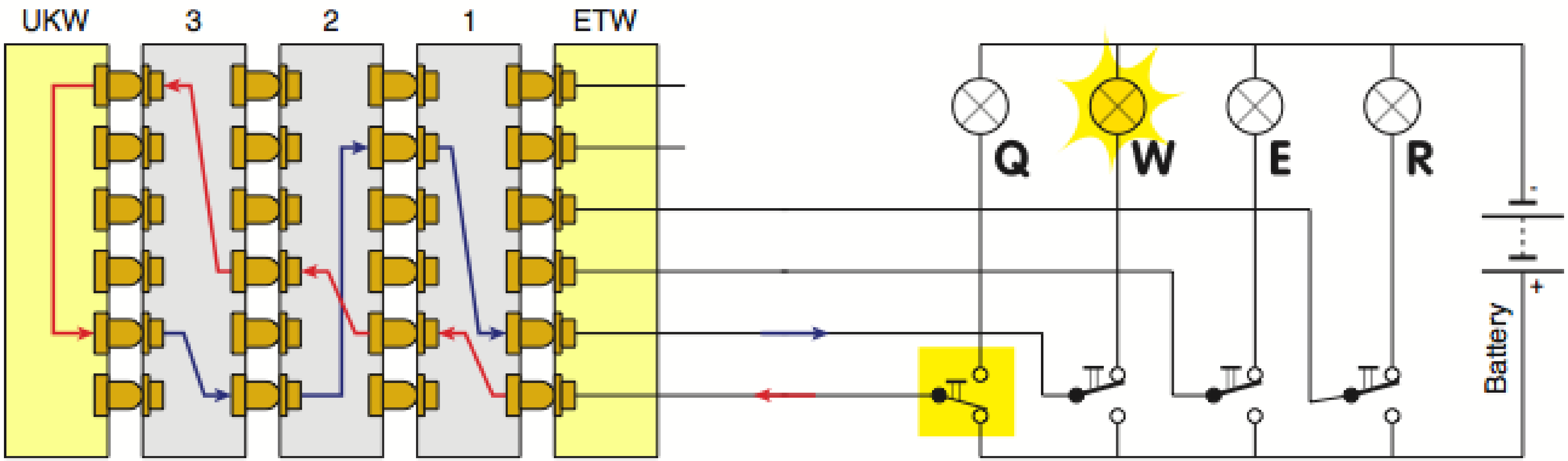
- Electromechanical
- 3 or 4 cipher wheels
- Broken during WWII
- Weaknesses
- Regular wheel stepping
- A letter can not become itself

Crypto Museum
cryptomuseum.com

Enigma

1923 - 1975

Machine

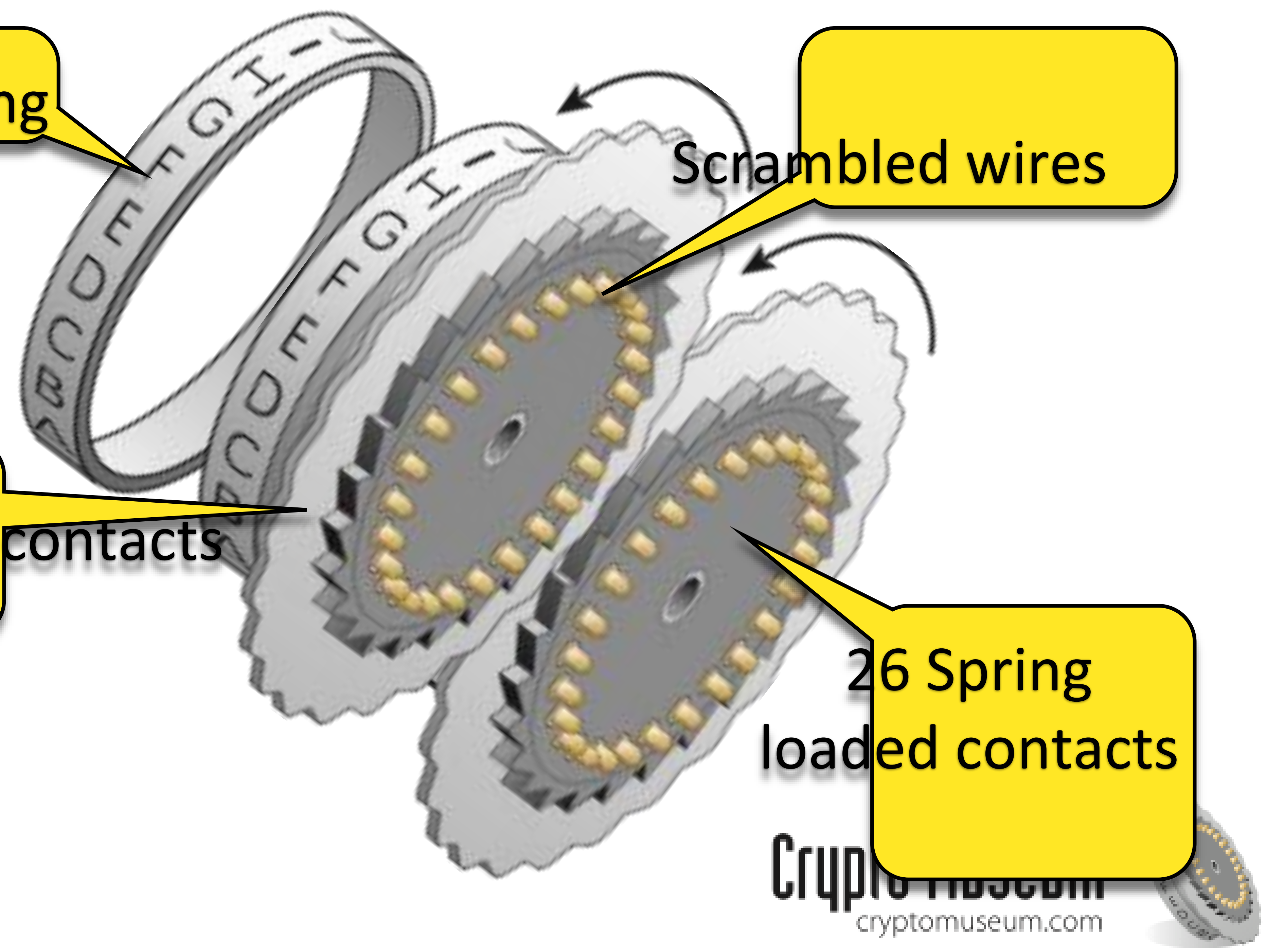


Crypto Museum
cryptomuseum.com

Enigma

1923 - 1975

Machine



Letter ring

Scrambled wires

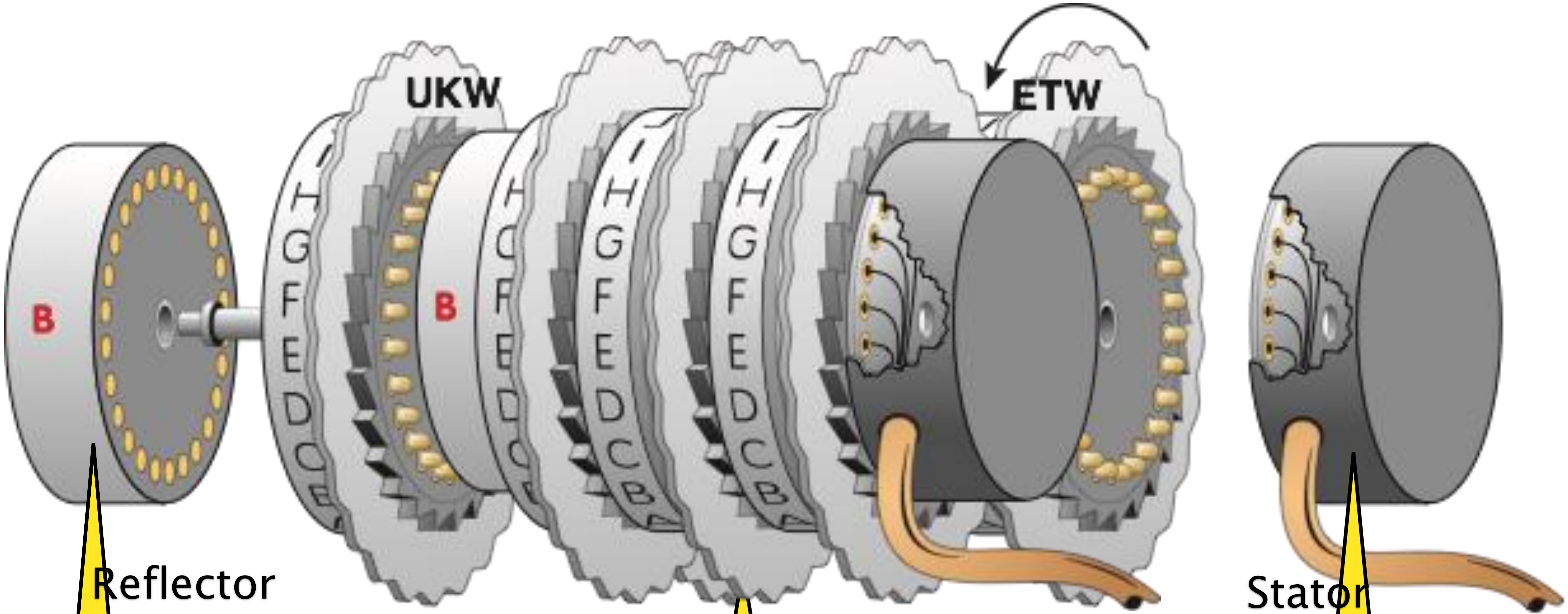
26 Fixed contacts

26 Spring loaded contacts

Enigma

1923 - 1975

Machine



Reflector
Umkehrwalze
UKW

Set of 3 wheels (rotors, *Walzen*)

Stator
Eintrittswalze
ETW

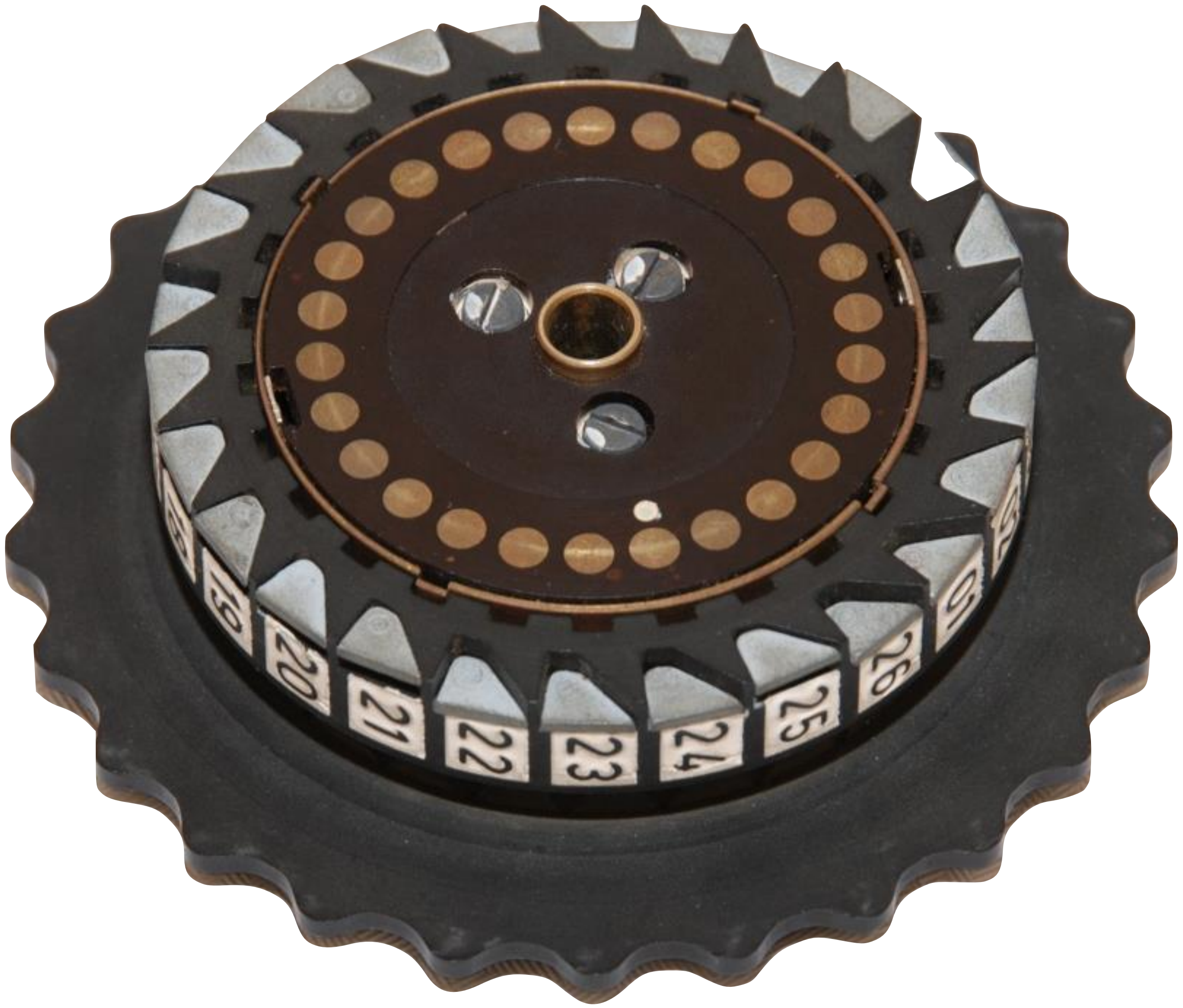
Crypto Museum
cryptomuseum.com

Enigma

Machine

Non-linearity - the Lückenfüllerwalze

- Programmable wheel
- Variable position and number of notches
- High degree of non-linearity
- Less predictable
- Long cipher period
- Too late to be of use
- All wheels taken by the American NSA



Crypto Museum
cryptomuseum.com

Fialka

Machine

USSR counterpart of Enigma

- 10 wheels
- Moving forward/backward
- Multiple notches
- Removable cores
- High degree of non-linearity
- No weaknesses like Enigma
- Used during Cold War
- Broken by NSA using Cray Computer

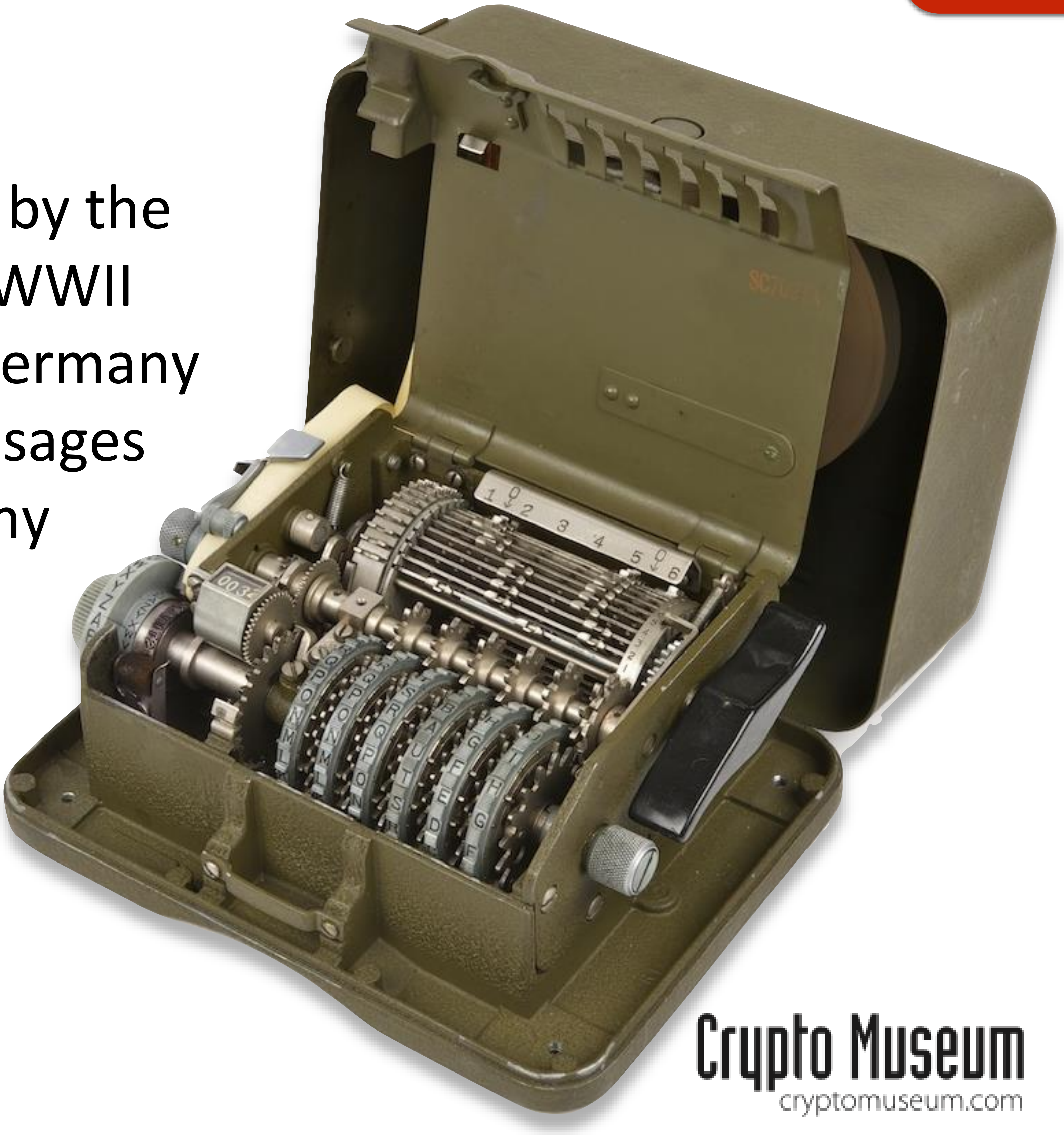
Crypto Museum
cryptomuseum.com

Hagelin

C-38 / M-209

Machine

- M-209 used by the USA during WWII
- Broken by Germany
- Tactical messages
- Used by many countries after WWII

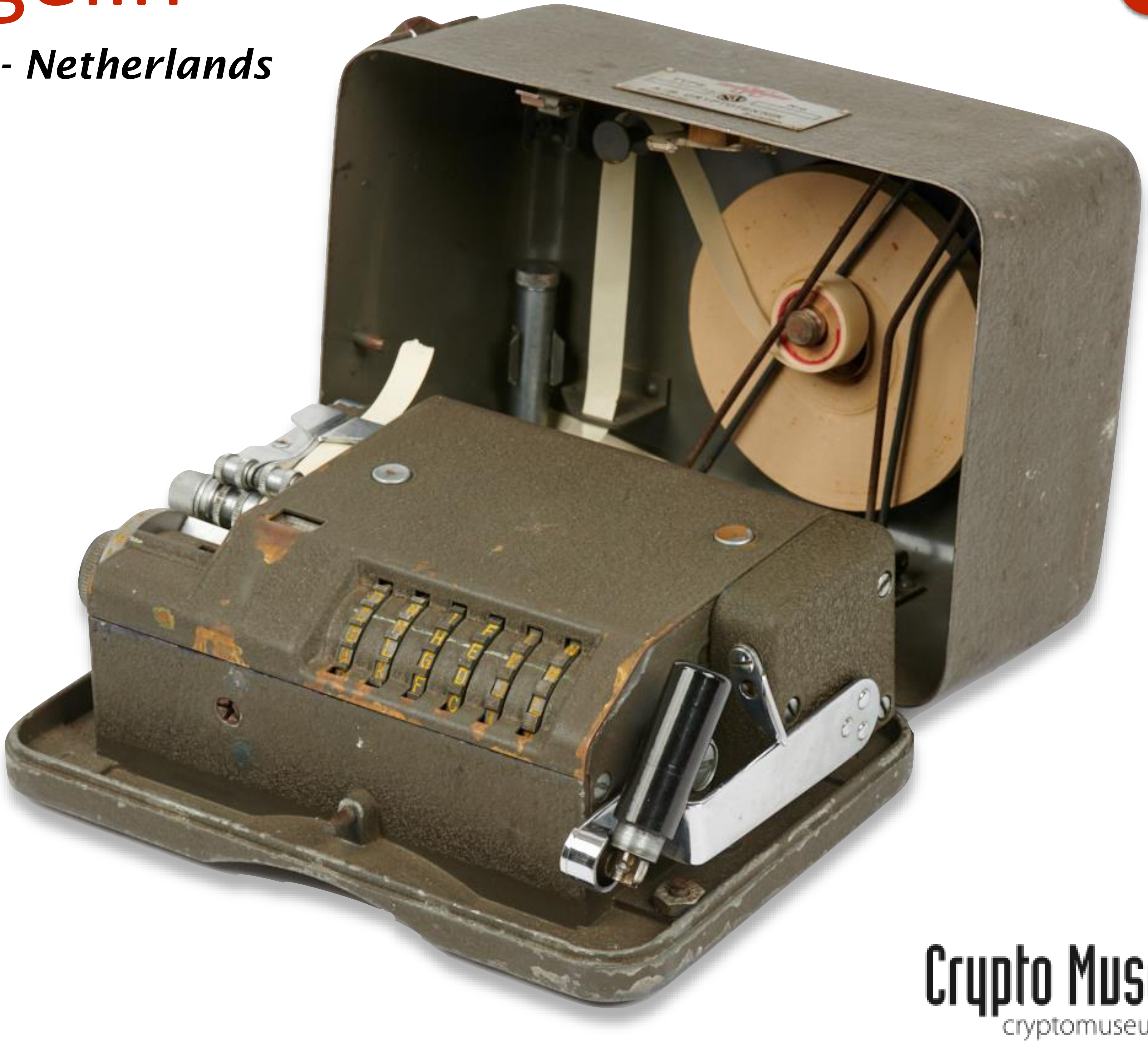


Crypto Museum
cryptomuseum.com

Hagelin

C-446 - Netherlands

Machine



Crypto Museum
cryptomuseum.com

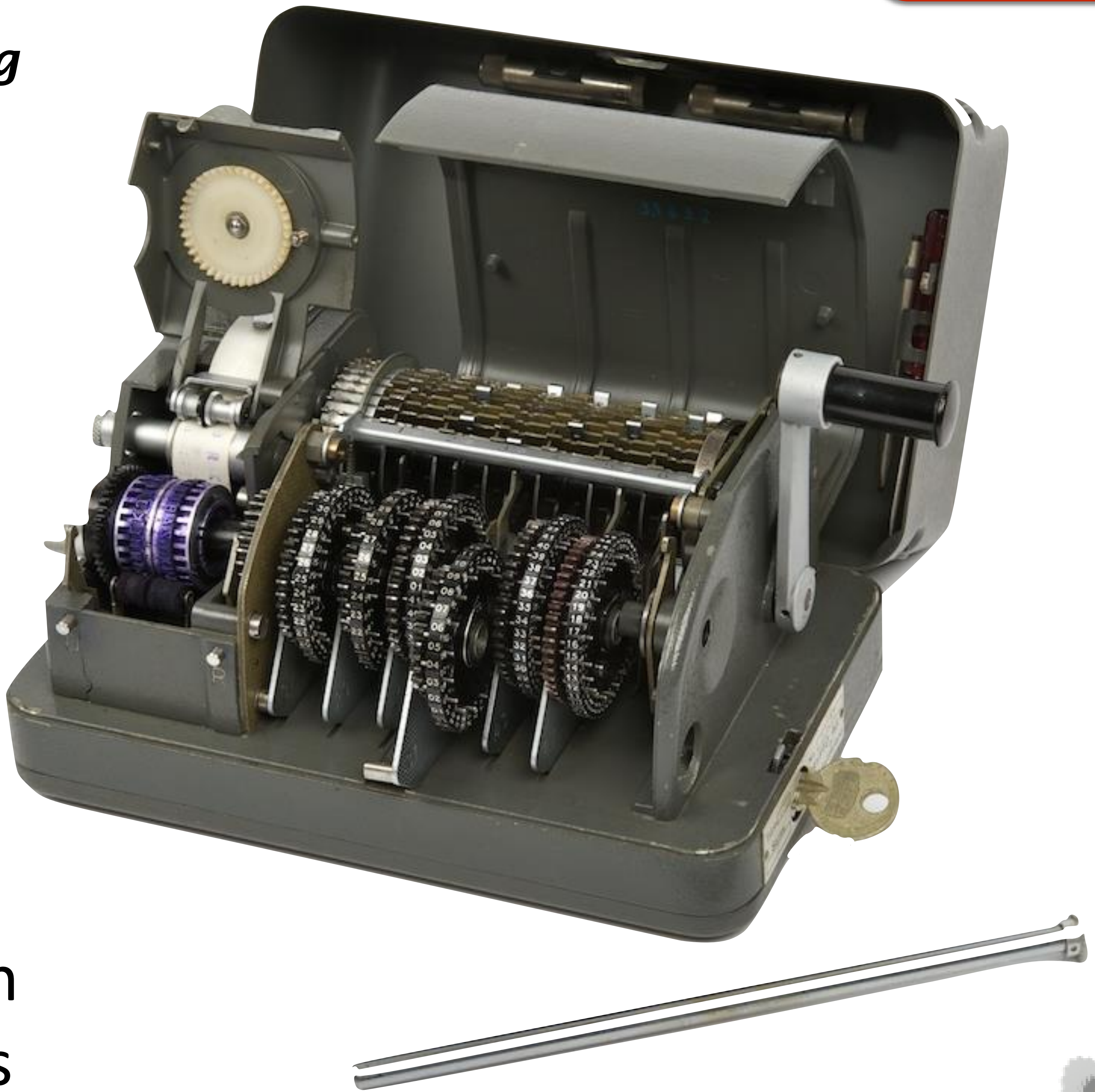
Hagelin

CX-52 - irregular stepping

Machine

- High degree of non-linearity
- Removable cipher wheels
- Irregular wheel stepping
- More difficult to break

- NSA intervention
- Friedman papers

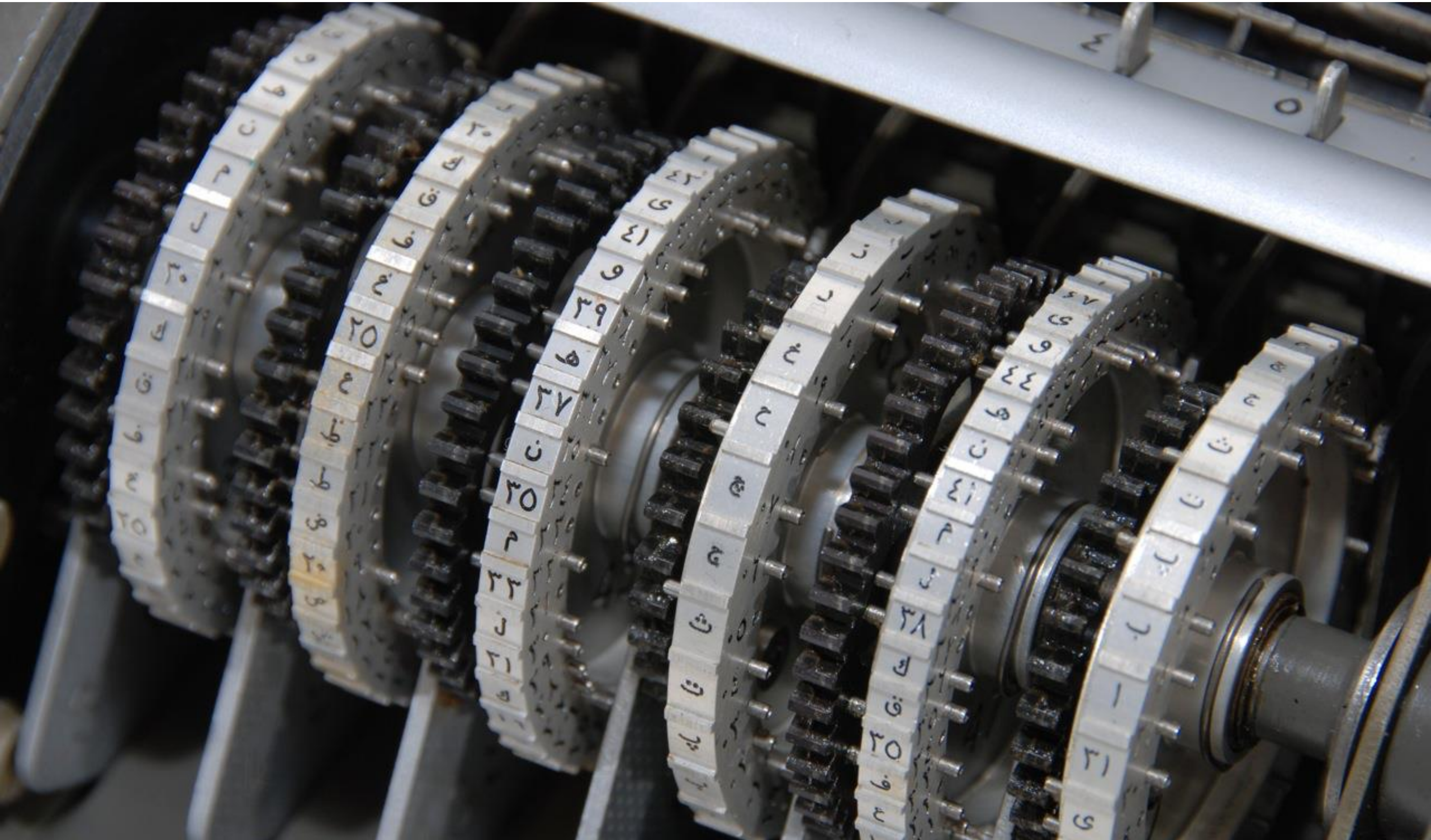


Crypto Museum
cryptomuseum.com

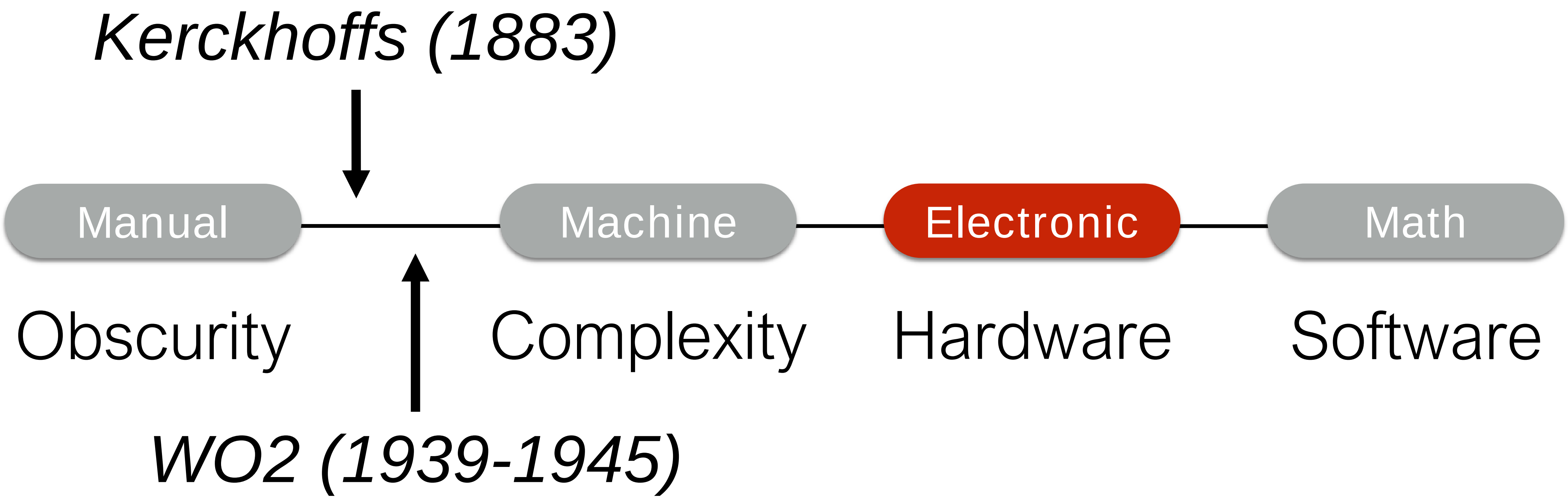
Hagelin

Machine

CX-52 - Arab version



Cryptography



Kerckhoffs (1883)

Manual — Machine — Electronic — Math

Obscurity

Complexity

Hardware

Software

WO2 (1939-1945)

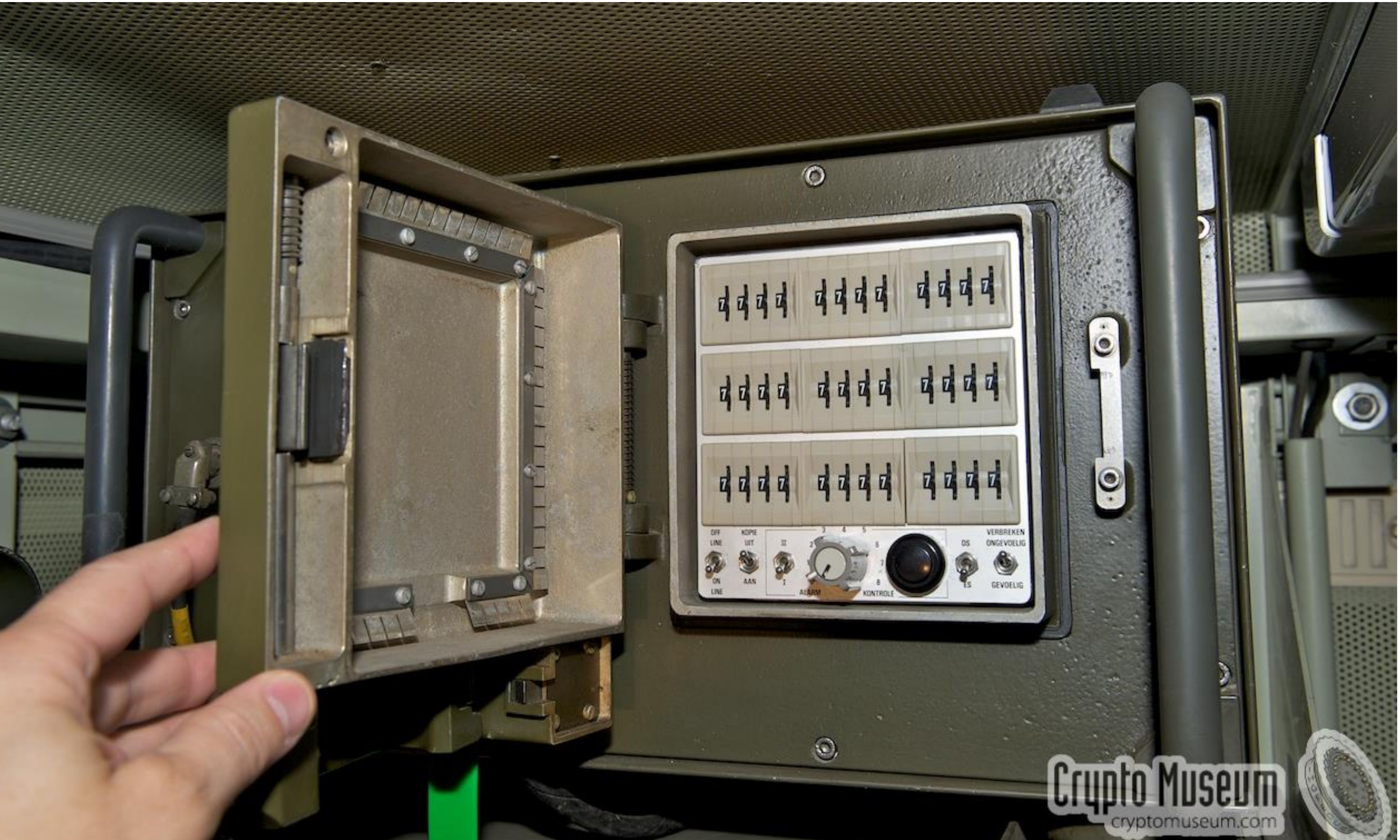
Hardware ciphers

- Easier to build
- More reliable
- Easier maintenance
- Easier to update/modify
- Easier in operation
- Public/secret algorithms
- Complexity and additional obscurity

Ecolex-X

Electronic

Wheels replaced by non-linear shift-registers

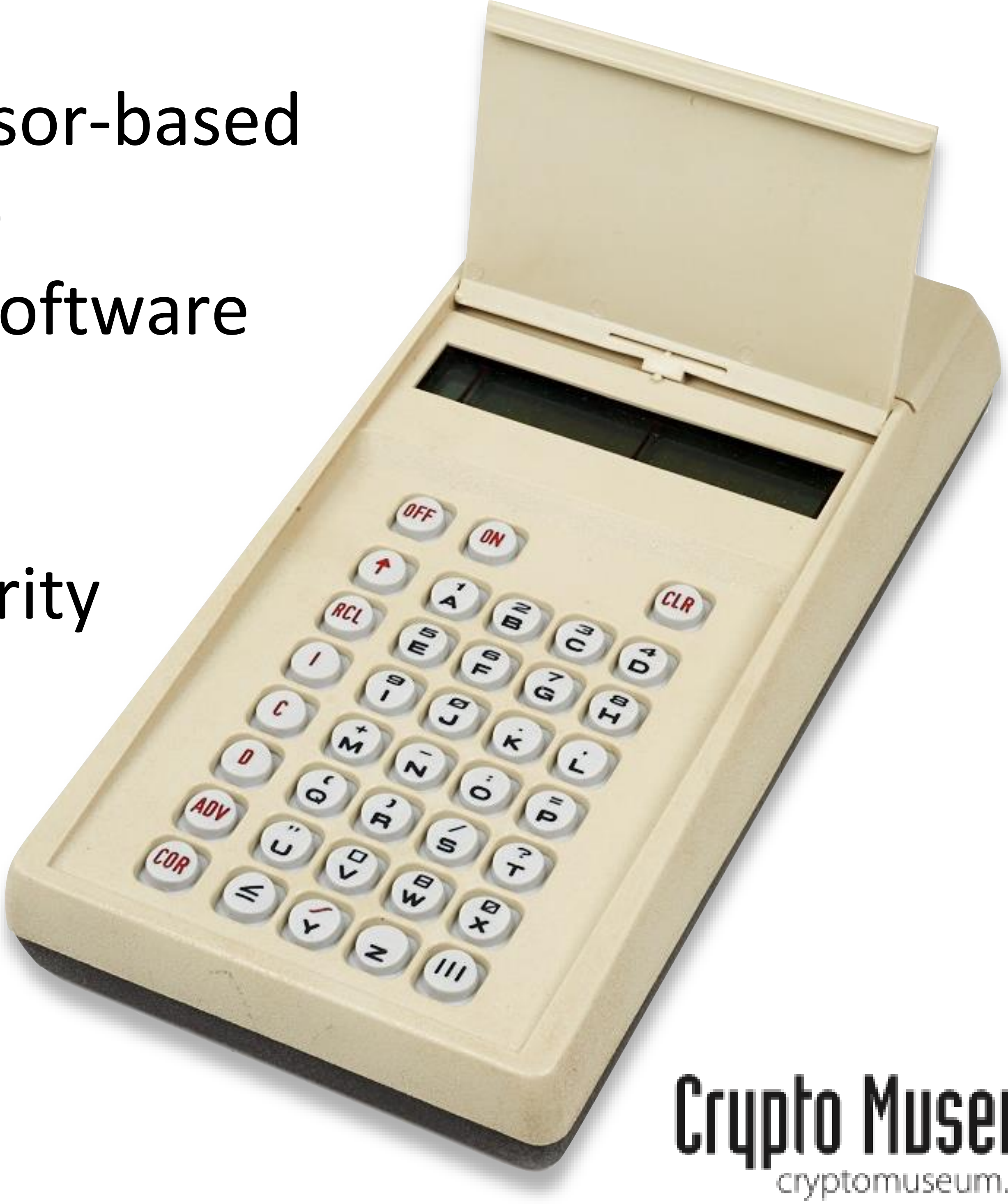


Hagelin

HC-520

Electronic

- First microprocessor-based encryption device
- Wheels made in software
- Low-power
- Easy to use
- High level of security
- Secret algorithm

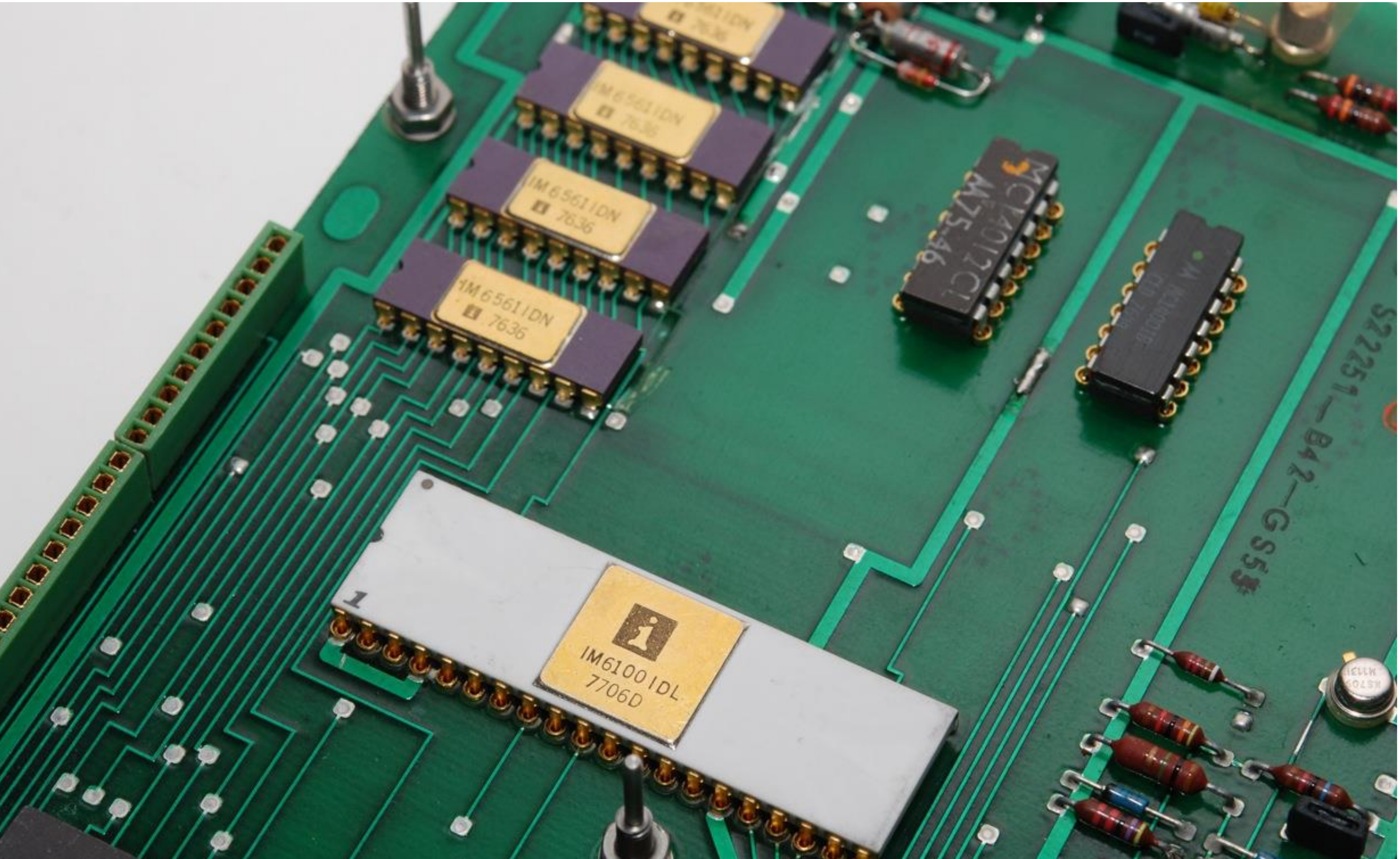


Crypto Museum
cryptomuseum.com

Hagelin

HC-520

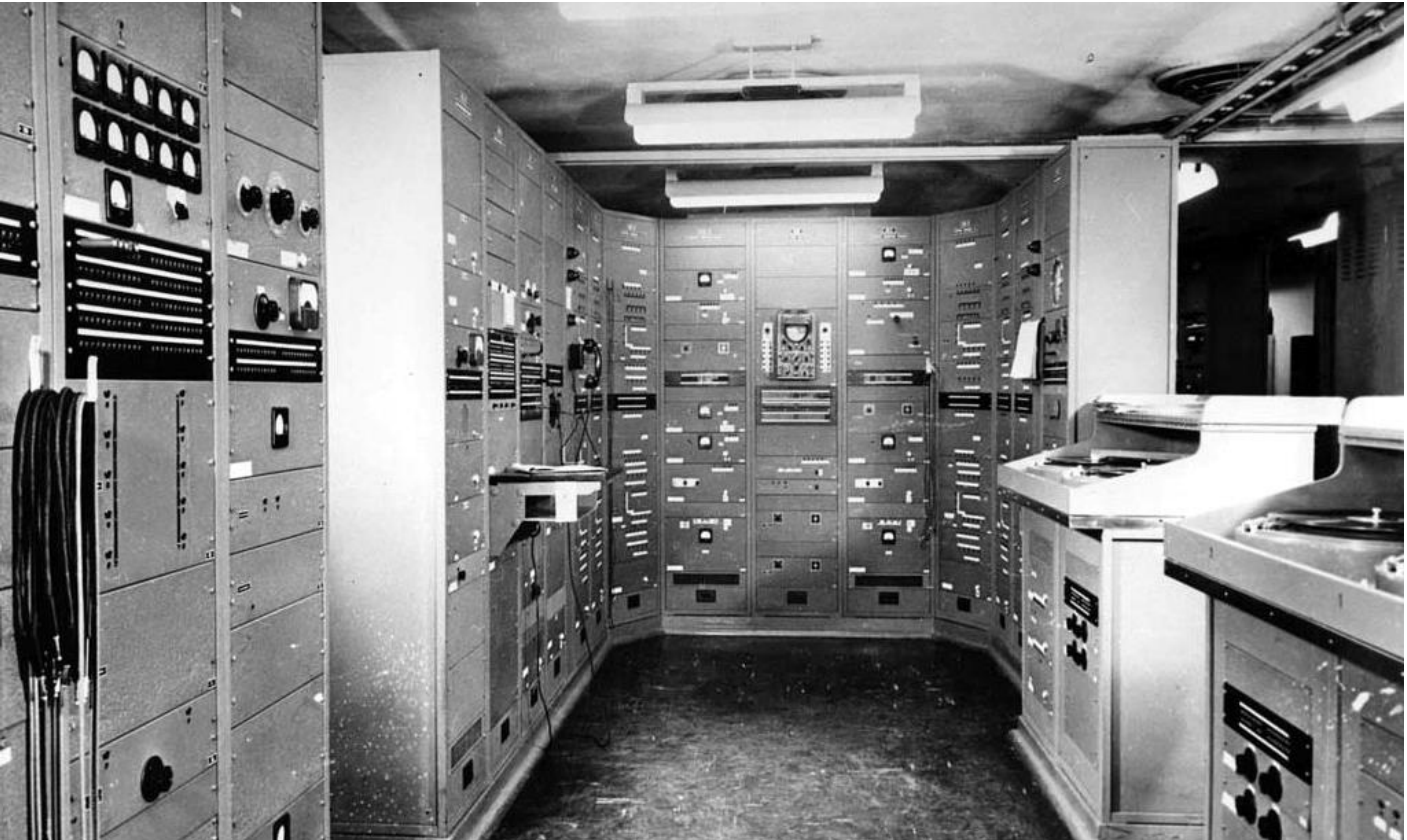
Electronic



SIGSALY

Electronic

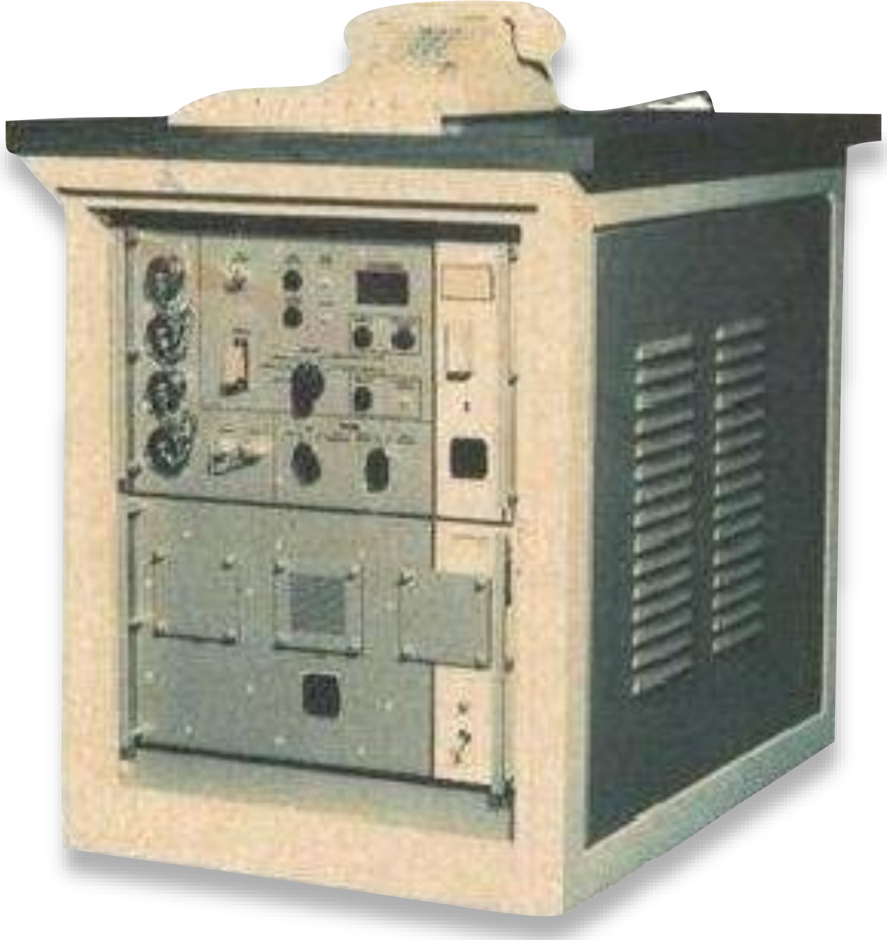
Secure speech during WWII

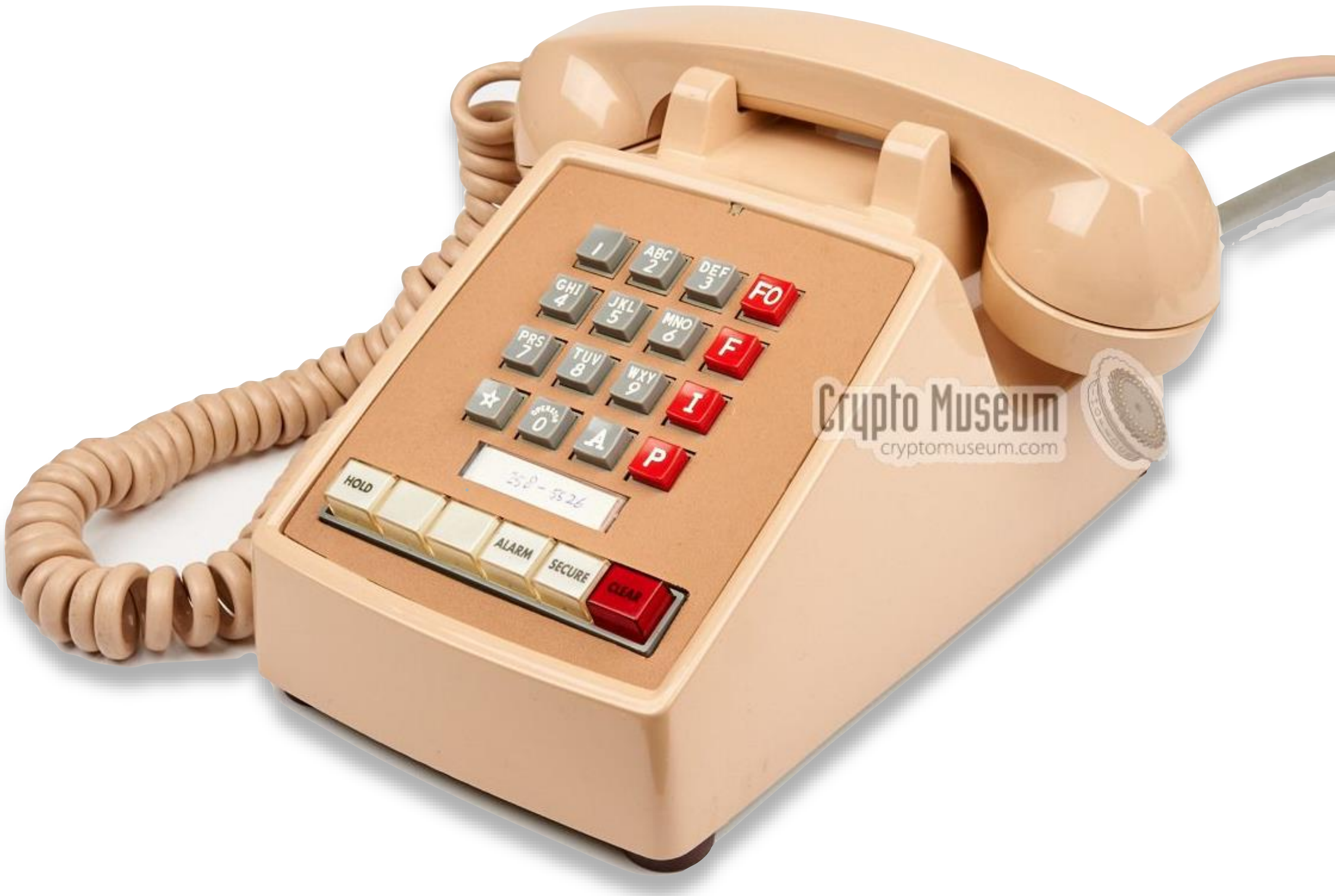


STU-I

Electronic

Speech encryption - secret SAVILLE algorithm



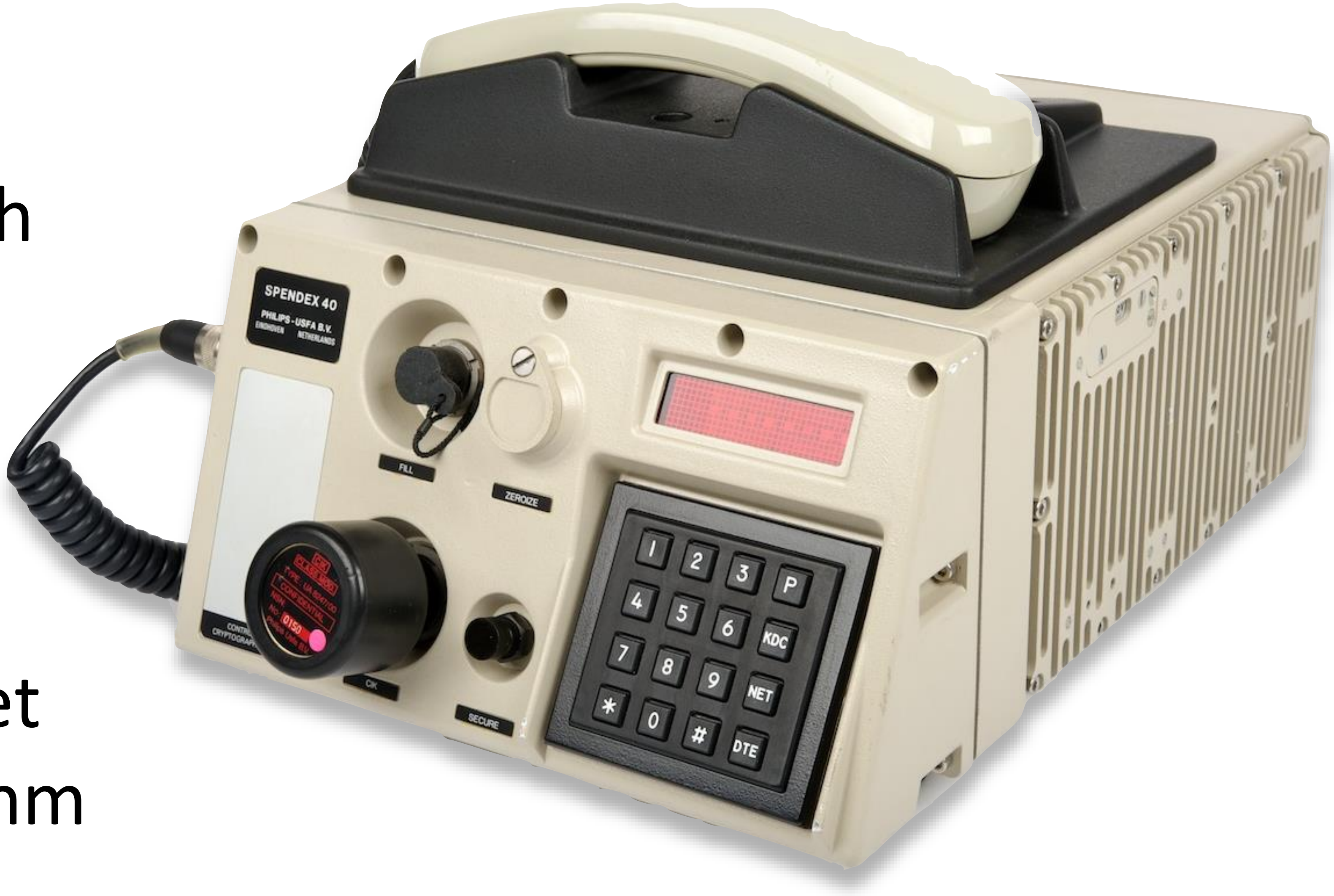


Spendex 40

Electronic

Secret SAVILLE algorithm

- Philips (1981)
- Compatible with STU-I
- Much smaller
- Permission from NSA to use highly secret SAVILLE algorithm

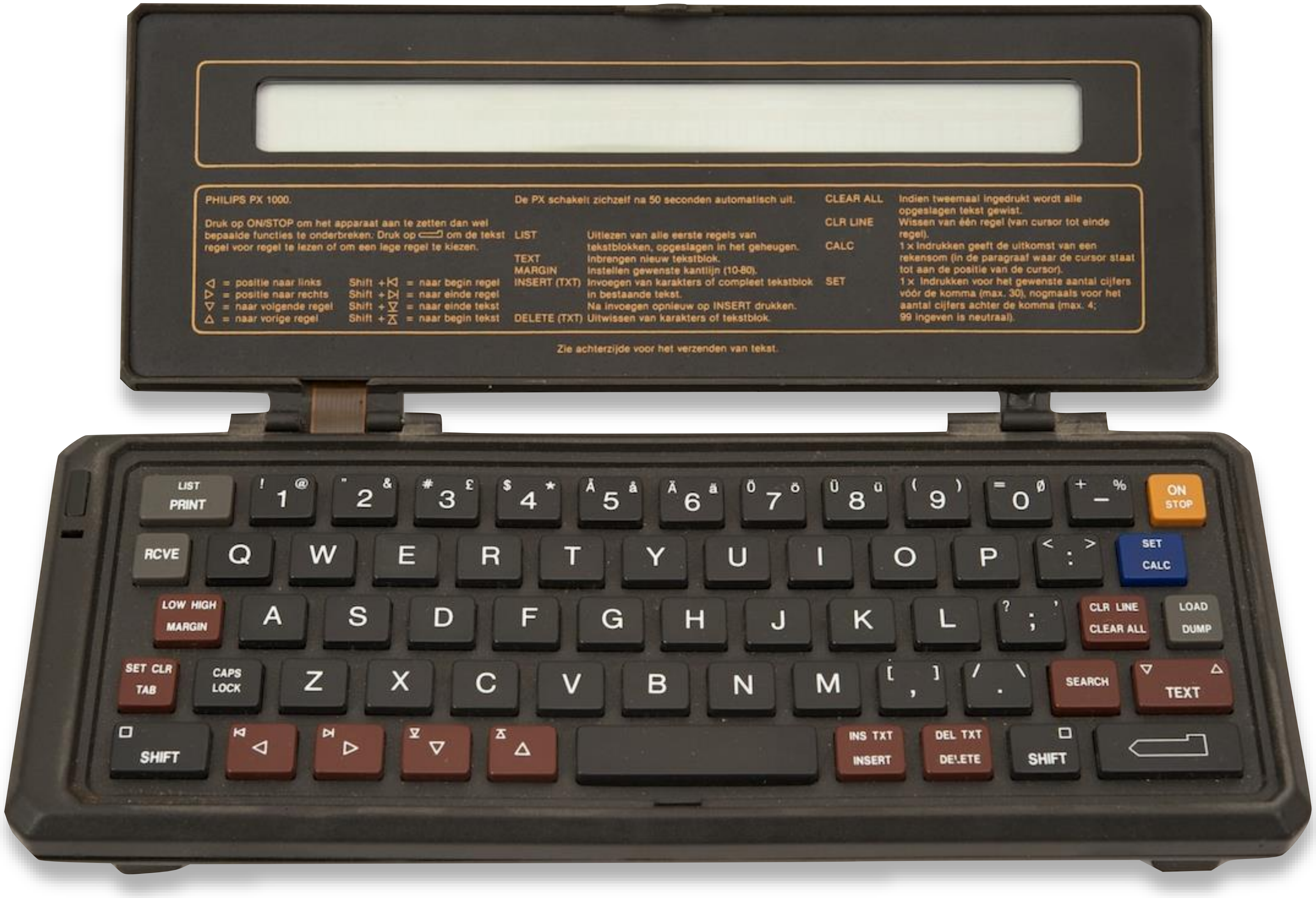


Crypto Museum
cryptomuseum.com

PX-1000

Electronic

1983 - Data Encryption Standard (DES)



PHILIPS PX 1000.

Druk op ON/STOP om het apparaat aan te zetten dan wel bepaalde functies te onderbreken. Druk op ⏎ om de tekst regel voor regel te lezen of om een lege regel te kiezen.

◁ = positie naar links
▷ = positie naar rechts
▽ = naar volgende regel
△ = naar vorige regel

Shift +⏮ = naar begin regel
Shift +⏭ = naar einde regel
Shift +▽ = naar einde tekst
Shift +△ = naar begin tekst

De PX schakelt zichzelf na 50 seconden automatisch uit.

LIST Uitlezen van alle eerste regels van tekstblokken, opgeslagen in het geheugen.
TEXT Inbrengen nieuw tekstblok.
MARGIN Instellen gewenste kantlijn (10-80).
INSERT (TXT) Invoegen van karakters of compleet tekstblok in bestaande tekst.
Na invoegen opnieuw op INSERT drukken.
DELETE (TXT) Uitwissen van karakters of tekstblok.

CLEAR ALL Indien tweemaal ingedrukt wordt alle opgeslagen tekst gewist.
CLR LINE Wissen van één regel (van cursor tot einde regel).
CALC 1 × Indrukken geeft de uitkomst van een rekensom (in de paragraaf waar de cursor staat tot aan de positie van de cursor).
SET 1 × Indrukken voor het gewenste aantal cijfers vóór de komma (max. 30), nogmaals voor het aantal cijfers achter de komma (max. 4; 99 ingeven is neutraal).

Zie achterzijde voor het verzenden van tekst.

Crypto Museum
cryptomuseum.com

PX-1000

Electronic

1983 - Data Encryption Standard (DES)

- DES publicly available
- Promoted by Philips, Siemens, Alcatel, Ericsson and others
- Affordable
- Secure
- Used by ANC (Mandela)

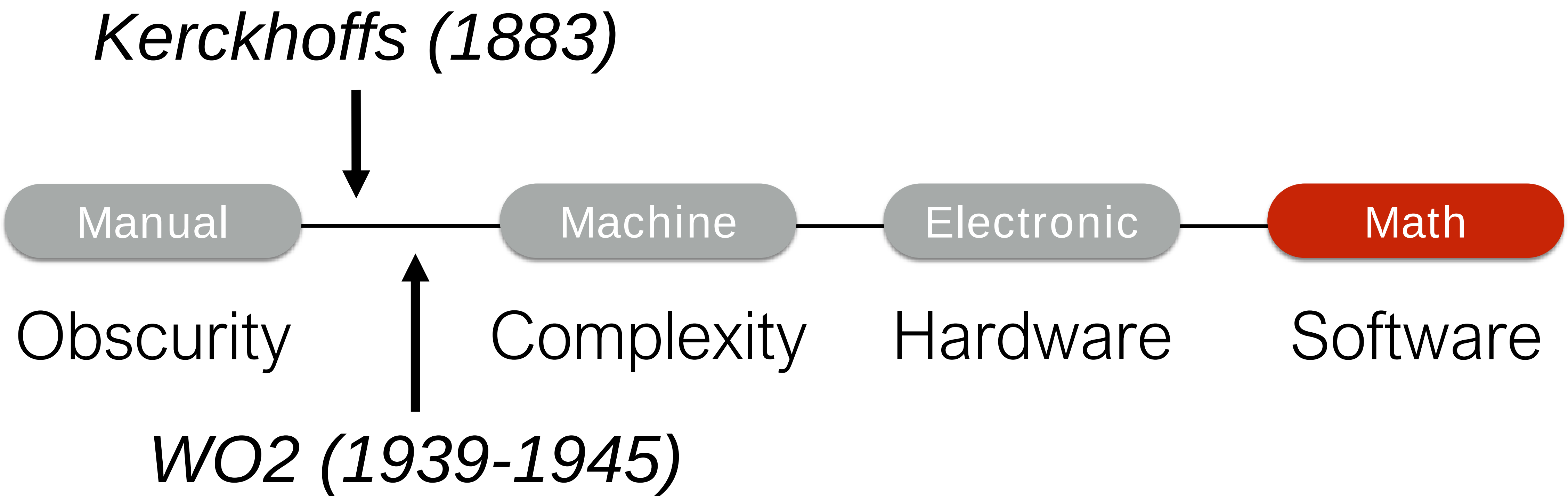
- Intervention by the NSA
- Less secure ‘government friendly’ algorithm

Barbie

Caesar cipher

Electronic

Cryptography



Kerckhoffs (1883)

Manual

Machine

Electronic

Math

Obscurity

Complexity

Hardware

Software

WO2 (1939-1945)

Crypto Museum
cryptomuseum.com

Software ciphers

- Public Key Encryption (PKE)
- Public algorithms: DES, 3DES, AES, etc.
- Government: public & secret algorithms
- Personal Computers (PCs)

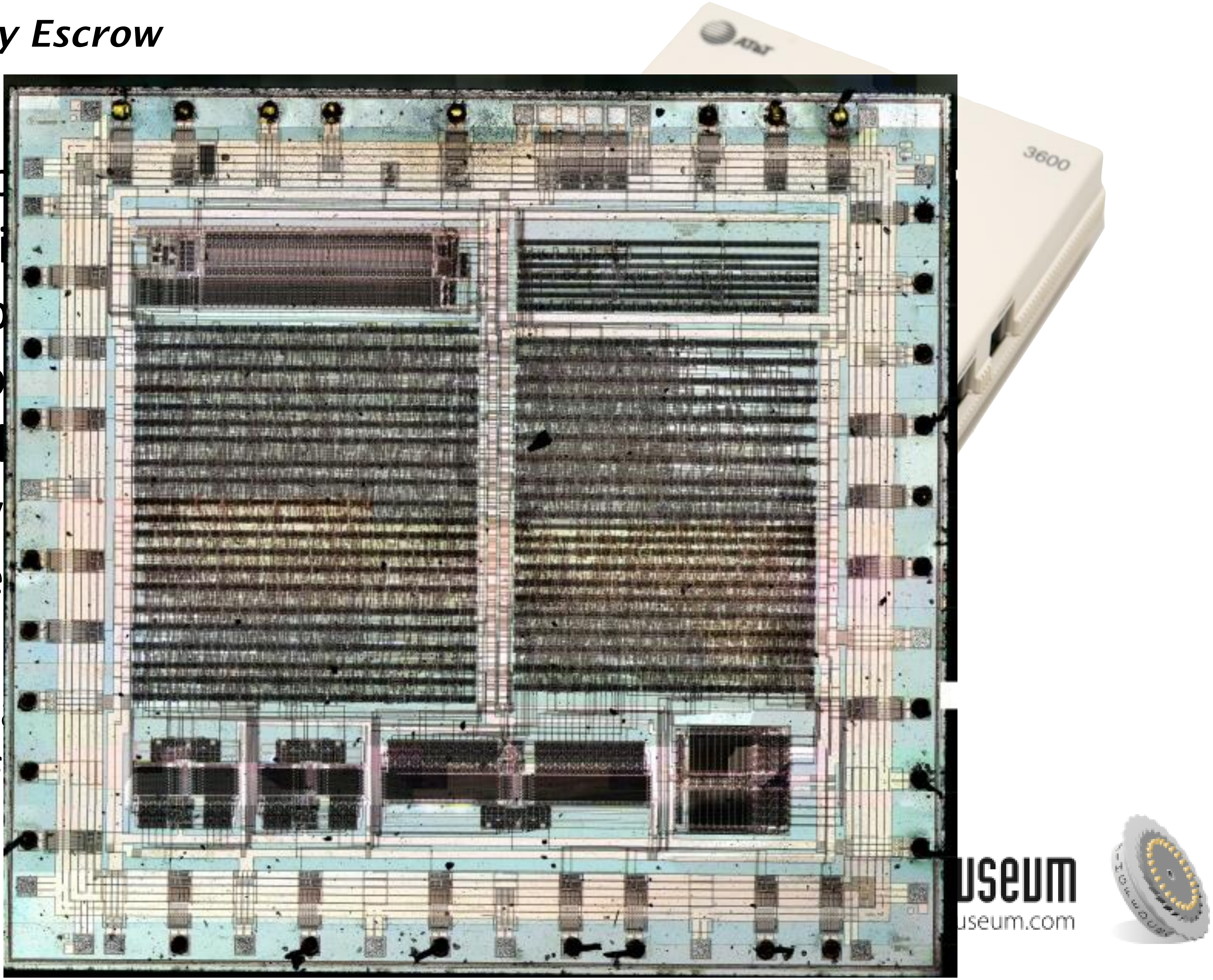
- Secure?
- Weaknesses?
- Side-channel attacks
- Platform manipulation
- Key Escrow

Clipper Chip

1993 - Key Escrow

Math

- Skip
- Initi
- Imp
  Clip
- Higl
- Key
  in e
  to t
- We
- Def



PvIB event

17 April 2018

Crypto Museum

cryptomuseum.com

One-Time Pad

OTP

The unbreakable code

One-Time Pad

OTP

The unbreakable code

PvIB event

17 April 2018

Crypto Museum

cryptomuseum.com