# MYTHOS ENIGMA ROTORMASCHINEN 1920 - 1970

Präsentation Enigma Tag – Enter Technikwelten Solothurn
22. Februar 2025 Dominik Landwehr

# ZUM AUTOR DOMINIK LANDWEHR

Kulturwissenschafter, Buchautor, Journalist.
Publikationen zu Technikgeschichte, Kryptologie, Kultur- und Regionalgeschichte.

Dissertatopm: Mythos Enigma. Die Chiffriermaschine als Medien- und Sammlerobjekt. Bielefeld 2007. Online als Open Access

27 merkwürdige Geschichten aus der Schweiz. Winterthur 2024. Online als Open Access

Online Zugang via:

www.sternenjaeger.ch


# MYTHOS ENIGMA

War Enigma die einzige Rotor-Chiffriermaschine?

War Enigma die beste Rotor-Chiffriermaschine?

Warum wurde Enigma zum Mythos?

# CHIFFRIERUNG IM ERSTEN WELTKRIEG

Im Ersten Weltkrieg gab es noch keine Maschinen für die Chiffrierung:

Stattdessen arbeitete man mit so genannten Handverfahren

**Chiffrierscheiben**

**Codebücher**

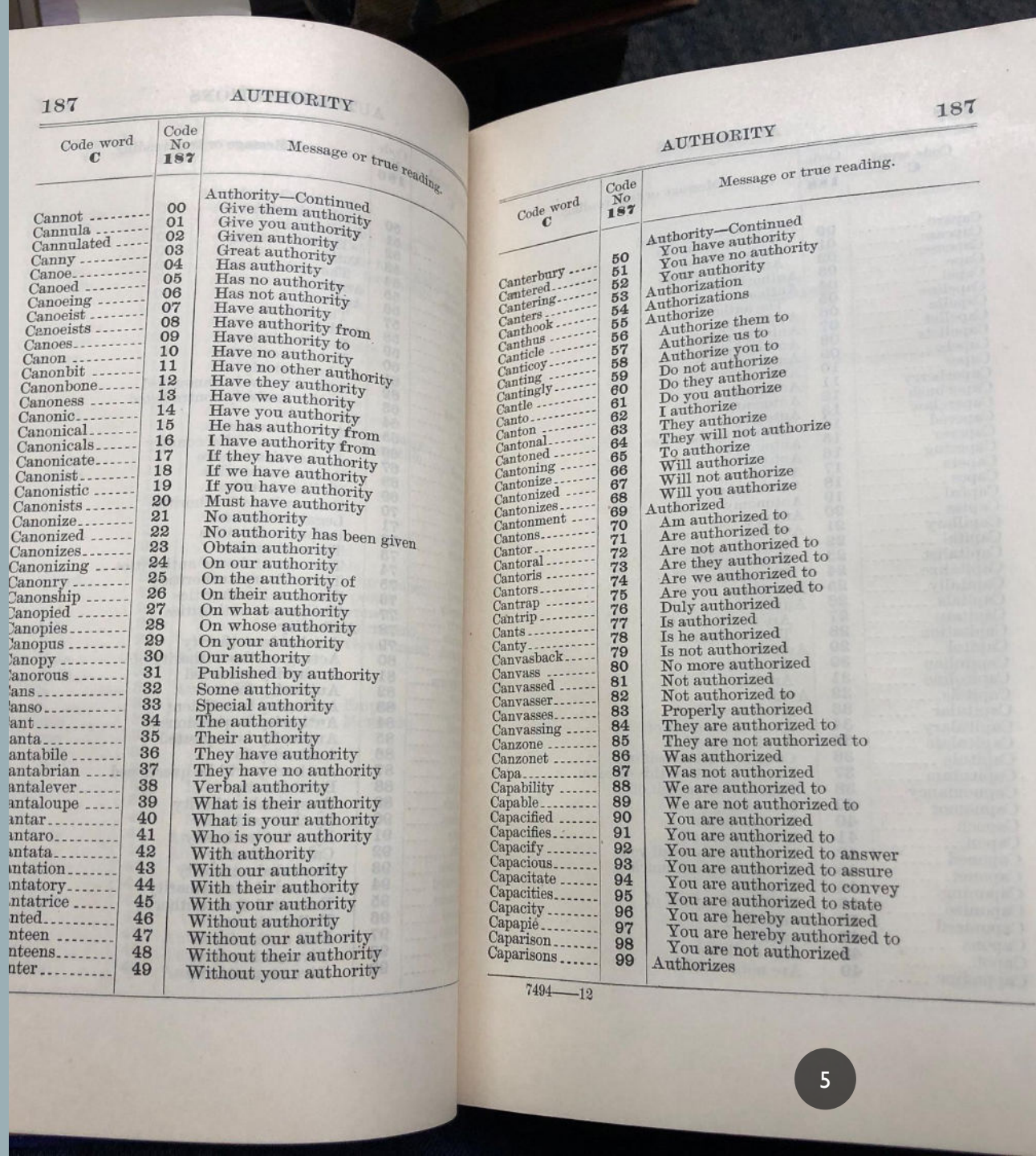
# CHIFFRIERUNG ZU BEGINN DES 20.JAHRHUNDERTS

Im Ersten Weltkrieg gab es noch keine Maschinen für die Chiffrierung:

Stattdessen arbeitete man mit so genannten Handverfahren

**Chiffrierscheiben**

**Codebücher**



187 AUTHORITY

| Code word C | Code No 187 | Message or true reading. |
|---|---|---|
| | | Authority—Continued |
| Cannot | 00 | Give them authority |
| Cannula | 01 | Give you authority |
| Cannulated | 02 | Given authority |
| Canny | 03 | Great authority |
| Canoe | 04 | Has authority |
| Canoed | 05 | Has no authority |
| Canoeing | 06 | Has not authority |
| Canoeist | 07 | Have authority |
| Canoeists | 08 | Have authority from |
| Canoes | 09 | Have authority to |
| Canon | 10 | Have no authority |
| Canonbit | 11 | Have no other authority |
| Canonbone | 12 | Have they authority |
| Canoness | 13 | Have we authority |
| Canonic | 14 | Have you authority |
| Canonical | 15 | He has authority from |
| Canonicals | 16 | I have authority from |
| Canonicate | 17 | If they have authority |
| Canonist | 18 | If we have authority |
| Canonistic | 19 | If you have authority |
| Canonists | 20 | Must have authority |
| Canonize | 21 | No authority |
| Canonized | 22 | No authority has been given |
| Canonizes | 23 | Obtain authority |
| Canonizing | 24 | On our authority |
| Canonry | 25 | On the authority of |
| Canonship | 26 | On their authority |
| Canopied | 27 | On what authority |
| Canopies | 28 | On whose authority |
| Canopus | 29 | On your authority |
| Canopy | 30 | Our authority |
| Canorous | 31 | Published by authority |
| Cans | 32 | Some authority |
| Canso | 33 | Special authority |
| Cant | 34 | The authority |
| Canta | 35 | Their authority |
| Cantabile | 36 | They have authority |
| Cantabrian | 37 | They have no authority |
| Cantalever | 38 | Verbal authority |
| Cantaloupe | 39 | What is their authority |
| Cantar | 40 | What is your authority |
| Cantaro | 41 | Who is your authority |
| Cantata | 42 | With authority |
| Cantation | 43 | With our authority |
| Cantatory | 44 | With their authority |
| Cantatrice | 45 | With your authority |
| Canted | 46 | Without authority |
| Canteen | 47 | Without our authority |
| Canteens | 48 | Without their authority |
| Canter | 49 | Without your authority |

AUTHORITY 187

| Code word C | Code No 187 | Message or true reading. |
|---|---|---|
| | | Authority—Continued |
| Canterbury | 50 | You have authority |
| Cantered | 51 | You have no authority |
| Cantering | 52 | Your authority |
| Canters | 53 | Authorization |
| Canthook | 54 | Authorizations |
| Canthus | 55 | Authorize |
| Canticle | 56 | Authorize them to |
| Canticoy | 57 | Authorize us to |
| Canting | 58 | Authorize you to |
| Cantingly | 59 | Do not authorize |
| Cantle | 60 | Do they authorize |
| Canto | 61 | Do you authorize |
| Canton | 62 | I authorize |
| Cantonal | 63 | They authorize |
| Cantoned | 64 | They will not authorize |
| Cantoning | 65 | To authorize |
| Cantonize | 66 | Will authorize |
| Cantonized | 67 | Will not authorize |
| Cantonizes | 68 | Will you authorize |
| Cantonment | 69 | Authorized |
| Cantons | 70 | Am authorized to |
| Cantor | 71 | Are authorized to |
| Cantoral | 72 | Are not authorized to |
| Cantoris | 73 | Are they authorized to |
| Cantors | 74 | Are we authorized to |
| Cantrap | 75 | Are you authorized to |
| Cantrip | 76 | Duly authorized |
| Cants | 77 | Is authorized |
| Canty | 78 | Is he authorized |
| Canvasback | 79 | Is not authorized |
| Canvass | 80 | No more authorized |
| Canvassed | 81 | Not authorized |
| Canvasser | 82 | Not authorized to |
| Canvasses | 83 | Properly authorized |
| Canvassing | 84 | They are authorized to |
| Canzone | 85 | They are not authorized to |
| Canzonet | 86 | Was authorized |
| Capa | 87 | Was not authorized |
| Capability | 88 | We are authorized to |
| Capable | 89 | We are not authorized to |
| Capacified | 90 | You are authorized |
| Capacifies | 91 | You are authorized to |
| Capacify | 92 | You are authorized to answer |
| Capacious | 93 | You are authorized to assure |
| Capacitate | 94 | You are authorized to convey |
| Capacities | 95 | You are authorized to state |
| Capacity | 96 | You are hereby authorized |
| Capapié | 97 | You are hereby authorized to |
| Caparison | 98 | You are not authorized |
| Caparisons | 99 | Authorizes |

7494—12

# DIE KRYHA
# DAS ERSTE CHIFFRIERGERÄT

Entwickelt von Alexander von Kryha (1891-1955)

Idee: Chiffrierscheibe mit Federantrieb

Ab 1926 auf dem Markt

Einfach:  Friedman knackte sie 1933 in 2:41 Stunden

# ROTORMASCHINE VON EDWARD HEBERN

Der Amerikaner Edward Hebern (1869 – 1952) war einer der Erfinder der Rotormaschine

Erfunden 1917, Patent 1921

Maschine war unsicher.

# DIE ROTORMASCHINE AUS SCHWEDEN

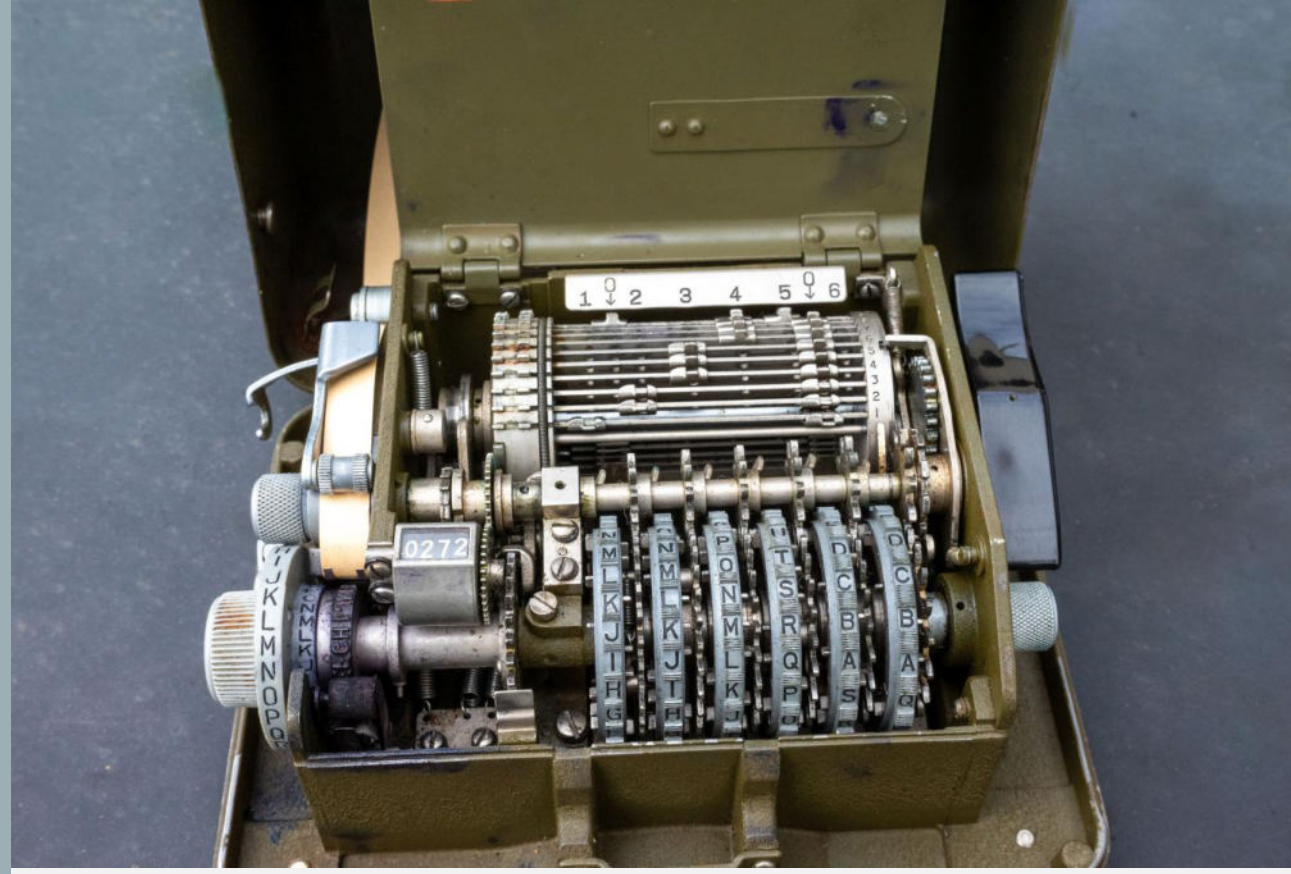
A.B.Cryptograph. Inhaber Arvid Damm

Boris Hagelin, später Gründer der Crypto AG verbesserte sie

# BORIS HAGELIN UND SEINE MASCHINEN

Boris Hagelin entwickelte Ende der 1930er Jahre die C-Serie. Darunter die C-38

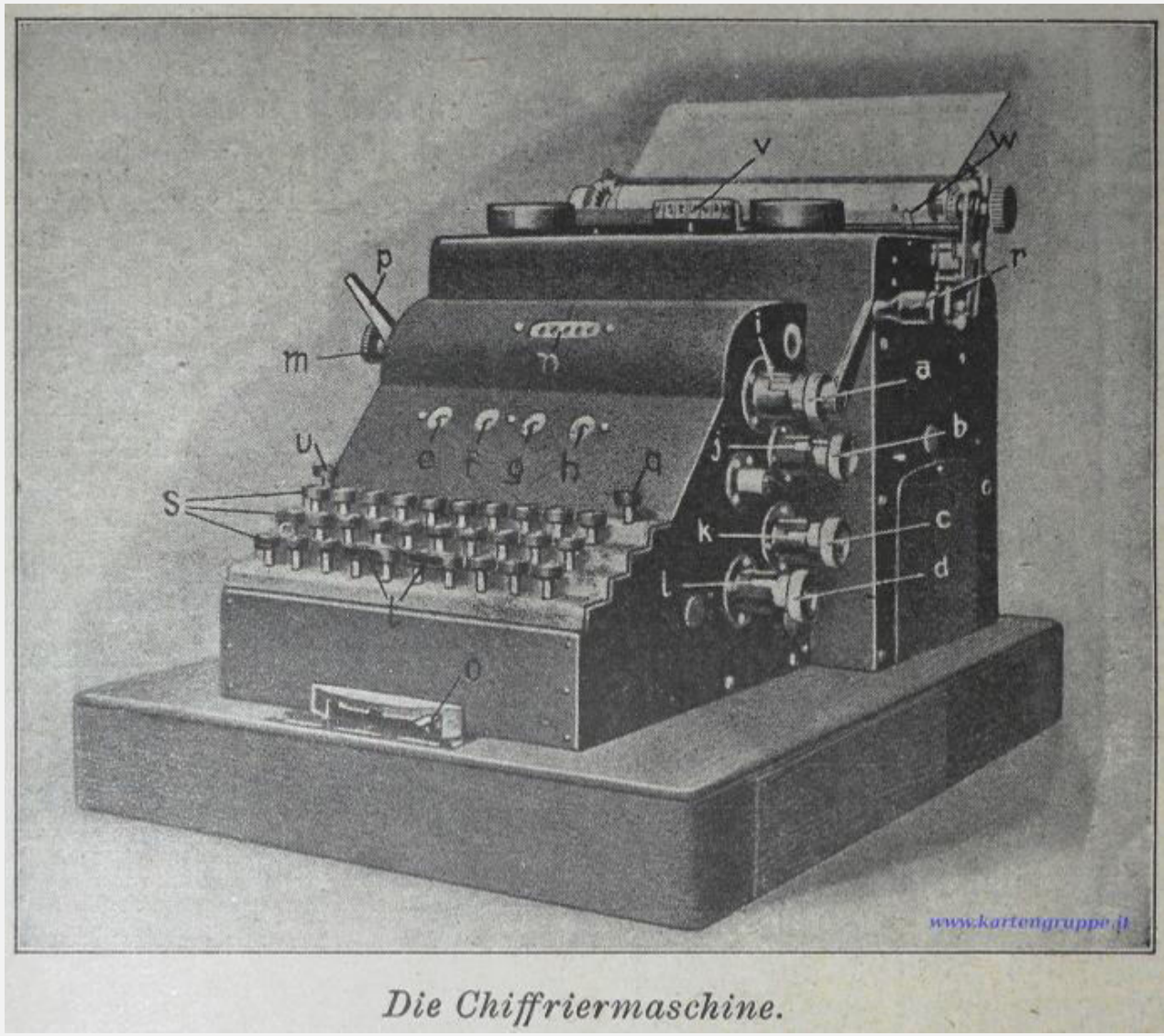
USA kaufte Lizenz und baute davon 140 000 Stück



# DIE ENIGMA FAMILIE

# DIE ENIGMA

Patent 1918 angemeldet
1923/24 kamen die ersten Maschinen auf den Markt

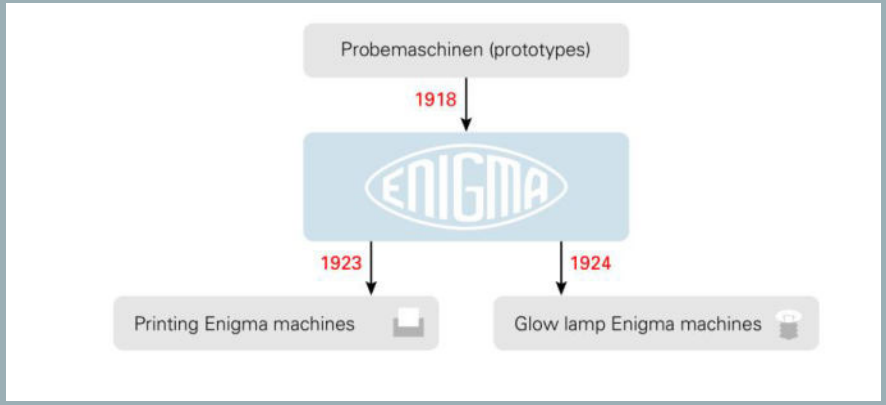


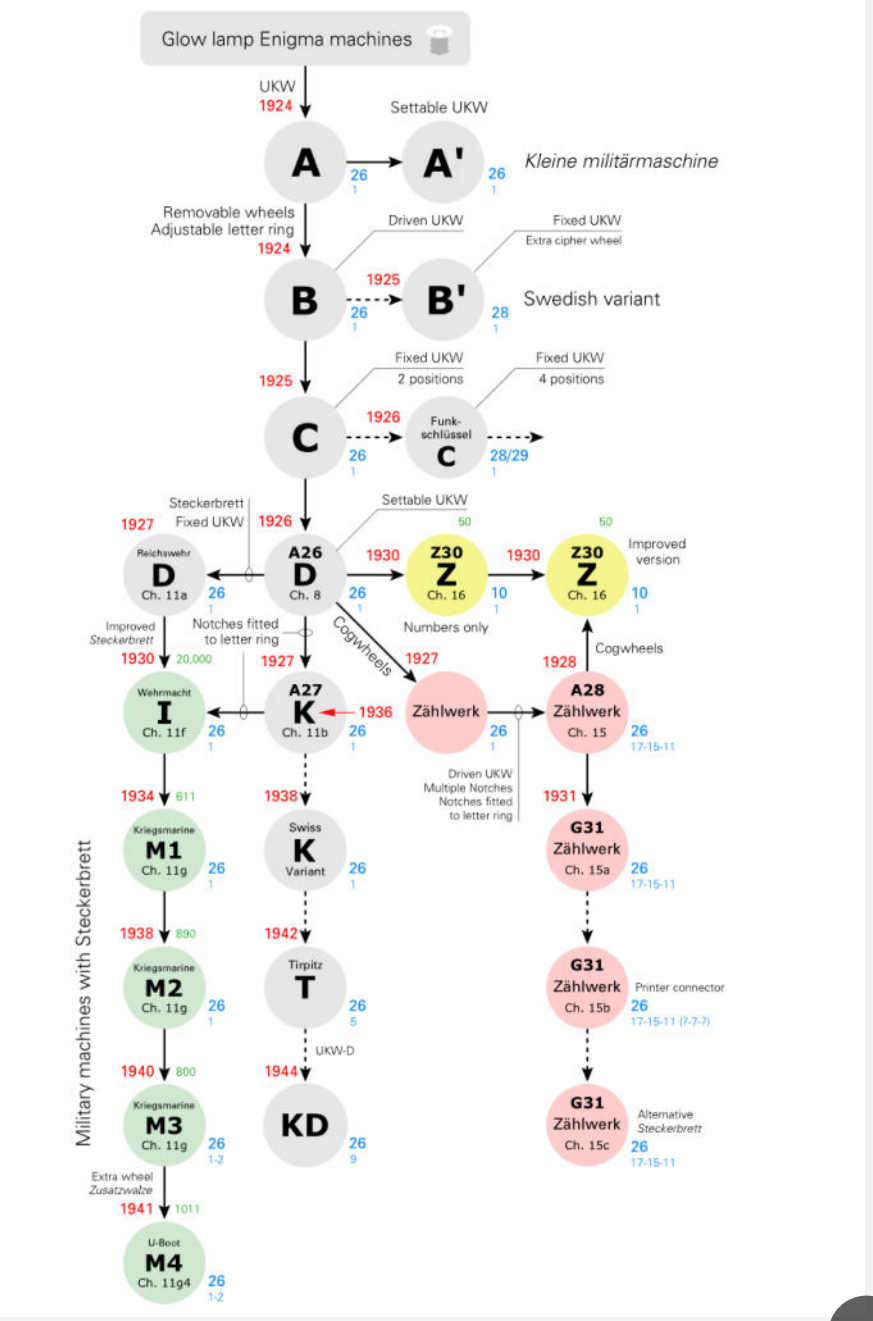

*Die Chiffriermaschine.*

# DER ENIGMA STAMMBAUM

Es gibt 2 Grundtypen:
Druckmaschinen + Glühlampenmaschinen

Quelle:




Quelle
https://www.cryptomuseum.com/crypto/enigma/tree.htm

# DIE ENIGMA DER WEHRMACHT

Wurde Mitte der 1920er Jahre bei der Wehrmacht in Deutschland eingeführt

Es gab verschiedene Typen der Maschine: Die raffinierteste war die Marine-Enigma. Sie hatte einen Rotor mehr.

# ANDERE ENIGMA MODELLE

Die Enigma wurde in zahlreichen Variationen hergestellt.

Ein Modell wurde auch kommerziell verkauft: Die Enigma K

Die sicherste Enigma war die Marine (Navy) Enigma: Sie hatte 4 statt 3 Rotoren

# DIE SCHWEIZER ENIGMA

Die Schweiz beschaffte kurz vor dem Zweiten Weltkrieg Enigma-Maschinen

Enigma K: K = kommerzielles Modell ohne Steckerbrett

Polen, Deutsche, Engländer und Amerikaner knackten sie

# ANDERE ROTORMASCHINEN IM ZWEITEN WELTKRIEG

Viele beeinflusst von der Enigma

# DIE TYPEX ROTORMASCHINE

Britische Erfindung, ab 1937 in Betrieb

Baute auf der Enigma auf

Verbesserungen: 5 Rotoren

Wurden benutzt um Enigma-Nachrichten zu entziffern

# USA: SIGABA

Ähnlich wie die Enigma aber besser

Total 15 Walzen, keine Umkehrwalze

Galt als sicher

# ANDERE DEUTSCHE ROTORMASCHINEN IM ZWEITEN WELTKRIEG

Teilweise wesentlich sicherer als Enigma.

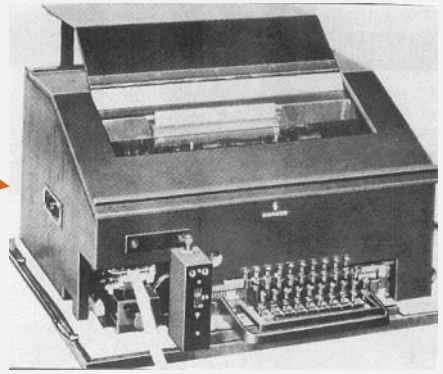
Auf höheren Befehlsebenen benutzt

Fernschreiber – an Drahtleitungen gebunden

# DIE SIEMENS FAMILIE DER FERNSCHREIBER «FISH»

Es gab drei verschiedene Typen von Fernschreiber. Die Briten verwendeten dafür den Codenamen «fish». Alle wurden von Siemens & Halske entwickelt:

1. Siemens SZ 40/42 (Schlüsselzusatzgerät) «tunny»
2. Geheimschreiber Siemens T52: Schlüsselfernschreibmaschine (SFM) T52 «sturgeon»
3. Siemens T43: Schlüssel-Fernschreibmaschine SFM T-43. «thrasher»

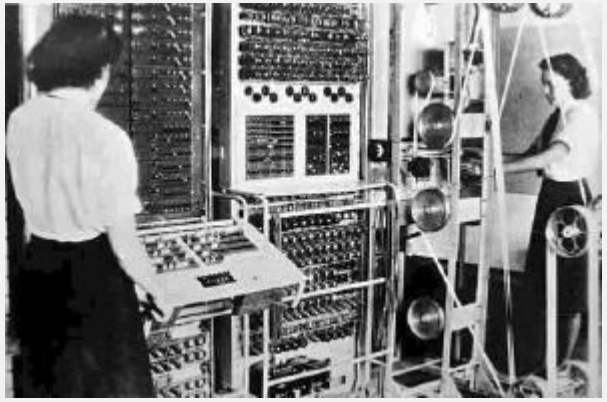


# LORENZ SZ40/42

Auch Lorenz Schlüsselzusatzmaschine genannt funktionierte mit jedem Fernschreiber. Leichter zu bedienen als die Enigma.

Wurde vom Oberkommando der Wehrmacht OKW verwendet. Meist über Telefonleitungen, deshalb gab es wenig Material.

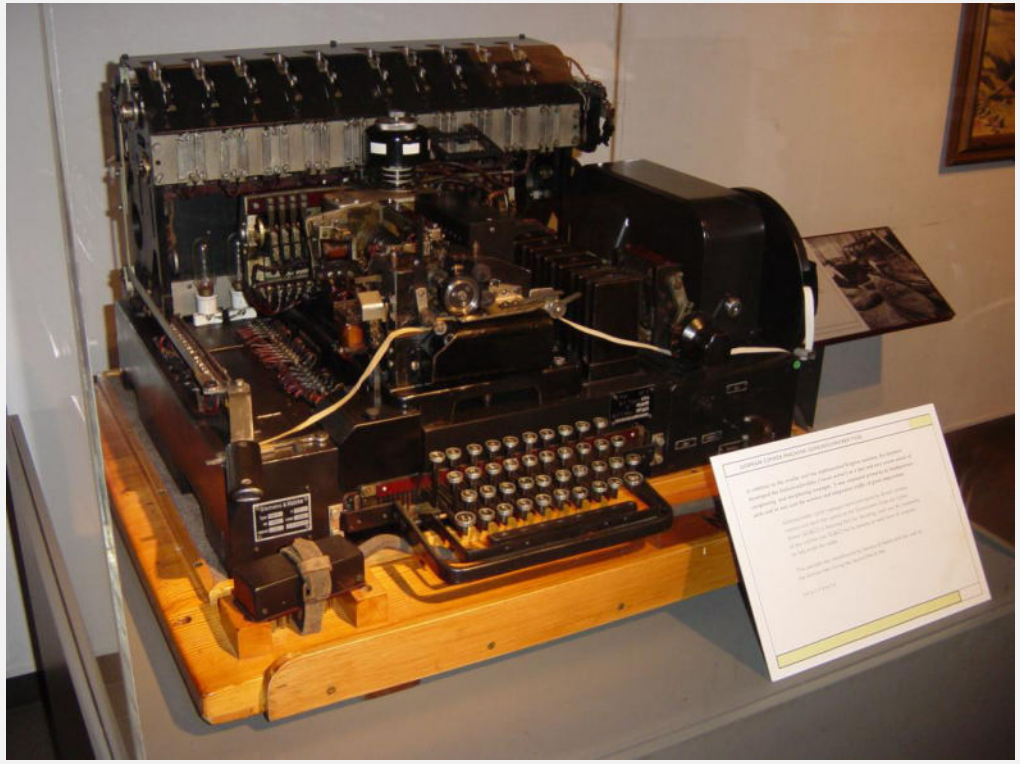
SZ40 war «tunny». Ab 1942 entschlüsselt, ab 1944 mit dem «Colossus» .



# GEHEIMSCHREIBER

Siemens T50. In seiner finalen Version war er nicht zu knacken. Maschine erzeugte Codeschlüssel selber, Bediener kam nie in Berührung damit.

Wurde von Marine und Luftwaffe auf höchster Ebene benutzt. Meist via Telefon deshalb gab es wenig Material für BP.  Durch die Vielzahl der entschlüsselten Enigma-Nachrichten wenig relevant.

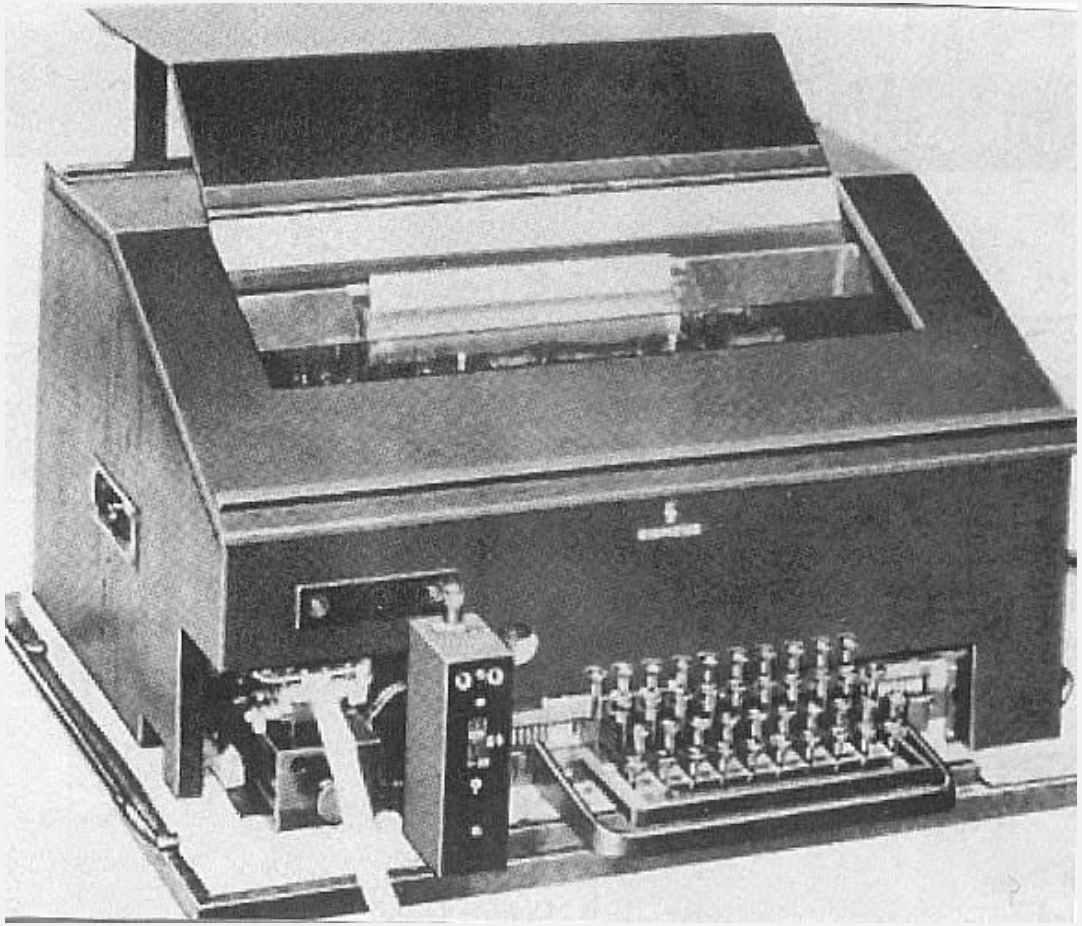


# SIEMENS T43

1943 durch Siemens entwickelt, ab 1944 in Betrieb. Arbeitete mit One Time Pad und deshalb nicht knackbar.

Die Maschine tauchte sehr spät auf. Es gab wohl nur wenige 30-60 Ex. Die Briten nannten sie «sägefeisch» oder «thrasher» wegen dem tpyischen Signal.

Einige wenige Maschinen gelangten in die Hände der Alliierten. Es ist unklar wo sie heute sind. Auch Bildmaterial ist rar.



# NACH DEM ZWEITEN WELTKRIEG

# SCHWEIZ: NEMA
# NEMA = NEUE MASCHINE

Ab 1943 entwickelt, 1948 bereit
Bis 1977 verwendet

5 Rotoren

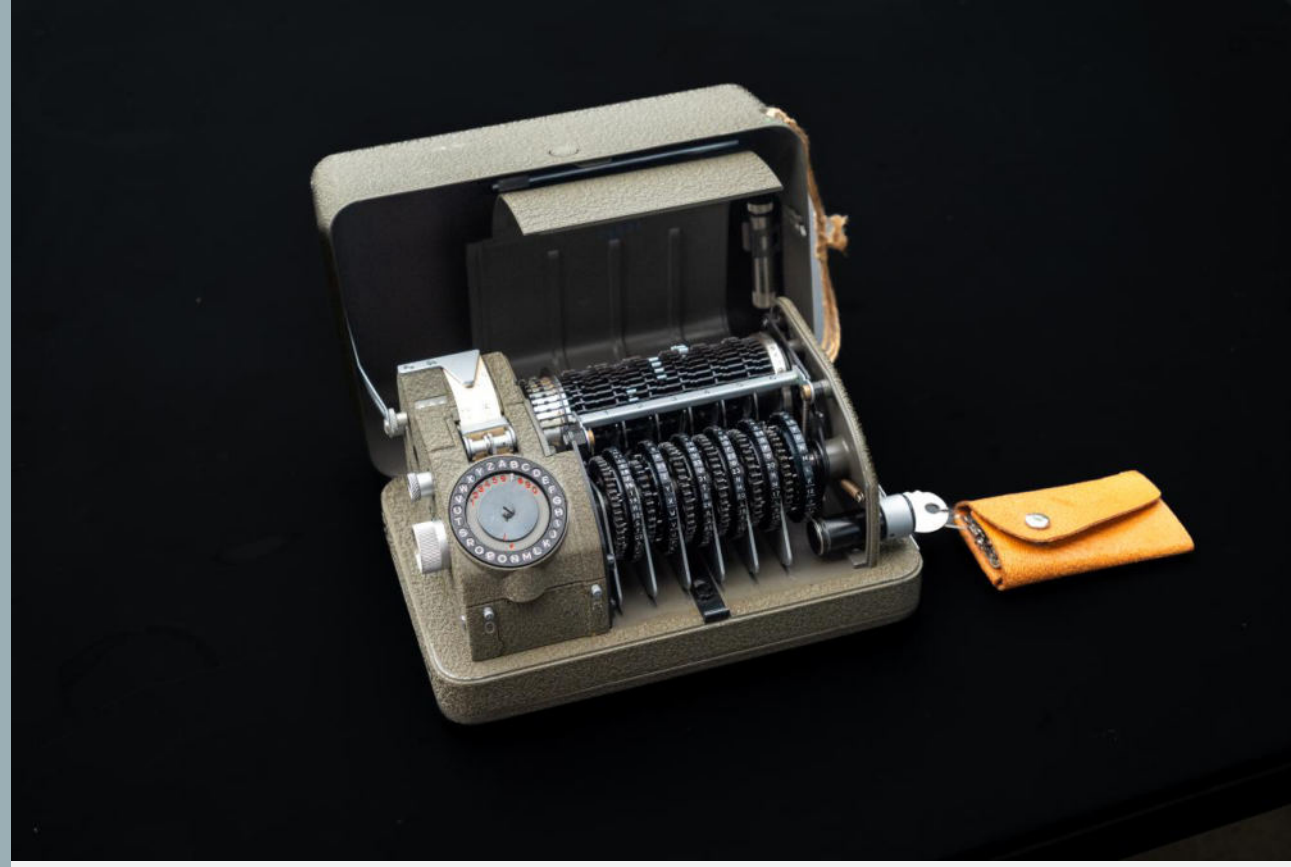
Unregelmässige Fortschaltung

3 Typen: Uebung, Krieg, Diplomatie

# BORIS HAGELIN UND DIE CRYPTO AG IN ZUG

Hagelin entwickelte die Maschin nach dem Krieg. Es war die erste verkaufte Maschine in der Schweiz.

Galt als sehr sicher. So sicher, dass sie dem NSA unheimlich war. Er verlangte ein «unsicheres» Manual für weniger vertrauenwürdige Kunden.



# FUNKFERNSCHREIBER SETZEN SICH DURCH

Text wird in 8-bit Code umgewandelt und kann danach beliebig chiffriert werden.

Verfahren gab es bereits im Zweiten Weltkrieg: Lorenz SZ 40, in England Tunny und Sturgeon.

Findet auch im Amateurfunk Anwendung

# RUSSLAND
# FIALKA

In der DDR von 1968 bis 1990 in Gebrauch
Nutzte ds Prinzip des Fernschreibers

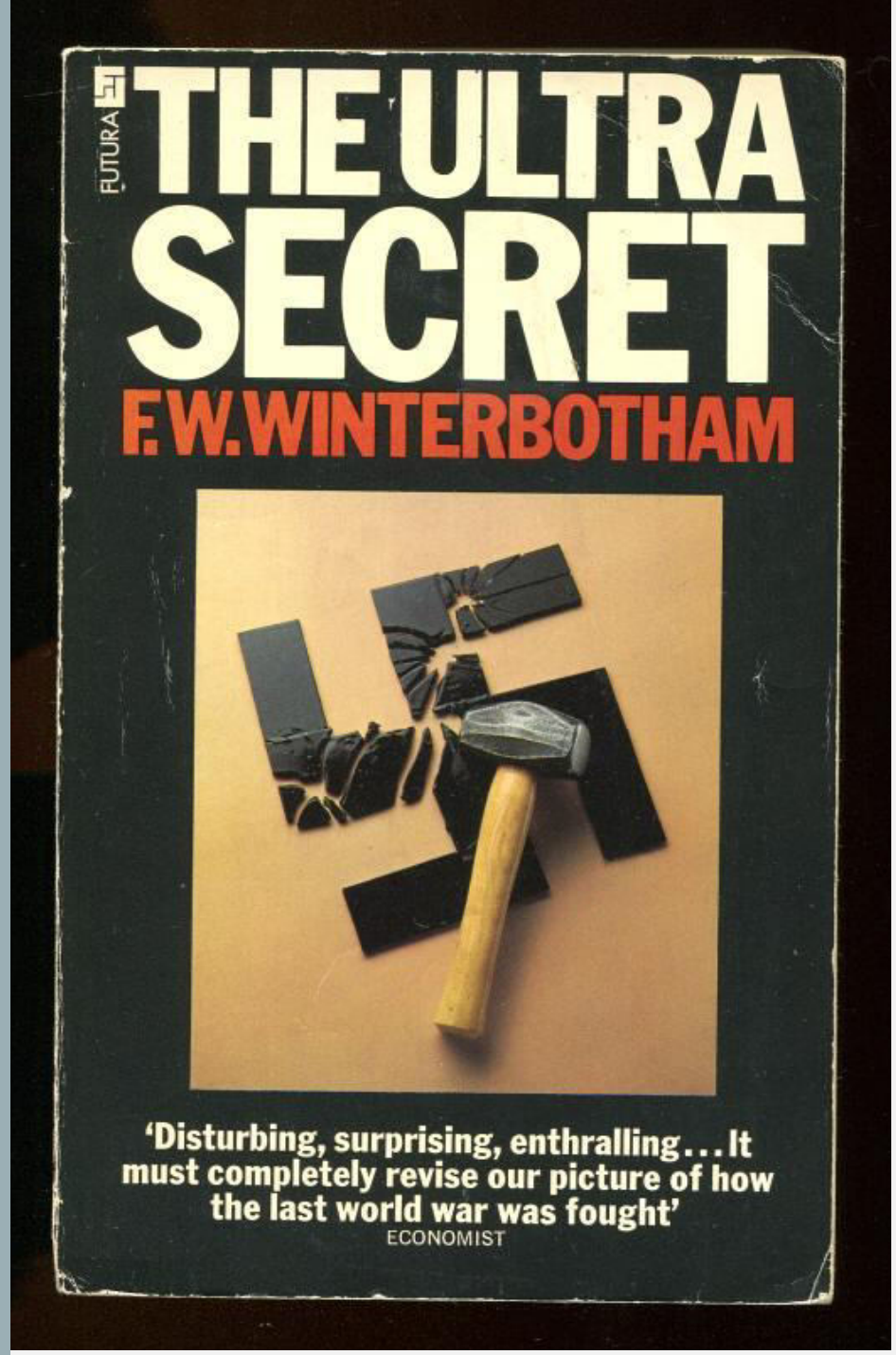
10 Rotoren

# WAR ENIGMA DIE EINZIGE MASCHINE?

# WAR ENIGMA DIE BESTE ROTORMASCHINE?

# WARUM WURDE DIE ENIGMA SO BERÜHMT

# MYTHOS ENIGMA: BLETCHLEY PARK



# MYTHOS ENIGMA: BLETCHEY PARK

# MYTHOS ENIGMA: ALAN TURING

# MYTHOS ENIGMA GOOD STORY

Gute vs. Bös

Intelligenz schlägt Dummheit

Stimmt das?

# DIE SIGSALY: EIN WEITERES GEHEIMNIS

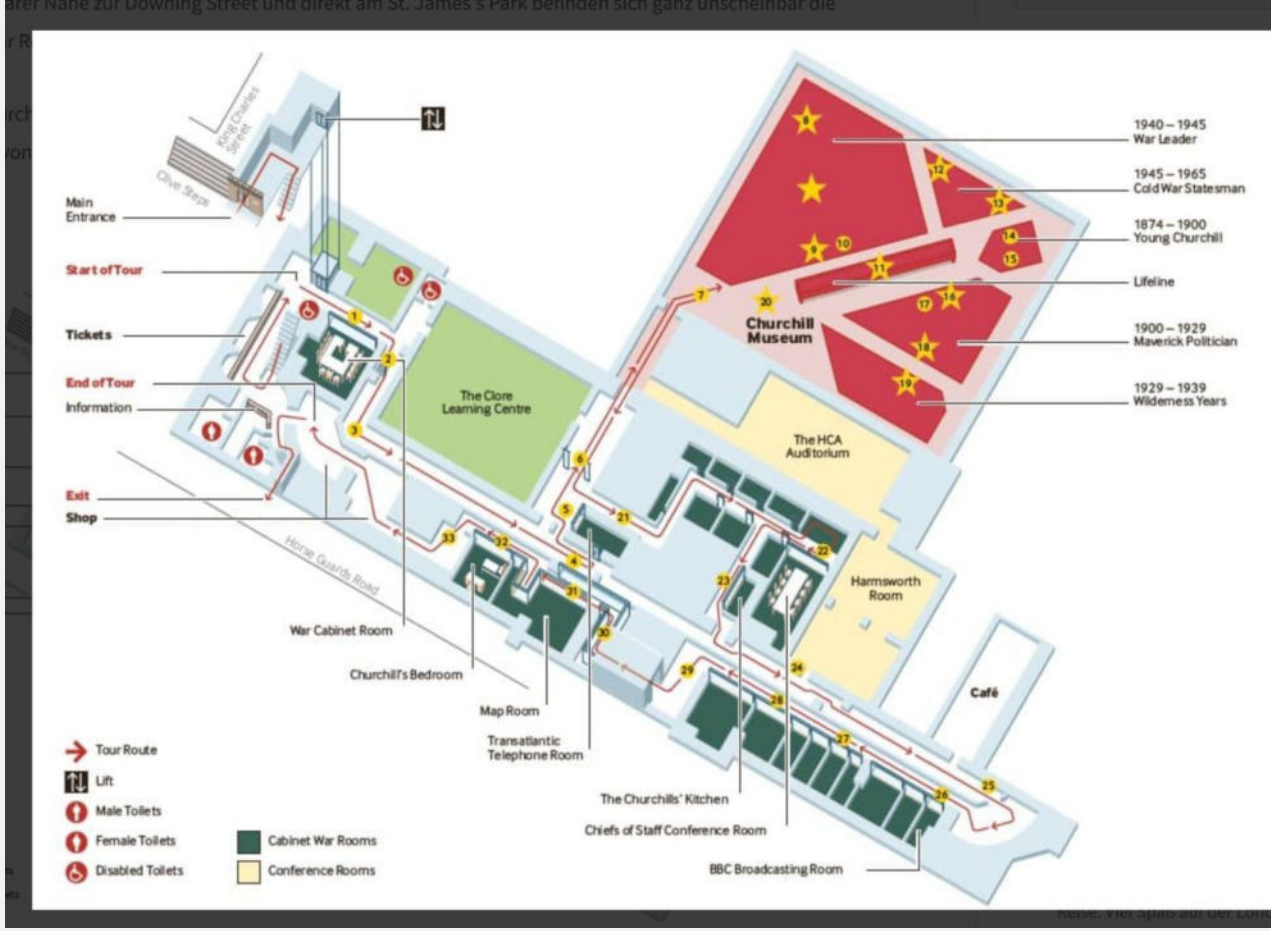
# SIGSALY

Das WC im Kommandobunker von Churchill war gar keines…

# SIGSALY

Sondern ein Telefon um direkt mit US Präsident Roosevelt zu reden

Er heisst heute
Transatlantic Telefon Room



# SIGSALY

# SIGSALY

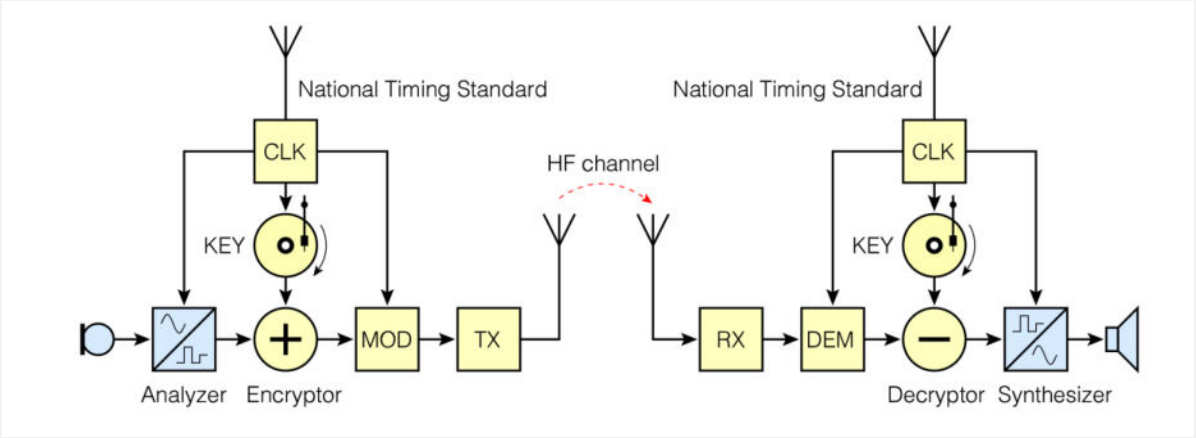
Ein hoch komplexes Sprachverschlüsselungssystem

Sprache wurde digitalisiert (!)
Das digitale Signal mit Rauschen überlagert

Rauschquelle: Langspielplatte mit natürlichem Weissem Rauschen.

Eine Weiterentwicklung des Sprachzerhackers «Voice Scrambers», der aber nicht sicher war.

Vocoder, wie sie in den 1970er Jahren in der Popmusik benutzt waren, spielten eine wichtige Rolle.

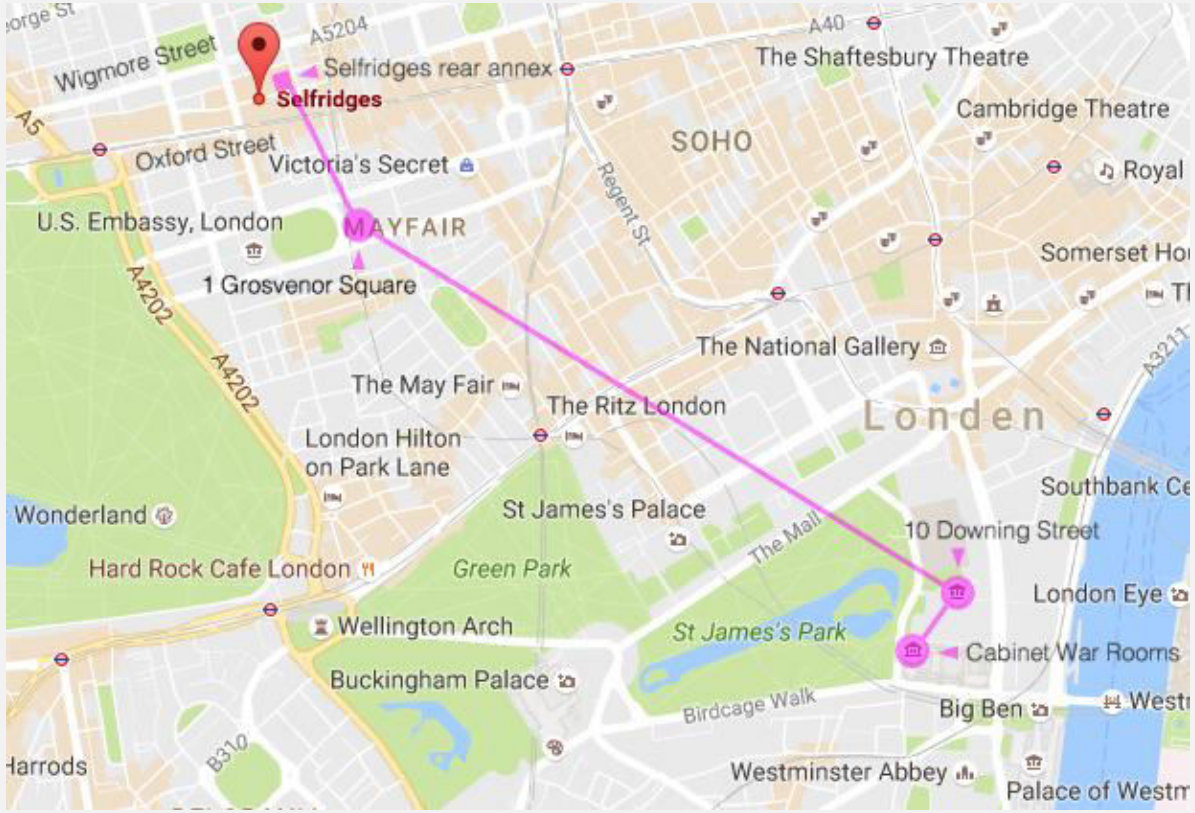


# SIGSALY

Die Basis-Station war unter einem Warenhaus nahe der US Botschaft in London – 60 Meter unter dem Boden.

Es gab 3 Sprechstationen.

Übermittlung der Signale über geschützte Telefonleitungen: In einem mit Gas gefüllten Rohr, dessen Druck kontrolliert wurde.



# WAS KAM NACH DEN ROTORMASCHINEN?

# FUNKFERNSCHREIBER

Nach dem Krieg hatten die Rotormaschinen ausgedient

Die Funkfernschreiber übernahmen

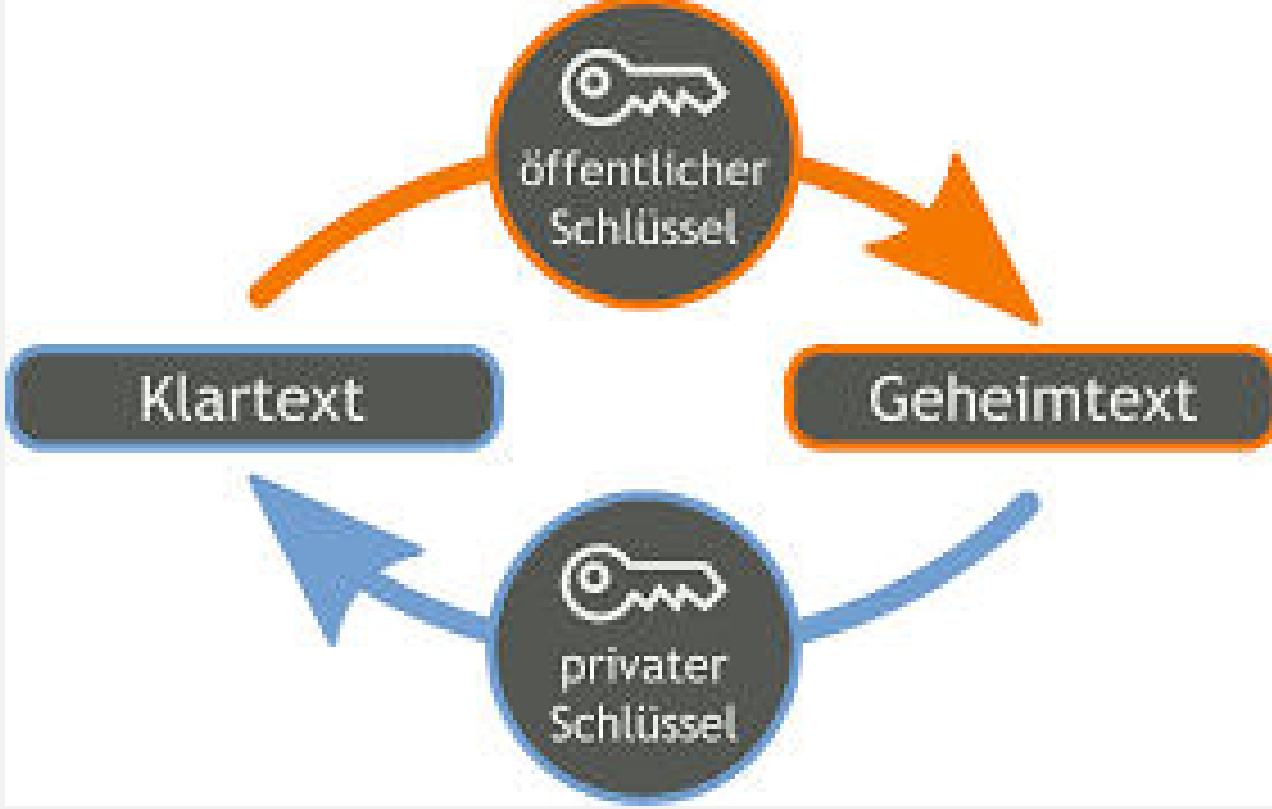
In der Schweiz stellten Gretag und Crypto AG solche Geräte her.

# ASSYMMETRISCHES CHIFFRIEREN

Die Grosse Revolution nach dem Zweiten Weltkrieg kam in den 1970er Jahren: Assymmetrische Chiffrierung

Lösung für Problem der Schlüsselverteilung
Privater und öffentlicher Schlüssel

Steckt in jedem Handy, in jeder Internetseite, in jeder Banktransaktion



# DANKE

Special Thanks to
Paul Reuvers & Marc Simons

https://www.cryptomuseum.com/

# DER AUTOR:
# DOMINIK LANDWEHR

www.peshawar.ch
www.sternenjaeger.ch

dominik.landwehr@bluewin.ch
+41 79 411 59 17