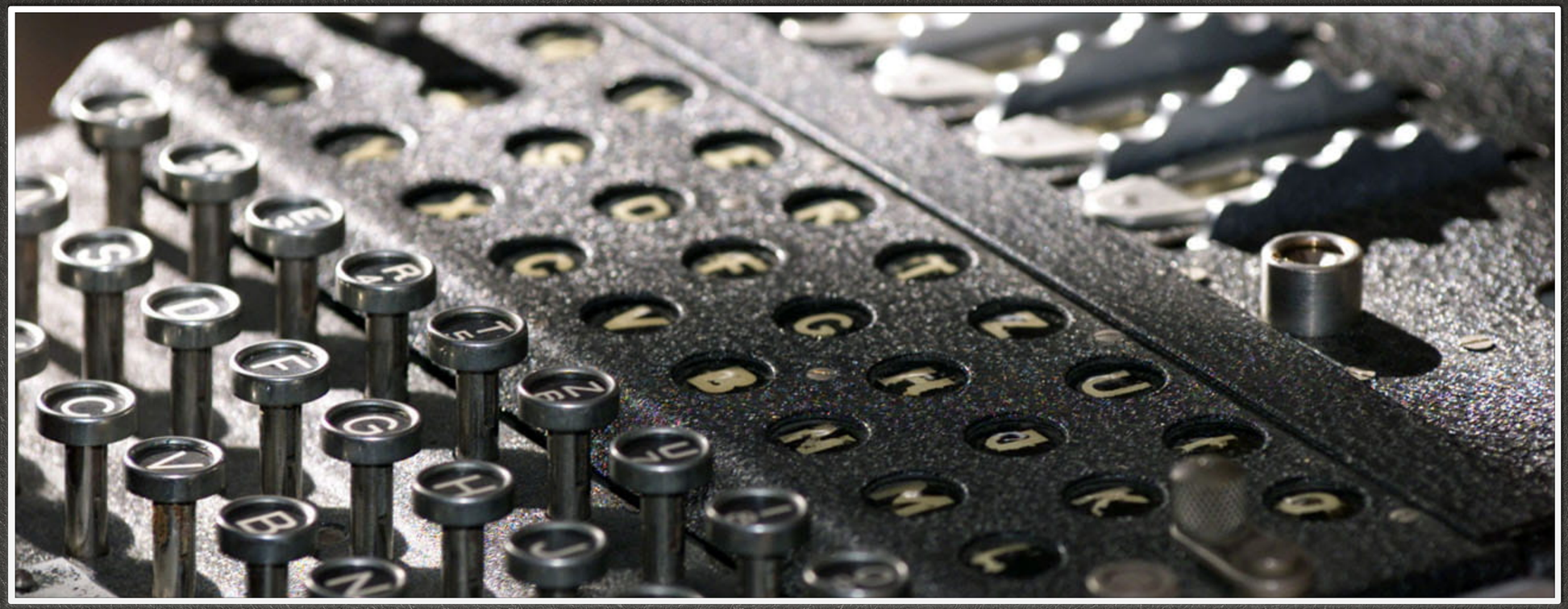


# MATEMATIKA A TAJEMSTVÍ ENIGMY

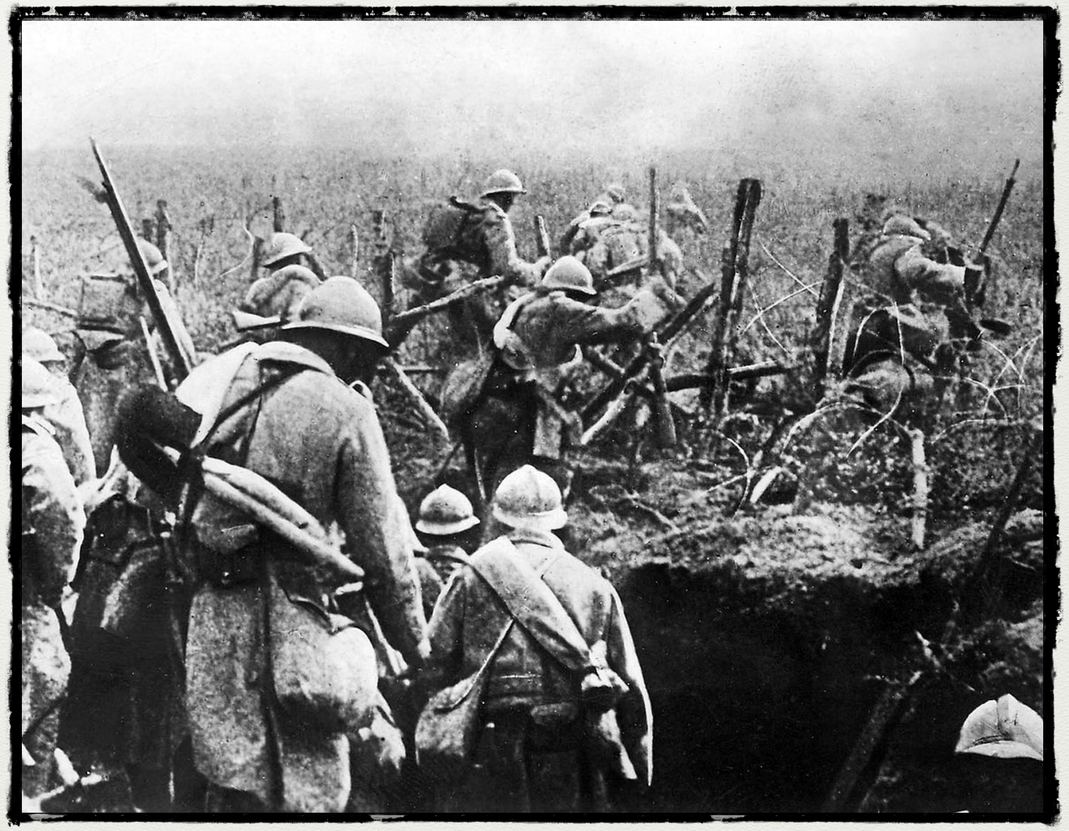
## Jak se matematikům dařilo luštit německé šifry

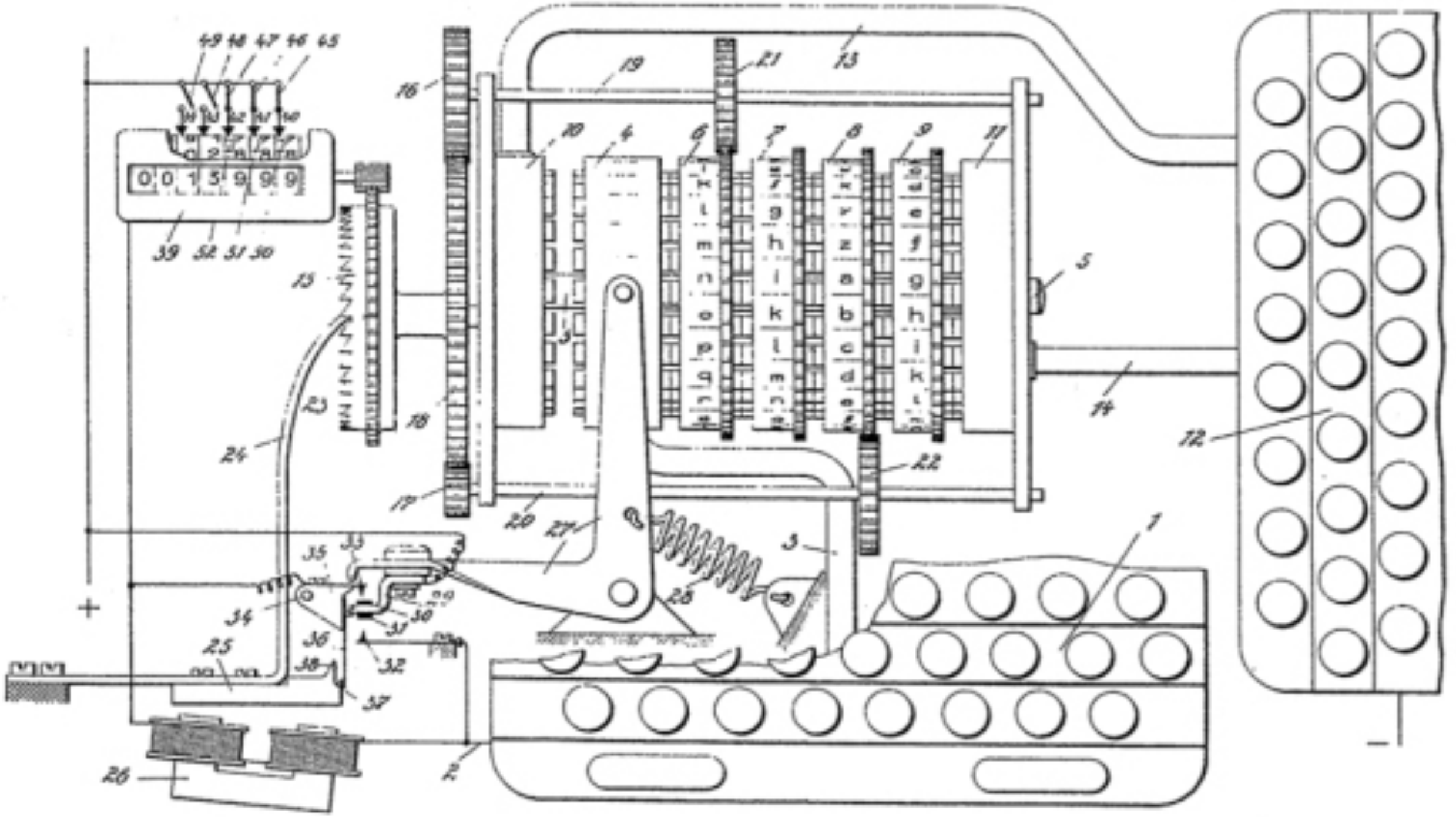
# Co nás čeká

- Situace v kryptoanalýze během 1. světové války a krátce po jejím konci
- Šifrovací stroj Enigma (způsob konstrukce a šifrování, manuály německé armády)
- Polské Biuro Szyfrów
- Polské metody luštění (metoda charakteristik, bomba, Zygalskiho děrné štítky)
- Britské metody luštění (okruhy komunikace, způsoby indikace, britská bomba, Herivelův tip)
- Význam luštění Enigmy ve válce a poválečný vývoj

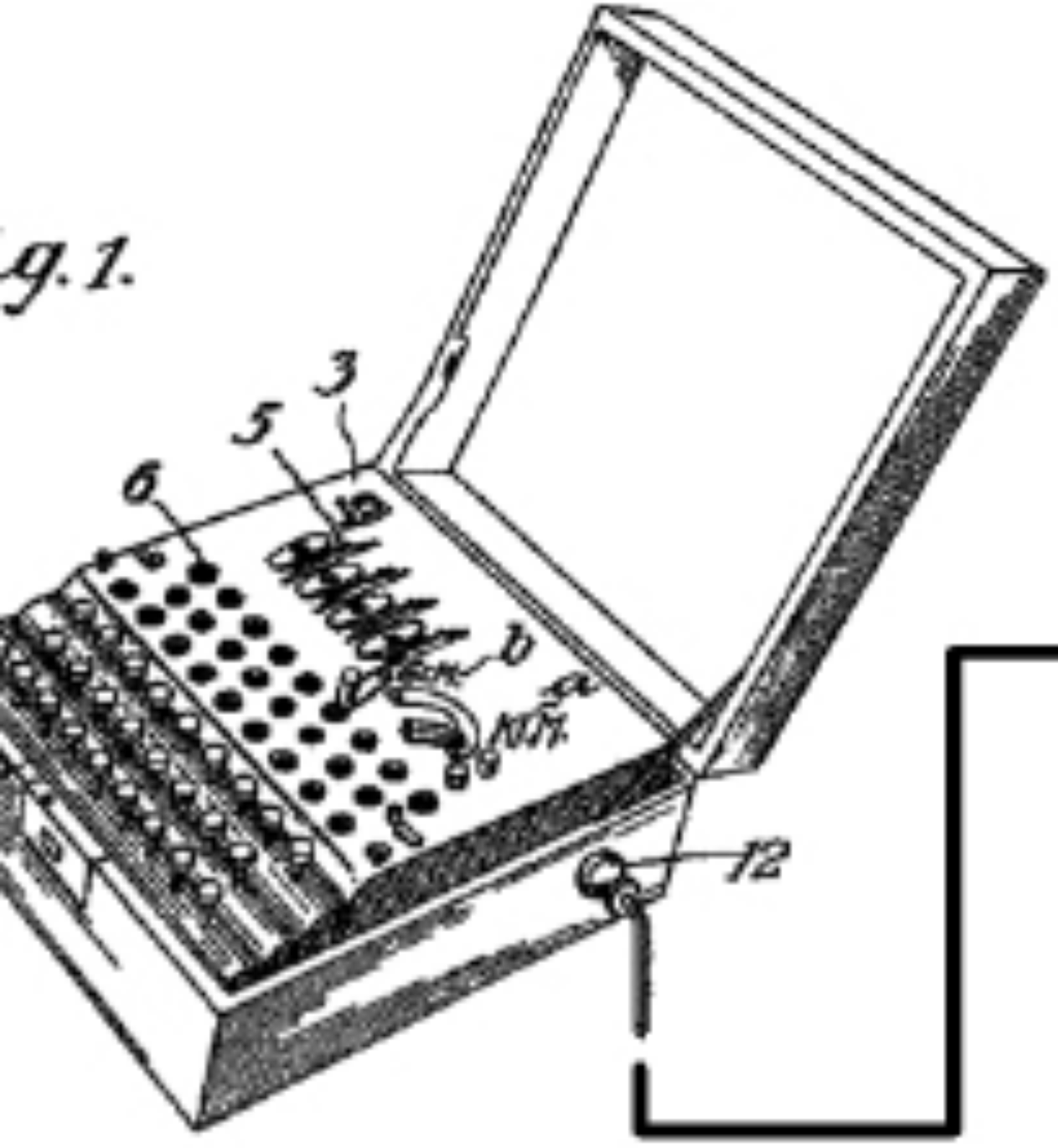
# Šifrování během 1. světové války

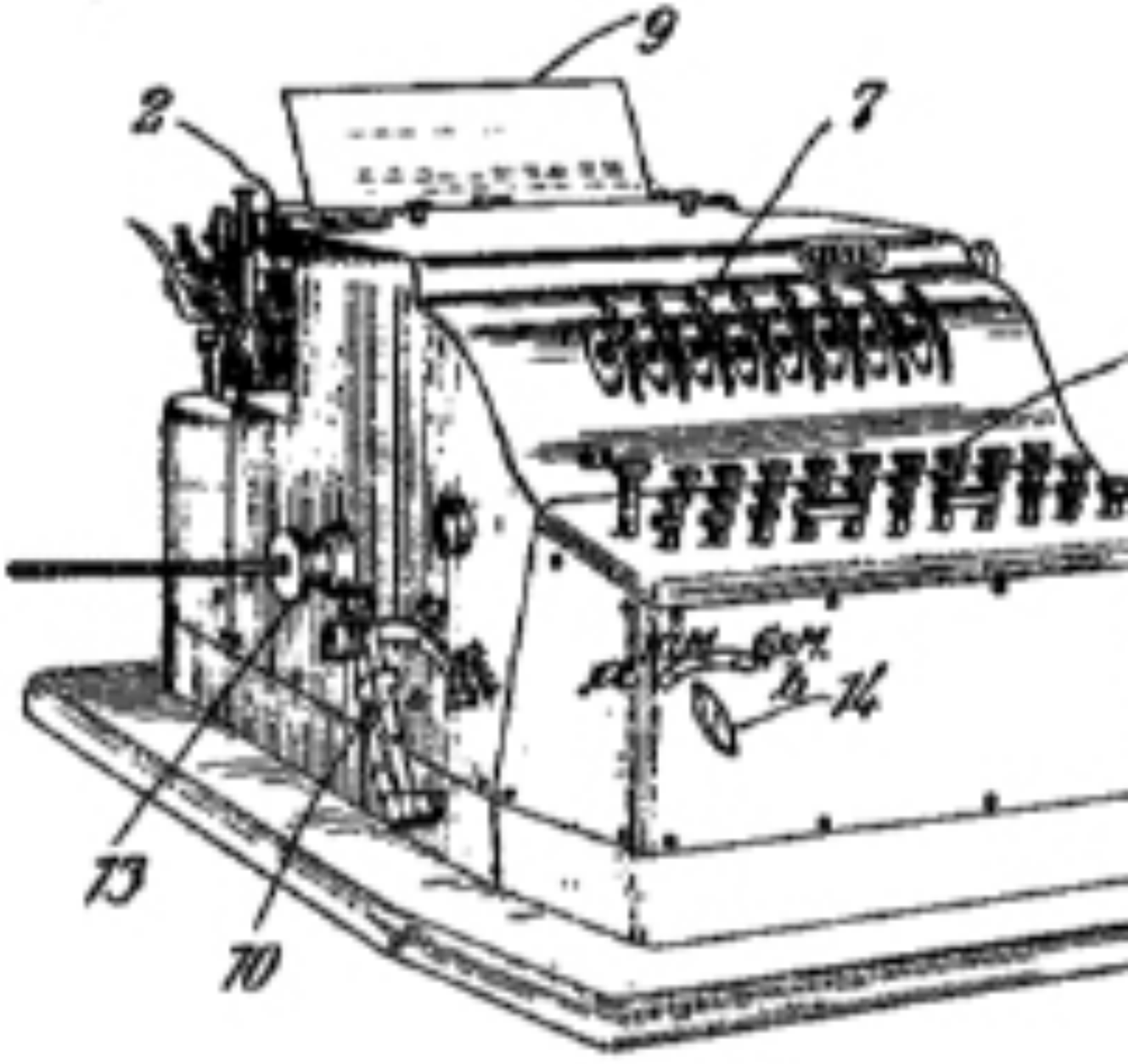
- Ruční šifry
- Oddělení 40 britské tajné služby (Diwlin Knox)
- Rozluštění Zimermannova telegramu (vstup USA do války)
- Rozluštění šifry ADVGFX
- Paměti W. Churchilla
- 1926 (Kriegsmarine), 1927-1928 (Reichswehr)

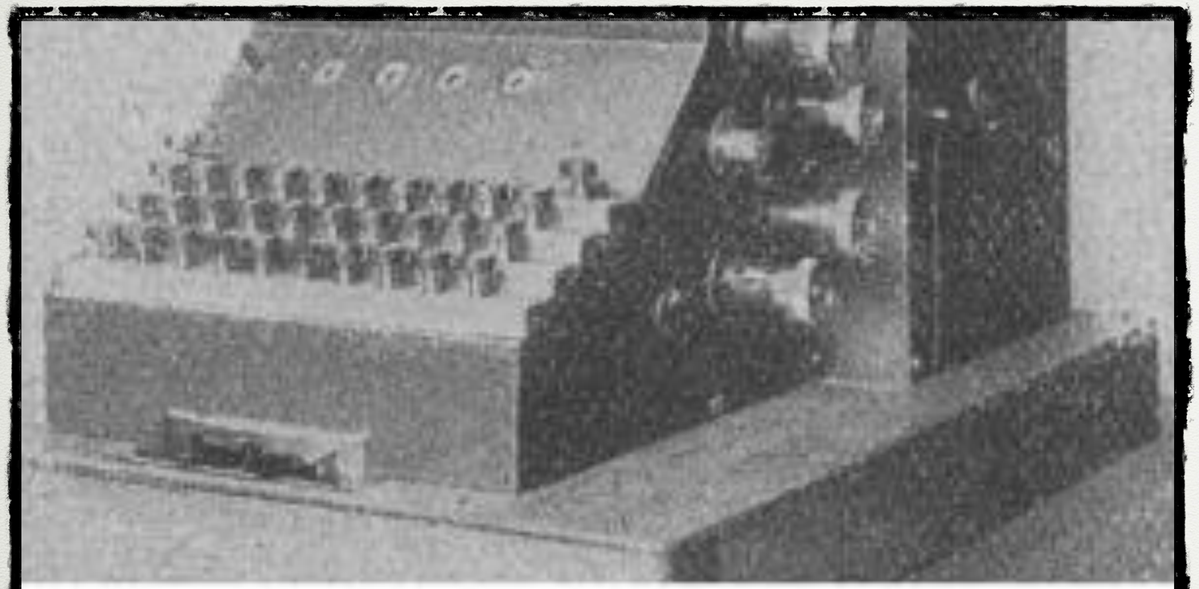


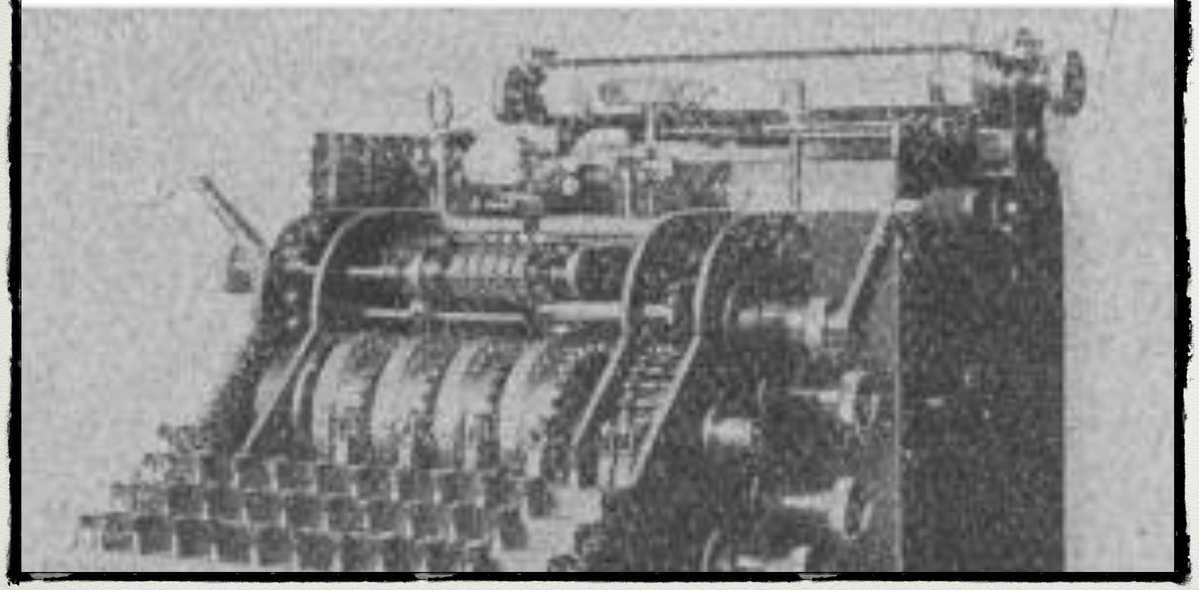

49 48 47 46 45
0 0 1 5 9 9 9
39 52 51 50
13
23
24
16
10
4
6
7
8
9
11
19
21
13
5
14
12
22
17
20
27
3
28
1
35
33
34
36
25
38
37
31
30
32
26
2
+
−

g. 1.



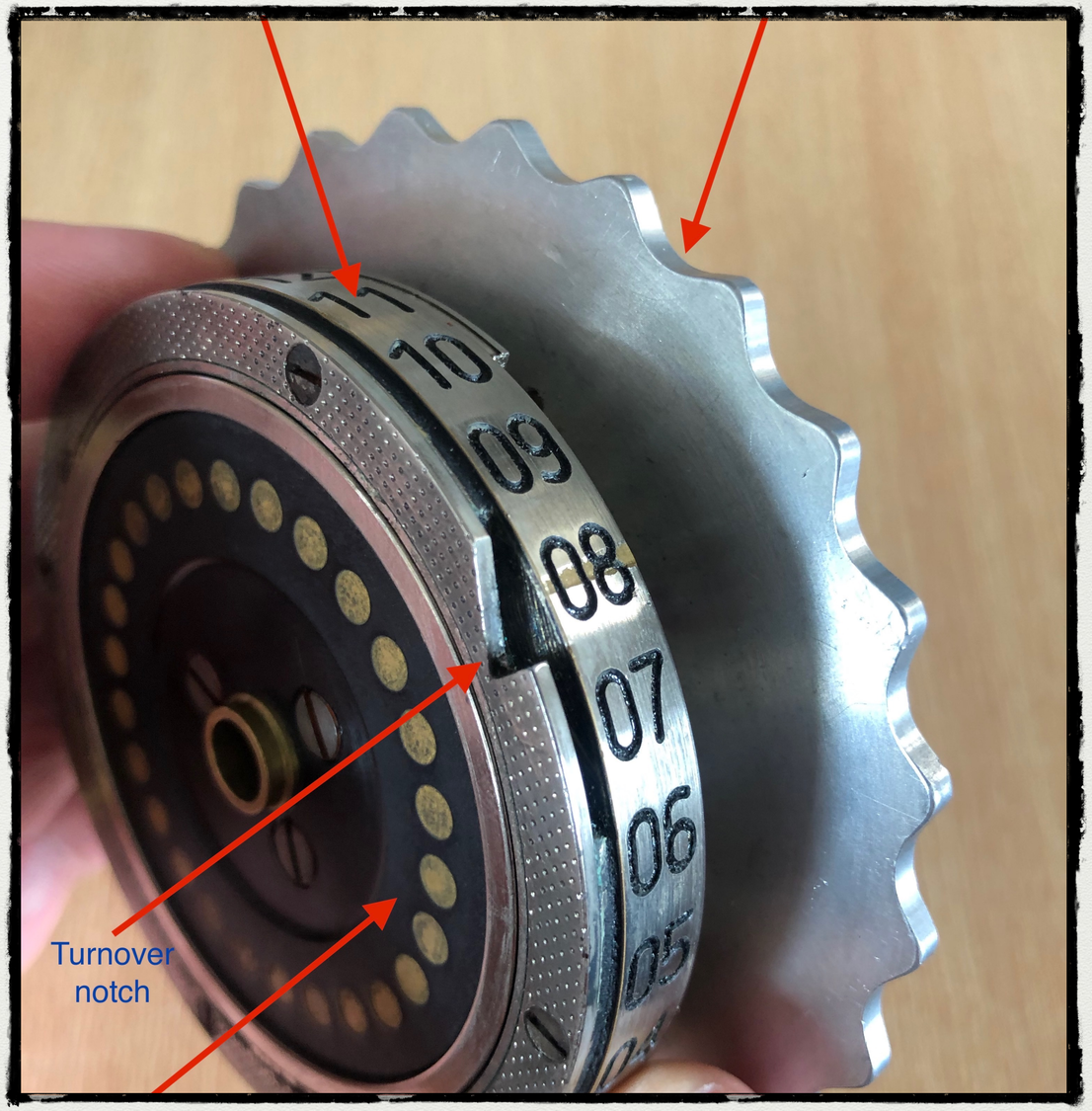








World
Science
Festival

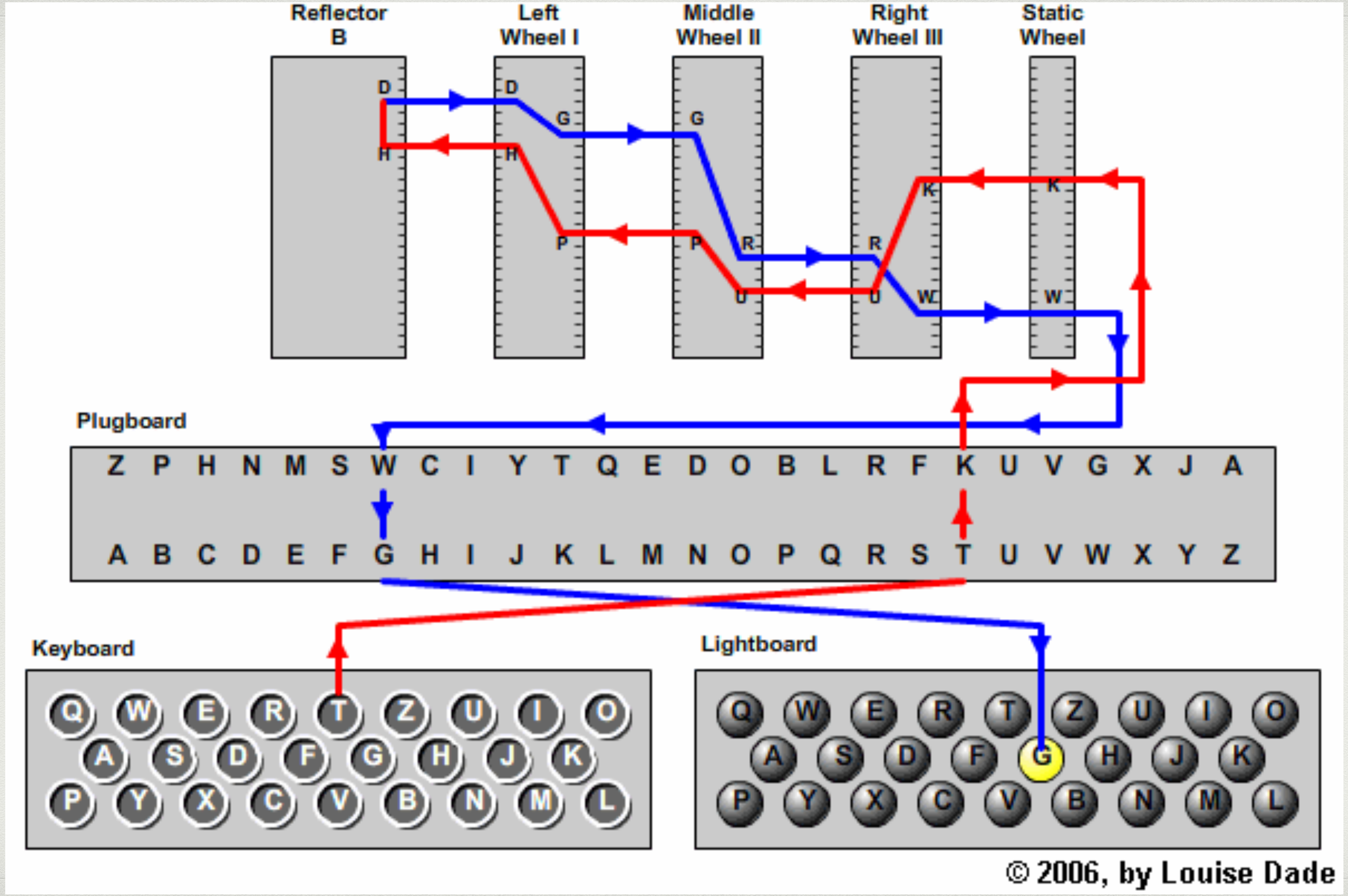

Crypto Museum
cryptomuseum.com
C
B
A
Z
Y
X
W
V
A818


11
10
09
08
07
06
05
Turnover
notch

06
05
04
03
02
01
26
25
24
23
10
09
08
07
06
05
04
03
02


Q
W
E
R
T
Z
U
I
O
A
S
D
F
G
H
J
P
Y
X
C
V
B
N
Klappe schliessen
ENIGMA


M5853
Crypto Museum
cryptomuseum.com


Reflector B
Left Wheel I
Middle Wheel II
Right Wheel III
Static Wheel
D
H
D
G
H
P
G
P
R
U
R
K
U
W
K
W
Plugboard
Z P H N M S W C I Y T Q E D O B L R F K U V G X J A
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Keyboard
Q W E R T Z U I O
A S D F G H J K
P Y X C V B N M L
Lightboard
Q W E R T Z U I O
A S D F G H J K
P Y X C V B N M L
© 2006, by Louise Dade

# Permutace a jejich cyklická struktura

$$\mathcal{S}_A = \{\pi : A \to A, \pi \quad bijekce\}$$

- V našem případě množina A bude představovat množinu písmen anglické abecedy.
- Permutace lze skládat tzn. $\pi \circ \sigma(x) = \pi(\sigma(x))$
- Permutace budeme zapisovat cyklicky.
- $O = (a, b, c, d, \ldots, z)$ je permutace otočení.

# Matematický model přístroje

- Na začátku máme rotory (I, II, III) (později byly přidány IV a V), označme jím odpovídající permutace A,B,C,D,E
- Permutace, které odpovídají nastavení propojovací desky označíme písmenem P.
- Permutaci odpovídající reflektoru označíme písmenem U.

# Matematický model přístroje

- Po natočení jednotlivých prstenců na nové polohy máme permutace $A_i = A \circ O^i$, $B_j = B \circ O^j$, $C_k = C \circ O^k$
- Máme na výběr celkem $26^3$ základních poloh ve kterých zasadíme kotouč do přístroje. Označme písmeny $n, p, q$ když prochází proud takto natočenými rotory šifruje se $A_{i,n} = O^{-n} \circ A_i \circ O^n$ (podobně ostatní permutace).
- Označíme-li $E_t = C_{k,q} \circ B_{j,p} \circ A_{i,n} \circ P$ pak Enigma při natočení prstenců na $i, j, k$ a jejich usazení na polohách $n, p, q$ šifruje permutací $E = E_t^{-1} \circ U \circ E_t$

# Počet nastavení přístroje

- Výběr pořadí prstenců (Wahlzenlage) $3! = 6$ později (1937) $5 \times 4 \times 3 = 60$
- Nastavení rotorů (Ringstellung) $26^3 = 17567$
- Počáteční poloha rotorů v přístroji (Grundstellung) $26^3 = 17567$
- Počet možných nastavení propojovací desky $\sum_{k=0}^{12} \frac{\Pi_{i=0}^{k} \binom{26-2i}{2}}{k!}$

# Počátky polské kryptoanalýzy

- Oddělení založeno roku 1918 během Polsko-Sovětské války
- Září 1919 - „Zázrak na Visle“ (obrat ve válce)
- Do čela oddělení zabývající se luštěním jmenován por. Jan Kowaleski - úspěšný luštitel sov. šifry
- S luštěním pomáhají i matematici např. Prof. Sierpinski

# Trable s Enigmou

- Březen 1927 první záchyt zprávy šifrované Enigmou
- Dosavadní metody luštění nefungují
- Z analýzy odposlechů vyplývá, že se jedná o polyalfabetickou šifru a prvních šest písmen je indikátor

# Dárek z Německa

- 1929 leden - k podezřelému balíku ve Varšavě přivolán M. Cziesky a A. Palluth
- Pořízena kopie přístroje, originál zpět v Německu.
- Enigma v balíku byla komerční verzí. Přesto z německé reakce je jasné že Enigmu používá i armáda.

# Matematici v akci

- Leden 1929 - v Poznani otevřen kurz kryptologie pro studenty matematiky.
- Z kurzu vybráni tři nejschopnější absolventi kurzu.
- Je jim nabídnuto místo v nově založeném Biuru Szyfrów

# Slabiny šifrování Enigmou

- Platí $U \circ U = id$, tedy $E \circ E = id$ (Enigma šifruje stejně jako dešifruje, tyto permutace se nazývají involuce)
- Libovolné písmeno se nešifruje samo na sebe ($E(x) \neq x$)
- Slabin nelze využít, dokud není známo nadrátování rotorů a reflektoru

# Špion Enigma

- H.T. Schmidt - bratr R. Schmidta vedoucího pracovníka německého šifrovacího oddělení
- 1.11.1931. Schůzka s R. Lemoinem
- 8.11.1931 předány manuály k obsluze Enigmy a nastavení na několik měsíců.

# Počátky luštění

- Deuxeme Burreau není schopna luštit zprávy ani s pomocí manuálů (neznalost nadrátování rotorů a reflektoru).
- Září 1932 nastavení a manuál předány polské tajné službě.
- Prosinec 1932, polští luštitelé propočítávají nadrátování rotorů v Enigmě.
- Sestaven simulátor Enigmy
- Zbývá najít rychlý způsob, jakým najít denní klíč.

- $R_I = \begin{pmatrix} a & b & c & d & e & f & g & h & i & j & k & l & m & n & o & p & q & r & s & t & u & v & w & x & y & z \\ e & k & m & f & l & g & d & q & v & z & n & t & o & w & y & h & x & u & s & p & a & i & b & r & c & j \end{pmatrix}$
- $R_{II} = \begin{pmatrix} a & b & c & d & e & f & g & h & i & j & k & l & m & n & o & p & q & r & s & t & u & v & w & x & y & z \\ a & j & d & k & s & i & r & u & x & b & l & h & w & t & m & c & q & g & z & n & p & y & f & v & o & e \end{pmatrix}$
- $R_{III} = \begin{pmatrix} a & b & c & d & e & f & g & h & i & j & k & l & m & n & o & p & q & r & s & t & u & v & w & x & y & z \\ b & d & f & h & j & l & c & p & r & t & x & v & z & n & y & e & i & w & g & a & k & m & u & s & q & o \end{pmatrix}$
- $U_A = \begin{pmatrix} a & b & c & d & e & f & g & h & i & j & k & l & m & n & o & p & q & r & s & t & u & v & w & x & y & z \\ e & j & m & z & a & l & y & x & v & b & w & f & c & r & q & u & o & n & t & s & p & i & k & h & g & d \end{pmatrix}$

# Manuál pro operátory (1928-1938)

- Denní klíč obsahuje: Pořadí rotorů (Wahlzenlage), nastavení rotorů (Ringstellung), počáteční polohu rotorů (Grundstellung), zapojení kabelů na propojovací desce (Steckerverbindung) (zde se propojovalo nejprve šest dvojic písmen, později 10)
- Operátor nejprve vybral rotory, poté je nastavil dle Ringstellung, usadil do přístroje, pootočil na správnou polohu a následně nastavil propojovací desku, dle denního klíče.
- Poté si vybral vlastní nastavení (Grundstellung) a toto nastavení poslal kolegovi na druhé straně zašifrované Enigmou nastavenou na denní klíč.
- Poté nastavil na svou vlastní polohu rotorů (Grundstellung) a v této poloze poslal zbytek zprávy.

# Fatální chyba

- Šifrování stejné trojice písmen dvakrát
- Sestavení tzv. charakteristik dne.
- Označme permutaci, kterou Enigma šifruje při nastavení $S$ jako $E_S$. Dále označme permutaci, kterou Enigma šifruje po $k$ stisknutí jako $E_{S+k}$
- Řekněme, že jsme na začátku zprávy přijali písmena $x_1, x_2, x_3, x_4, x_5, x_6$
- Pak $E_{S+1}(x_1) = E_{S+4}(x_4), \quad E_{S+2}(x_2) = E_{S+5}(x_5), \quad E_{S+3}(x_3) = E_{S+6}(x_6)$

# Charakteristiky dne

- Z dostatečného množství odposlechů je možné sestavit permutace
  $E_{S+1} \circ E_{S+4}, \quad E_{S+2} \circ E_{S+5}, \quad E_{S+3} \circ E_{S+6}$
- Tyto permutace nazval Rejewski charakteristiky dne.
- Nastavení je příliš mnoho potřebujeme rozdělit rozluštění poloh rotorů, propojovací desky a nastavení prstenců.

# Matematické věty

- Cyklická struktura permutací
- **Věta (O konjugovaných permutacích):** Nechť $\pi, \sigma$ jsou permutace na stejné množině. Pak $\pi, \sigma$ jsou konjugované, právě když mají stejnou cyklickou strukturu.
- Důsledkem této věty, je, že cyklická struktura charakteristik dne nezávisí na nastavení propojovací desky.

# Matematické věty

- **Věta (Rejewski):** Složením dvou vlastních involucí vznikne permutace, která má vždy sudý počet cyklů libovolné délky.
- Tato věta umožnila rychlejší sestavení cyklické struktury char. dne a vytvoření katalogu nastavení.


A B C D E F G H I
J K L M N O P Q
R S T U V W X Y Z
BREAK THE CODE!
www.theCODEBREAKERS.org

# Příklad luštění

z,d,q,o,f,x,l,g,c,t,h

e,v

y,s,

a,k

# Metoda charakteristik

- Roku 1935 sestaven katalog nastavení
- Čtení německých zpráv většinou 15-20 minut po zahájení radiového provozu.
- Roku 1937 přidány další dva rotory IV a V. Přidání reflektoru B (čtení zpráv jen občas)
- 15.září 1938, změna způsobu indikace, metoda charakteristik dále nepoužitelná.

# Bomba, děrné štítky

- Samiččí indikátory
- Děrné štítky
- 1938 - změny nastavení každý den (Prstence, nastavení prstenců, deska, poloha, reflektor)-přílišná výpočetní složitost (pro každé Wahlzenlage potřeba jiná bomba)
- Červenec 1939 - setkání tajných služeb v Pyry u Varšavy.

# Další osud polských matematiků

- Září 1939 - přesun z Varšavy do pevnosti Przsemyszl, později do Bukurešti
- Říjen 1939 - přesun lodí do Francie.
- 1940 - po kapitulaci Francie, přesun do Vichistické Francie, práce na zámku Chateau de Fouzes (u Avignonu).
- 1943 - útěk do Španělska, později lodí do Afriky.

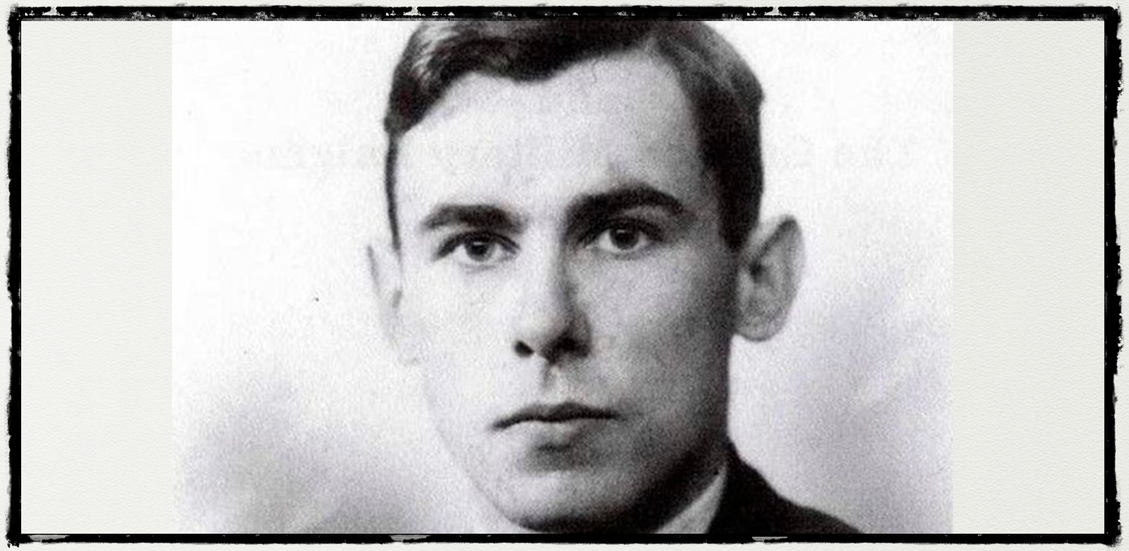
# Luštění v Bletchley parku

# Vznik GC&CS

- 1919 - vznikla sloučením dvou služeb MI1b a NID25
- Šéfem (do 1942) Allastair Denniston (bronzová olympijská medaile v hokeji)
- 1933 vytváří síť kontaktů v Cambridge a Oxfordu (seznam dobrovolníků)
- 1938 SIS kupuje rezidenci v Bletchley parku pro potřeby GC&CS

# Německé okruhy komunikace

- Enigma Wehrmachtu a Luftwaffe (Enigma I, jiné klíče, stejný systém indikace)
- Námořní Enigma (M1,M2,M3,M4) - síť Triton
- Námořní Enigma síť Heimish (M1,M2,M3)
- Enigma Abwehru
- Důstojnická šifra



- Polské metody (děrné štítky) funkční od ledna 1940
- 1.5.1940 změna systému indikace u Luftwaffe a Wermachtu (indikátor se již neposílá dvakrát, metoda děrných štítků nepoužitelná)
- Březen 1940 A. Turing a G. Welchman konstruují britskou bombu
- 22.5.1940 Herivelův tip výrazně urychluje luštění od této doby je průběžně čtena Enigma Luftwaffe a Wermachtu.

# Námořní Enigma

- Odlišný systém indikace
- Rozdělení na síť domácí vody (Heimish) a ponorkové loďstvo (Triton)
- Indikace pomocí tabulek bigramů a trigramů
- Luštění až do června 1943 nepravidelné s výpadky

# Poslední zachycená šifrovaná zpráva

- 6.5. 1945 Cuxhaven (Dánsko): Cuxhaven am 6/5 14:00 - durch britische Truppen besetzt - Ab sofort wird Funkverkehr eingestellt - Wünsche euch nochmals alles Gute - Lt. Kunckel - - Für immer - Alles Gute - Auf Wiedersehen -