Enigma

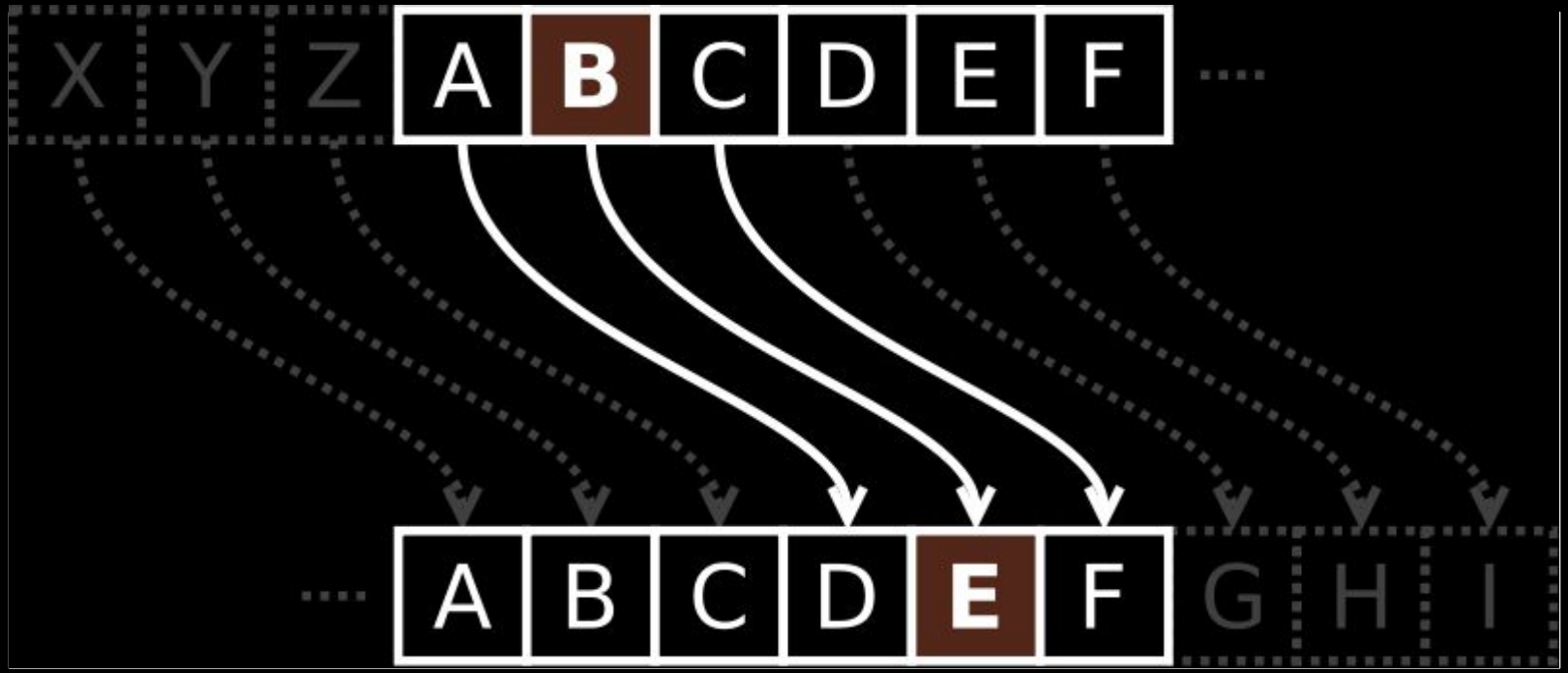
Stanisław Boczarski, Dominik Dygas, Franciszek Gajownik, Karol Zaremba
Krótki kurs historii matematyki, rok akademicki 2024-2025
Wydział Matematyki i Nauk Informacyjnych Politechniki Warszawskiej

Plan prezentacji

- Działanie Enigmy
- Zarys historyczny, czyli rola Polaków w pracach nad Enigmą
- Matematyczne zagadnienia dot. Enigmy
- Losy Enigmy i Polaków po wojnie
- Przykładowy/uproszczony kod i jego rozszyfrowanie

Jak właściwie działała enigma?

Kod Cezara



Kod Cezara

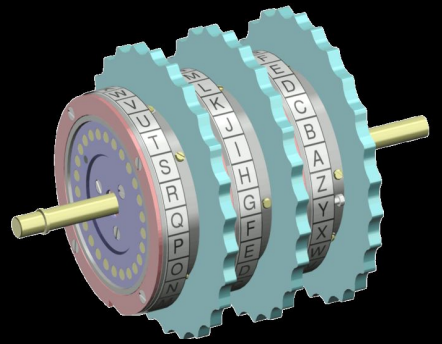
Kod szyfrujący enigmy był dużo bardziej skomplikowanym, jego działanie opierało się na ciągłych zmianach w odpowiedniości znaków.

Znaczy to tyle, że dwukrotne wybranie na maszynie tego samego znaku prawie nigdy nie dawało dwóch tych samych znaków jako komunikat, który był nadawany.

Jak właściwie działała enigma?

Główną dla wersji uproszczonej częścią odpowiadająca za kodowanie, były trzy wymienne koła mające po 26 znaków, służące do przekształcania liter zadanych przez użytkownika.

Obecne były jeszcze dwie zębatki, które były niezmienne dla każdej maszyny niemieckiej.



Jak właściwie działała enigma?

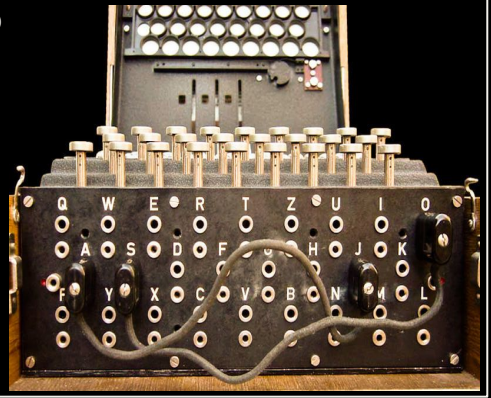
Ponadto wirniki odpowiadające za kodowanie miały 5 różnych wersji, a wersje różniły się kolejnością liter w zapisie.

A zatem możliwości kodowania w tej wersji maszyny było 5 x 4 x 3, na wybór “zębatki” widocznej po prawej i po 26 ustawień każdego z nich, czyli razem 1 054 560 możliwości.

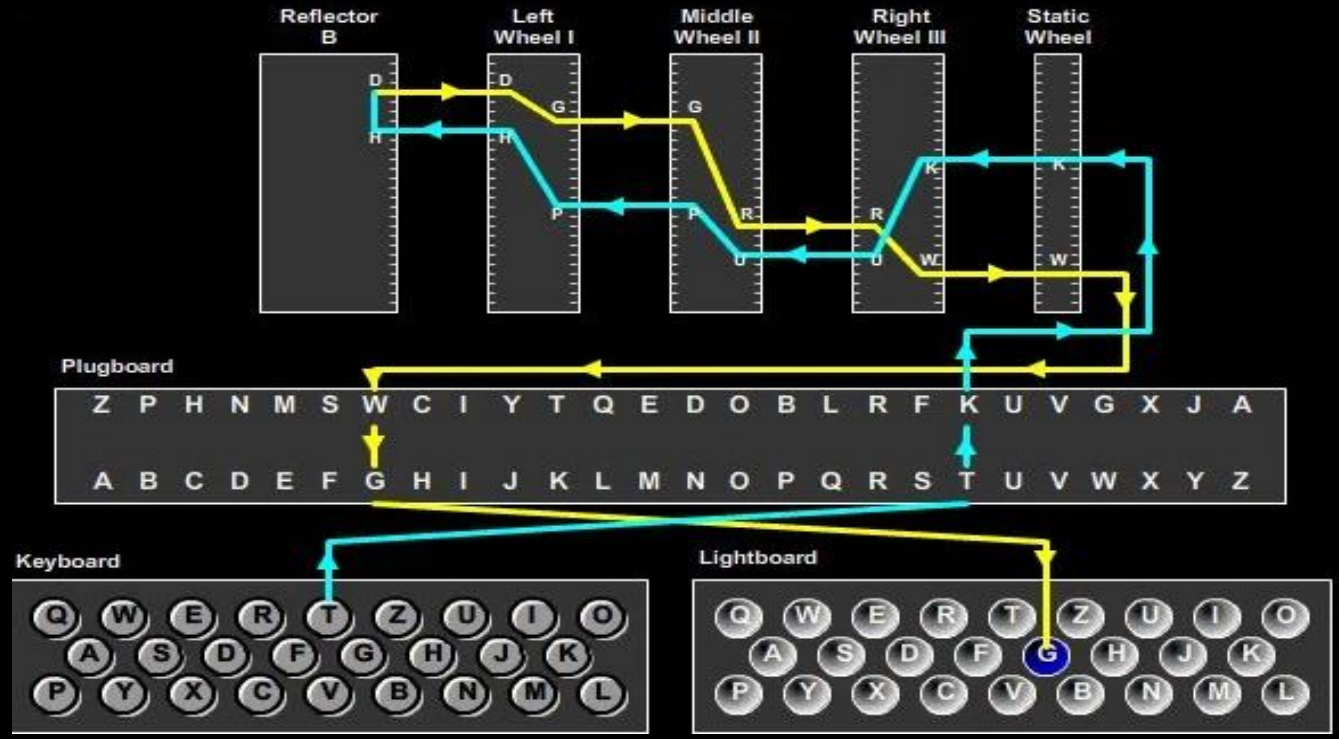
Jak właściwie działała enigma?

Wersja uproszczona przedstawiona na poprzednich slajdach nie była używana przez wojsko, lecz w łączności administracyjnej i cywilnej.

Dla wersji używanej na froncie działającej na podobnej zasadzie, jednak z dużo większą liczbą możliwości, sposobów na zakodowanie szyfru było 158,962,555,217,826,360,000.



Jak właściwie działała enigma?



Jak właściwie działała enigma?

Oprócz złożoności maszyny i jej działania, sam kod, kiedy posiadało się informację na temat ustawienia numerów zębatek i ich kolejności oraz wtyczek, nie był trudny do złamania.

Jednak konfiguracja była zmieniana każdego dnia, co znacznie utrudniało poznanie kodu.

Geheim! **Sonder - Maschinenschlüssel BGT**

Datum	Walzenlage	Ringstellung	Steckerverbindungen	Grundstellung
31.	IV II I	F T R	HR AT IW SK UY DF GV LJ BO MX	vyj
30.	III V II	Y V P	OR KI JV OE ZK KU BF YC DS GP	cqr
29.	V IV I	O H R	UX JC PB BK TA ED ST DS LU FI	vhf

Jak właściwie działała enigma?

Początki prac nad enigmą

W 1919 roku Jan Kowalewski rozpoczął pracę w Sekcji Szyfrów zajmującej się nasłuchiwaniem zagranicznych depesz.

Pewnego razu na nocnym dyżurze, dla zabicia czasu podjął próbę rozszyfrowania sowieckiej depeszy. Posługując się grzebieniem udało mu się rozszyfrować wiadomość.

To wydarzenie ujawniło wielki talent kryptograficzny Kowalewskiego. Dzięki jego pracy Polacy w późniejszych latach odszyfrowywali praktycznie wszystkie Sowieckie depesze, co miało kluczowe znaczenie w wojnie z Bolszewikami.


Walki polsko-bolszewickie
1919 – 1920
Litwa
Niemcy
Niemcy
Rosja
Polska
Rumunia
Kołobrzeg
Słupsk
Gdańsk
Królewiec
Kowno
Święciany
Połock
Witebsk
Wilno
Wilejka
Suwałki
Sejny
Olsztyn
Grudziądz
Pila
Bydgoszcz
Toruń
Mława
Łomża
Grodno
X 1920
Lida
Mińsk
Nowogródek
IX 1920
Baranowicze
Białystok
Włocławek
Poznań
Września
Płock
VII 1920
Warszawa
Siedlce
Brześć Litewski
Pińsk
Mikaszewice
Mozyr
Leszno
Ostrów Wlkp.
Głogów
Łódź
Wrocław
Dęblin
Lublin
Sarny
Kowel
IX 1920
Chełm
Łuck
Równe
VI 1920
Kijów
Częstochowa
Kielce
Opole
Kłodzko
Sandomierz
Zamość
Lwów
Katowice
Kraków
Tarnów
Cieszyn
Nowy Targ
Nowy Sącz
Przemyśl
Lwów
Brody
Żytomierz
IV 1920
Berdyczów
Tarnopol
Stryj
Winnica
Kamieniec Podolski
Stanisławów
kierunki uderzeń Armii Czerwonej
kierunki uderzeń wojsk polskich
najdalszy zasięg ofensywy Armii Czerwonej w 1920 r.
najdalszy zasięg ofensywy polskiej w 1920 r.
obszary plebiscytowe
linia Curzona

W 1931 roku sekcja szyfrów została połączona z Polskim Radiem-Wywiadem, tworząc Biuro Szyfrów, które objął major Gwido Langer, a jego zastępcą został kapitan Maksymilian Ciężki.

Ciężki uważał, że klucz do łamania szyfrów tkwi nie w lingwistyce, lecz w matematyce.

Gwido Langer (1894 - 1948)

Początki prac nad enigmą

Ciężki zorganizował tajny kurs kryptologii na Uniwersytecie Poznańskim, gdzie trzej studenci – Marian Rejewski, Jerzy Różycki i Henryk Zygalski – wyróżnili się, stosując matematyczne podejście do szyfrów.

W 1932 roku Ciężki włączył ich do pracy w Biurze Szyfrów.

Maksymilian Ciężki (1898 - 1951)

Początki prac nad enigmą

W 1932 roku, dzięki francuskiemu oficerowi wywiadu Gustavowi Bertrandowi w ręce Biura Szyfrów trafiła instrukcja obsługi maszyny enigma oraz jej ustawienia na wrzesień i październik tego samego roku.

Gustave Bertrand (1896 - 1976)

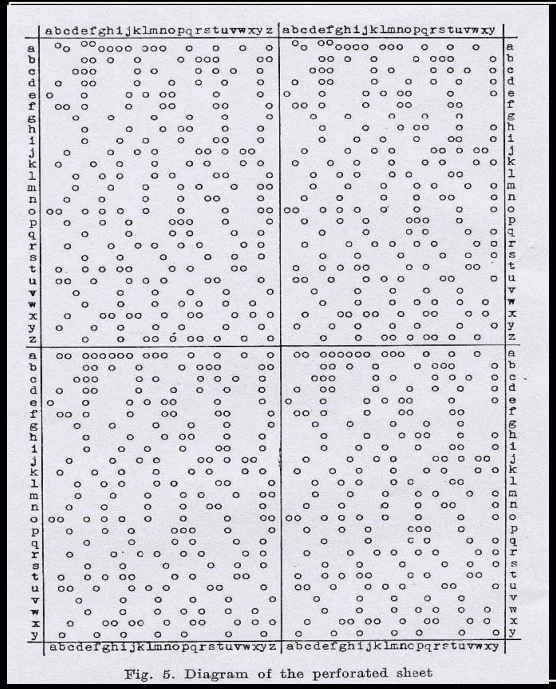


Fig. 5. Diagram of the perforated sheet

W 1938 roku pojawił się duży problem. Niemcy wprowadzili do Enigmy dodatkowe wirniki. Oznaczało to zapotrzebowanie na stworzenie wielu dodatkowych bomb kryptologicznych, aby móc dalej poprawnie odczytywać zaszyfrowane depesze. Wymagało to znacznych nakładów finansowych, których Wojsko Polskie zwyczajnie nie posiadało.

Zadecydowano, że sekret złamania Enigmy trzeba przekazać Francuzom i Anglikom, którzy posiadali odpowiednie środki, aby kontynuować dalsze prace.

Konferencja Kryptologiczna w Pyrach

24 lipca Polacy zaprosili francuskich i angielskich kryptologów na konferencję kryptologiczną w Pyrach pod Warszawą w celu przekazania im osiągnięć związanych z Enigmą.

Przez kilka dni polscy matematycy wraz z majorem Maksymilianem Ciężkim prowadzili wykłady dla zagranicznych gości o tym, jak rozpracowali Enigmę i o stosowanych metodach.

Wraz z początkiem Września 1939 roku całe Biuro Szyfrów ewakuowano przez Rumunię do Paryża, a wszelkie ślady działalności i dokumenty zostały spalone.

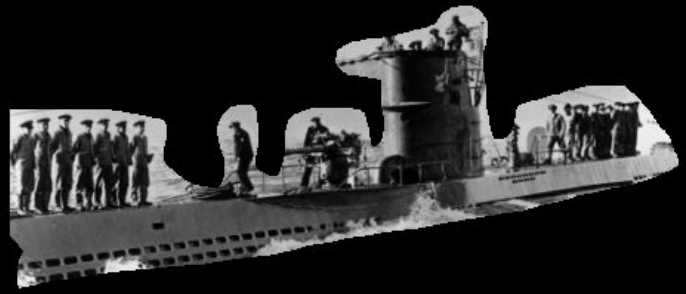
W czasie wojny wielokrotnie przenosili się z miejsca na miejsce, jednak długi czas dalej pracowali z Francuzami nad Enigmą.

W 1942 roku Jerzy Różycki zginął w katastrofie statku pasażerskiego podczas podróży z Algierii do Francji.

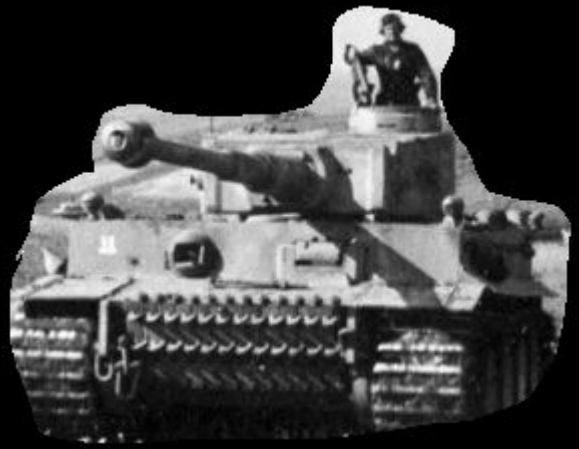
Marian Rejewski i Henryk Zygalski zostali złapani w Hiszpanii, jednak po interwencji Czerwonego Krzyża uwolniono ich i przetransportowano do Londynu,, gdzie dołączyli do Polskich Sił Zbrojnych.

W roku 1943 w Hiszpanii aresztowano Maksymiliana Ciężkiego i Gwido Langera, jednak Niemcy nie zdawali sobie sprawy, kto trafił w ich ręce. Dopiero po jakimś czasie dowiedzieli się kim są jeńcy i zaczęły się przesłuchania. Polakom udało się jednak przekonać Niemców, że jedyne sukcesy jakie odnieśli w sprawie Enigmy, miały miejsce do 1938 roku, czyli jeszcze przed zmianą szyfrów i wprowadzeniem dodatkowych wirników. Naziści stracili zainteresowanie tym tematem i dzięki temu udało się uratować sekret Enigmy.

Gdzie pomogła Enigma?



Zatapianie U-Bootów



Bitwa na Łuku Kurskim

Sylwetki polskich kryptologów pracujących nad enigmą

Sylwetki polskich kryptologów

Marian Rejewski

Matematyczna podstawa sukcesu

Jerzy Różycki

Analityczna precyzja

Henryk Zygalski

Wynalazca kart perforowanych

Aspekty matematyczne

Działem matematyki potrzebnym do złamania szyfru enigmy była w znacznej mierze m.in.teoria grup, mówiąc ściślej - grupy permutacji. Istotnie - permutacje dobrze modelowały zmiany alfabetu, które występowały w trakcie obracania się bębenków maszyny, czyli szyfrowania liter.

Aspekty matematyczne

G - niepusty zbiór
$\star$ - działanie binarne na G, czyli $\star$: G $\times$ G $\to$ G.
Mówimy, że para (G,$\star$) jest **grupą,** jeżeli spełnione są następujące warunki:

Łączność: Dla wszystkich a,b,c $\in$ G zachodzi:

$$(a \star b) \star c = a \star (b \star c)$$

Istnienie elementu neutralnego: Istnieje e $\in$ G taki, że dla każdego a $\in$ G mamy:

$$a \star e = e \star a = a$$

Istnienie elementu odwrotnego: Dla każdego a $\in$ G istnieje b $\in$ G, taki że

$$a \star b = b \star a = e$$

X_n = {1, ..., n} - zbiór n elementowy (u nas n = 26, aby $X_n \cong$ {a, b, c, ..., z})

S_n - zbiór bijekcji z X_n do X_n (permutacji)

Wraz z działaniem ○, S_n tworzy grupę (S_n, ○) zwaną grupą permutacji.

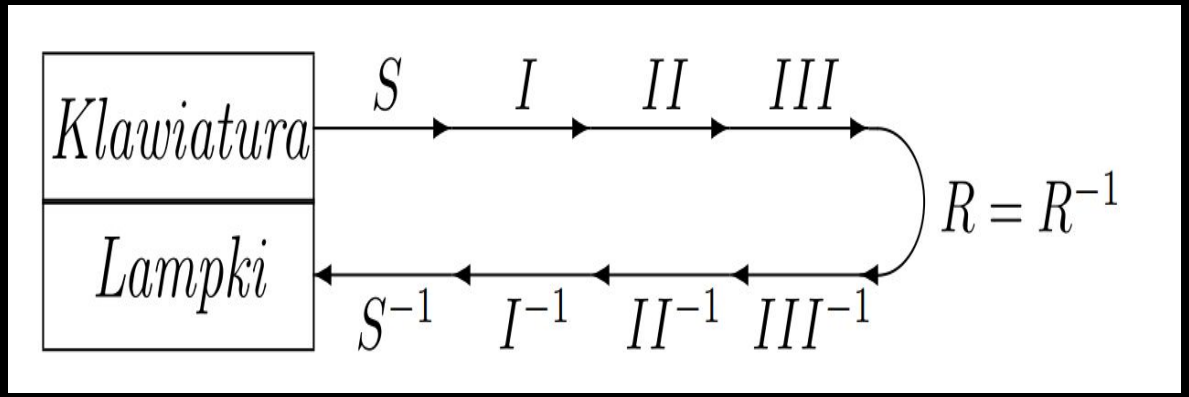
X_n = {1, ..., n} - zbiór n elementowy (u nas n = 26, aby $X_n \cong$ {a, b, c, ..., z})

S_n - zbiór bijekcji z X_n do X_n (permutacji)

Wraz z działaniem ∘, S_n tworzy grupę (S_n, ∘) zwaną grupą permutacji.

Twierdzenie:

Dowolną permutację $\sigma \neq e \in S_n$ można przedstawić w postaci iloczynu cykli rozłącznych długości ≥ 2.



$$S = (a_1b_1)\ldots(a_6b_6) = S^{-1}$$

$$I = P^{\alpha+1}NP^{-\alpha-1}$$

$$II = P^{\beta}MP^{-\beta}$$

$$III = P^{\gamma}LP^{-\gamma}$$

Sposób szyfrowania depeszy

Jeżeli S, α, β, i γ to klucz dzienny, a α^*, β^*, i γ^* to wybierany przez szyfranta klucz depeszy, to początek każdej depeszy był postaci

$$A_1(\alpha^*), A_2(\beta^*), A_3(\gamma^*), A_4(\alpha^*), A_5(\beta^*), A_6(\gamma^*),$$

gdzie A_i , $i = 1, \ldots, 6$, to permutacje, które danego dnia były stałe oraz dało się je rozłożyć na transpozycje rozłączne - wtedy cechowała je równość $A_i = A_i^{-1}$.

Sposób szyfrowania depeszy

Odtworzenie połączeń wewnętrznych

Chcąc otrzymać połączenia wewnętrzne otrzymujemy

$$A_i = S^{-1}P^{\alpha+1}N^{-1}P^{-\alpha-1}QP^{\alpha+1}NP^{-\alpha-1}S,$$

$i = 1, \ldots, 6$, gdzie $Q = P^{\beta}M^{-1}P^{-\beta+\gamma}L^{-1}P^{-\gamma}RP^{\gamma}LP^{-\gamma+\beta}MP^{-\beta}$.

W ten sposób otrzymujemy układ 6 równań z 4 niewiadomymi - S, N, Q, α. Jest to układ, w którym jako niewiadomymi lub współczynnikami są permutacje.

Odtworzenie połączeń wewnętrznych

Teoria grup permutacji oraz ich struktura cykliczna pozwoliła Rejewskiemu znajdować początkowe ustawienia bębenków, tzn. znaleźć używany klucz. Ponadto poprzez rozwiązywanie równań z permutacjami potrafił odczytywać ustawienie łącznicy, która zwiększała liczbę kombinacji szyfru oraz znacznie utrudniała złamanie kodu.

CAUCHY

O

Z

M

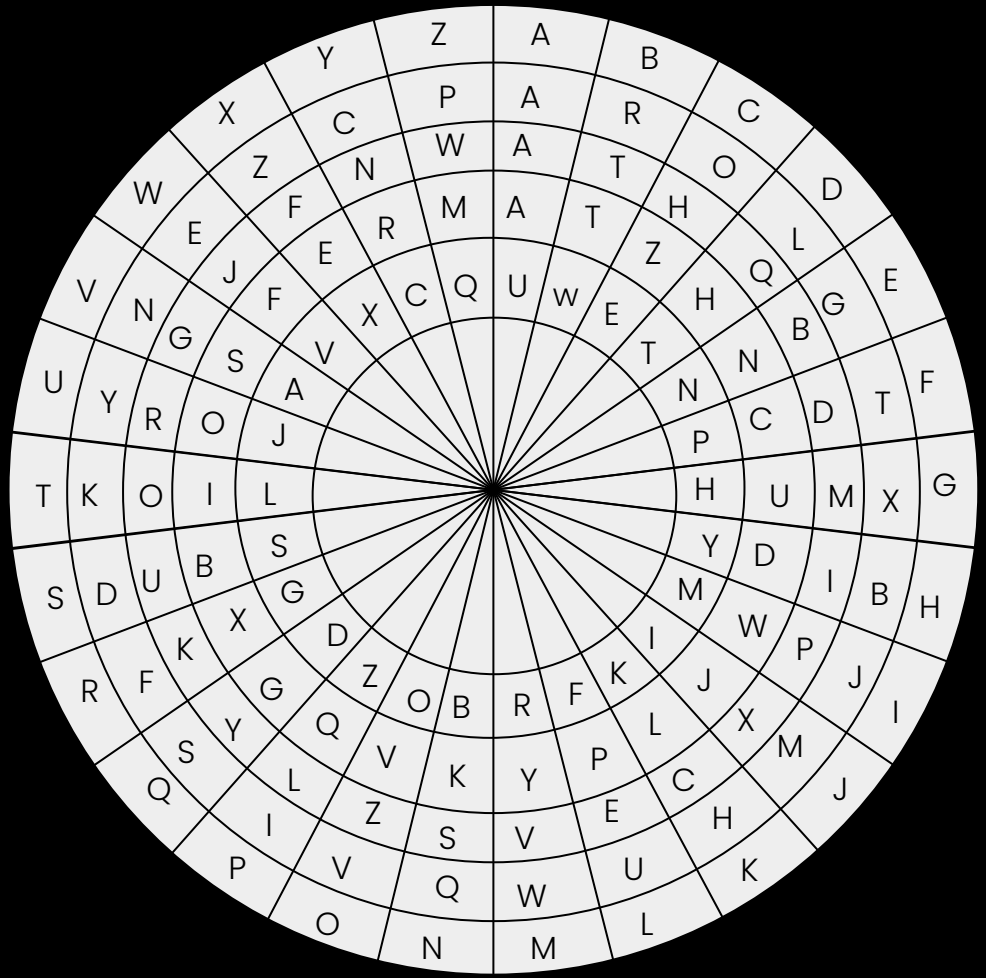
...

R

X

F

TYVDHB



Gwido Langer

Śmierć
1948

Pochówek w Polsce
2010

1945
Koniec wojny i zakończenie działalności Biura Szyfrów

1951
Śmierć

2008
Pochówek w Polsce

Maksymilian Ciężki

Powojenne losy

Marian Rejewski

1945 Koniec wojny i zakończenie działalności Biura Szyfrów

1973 Powrót do rodzinnej Bydgoszczy

Uniwersytet w Surrey

1978 Śmierć

1979 Wspomnienia Bertranda

1980 Film "Sekret Enigmy"

2000 Śmierć

Order Odrodzenia Polski

2014 Odznaczenie IEEE "Milestone"

2019 Symboliczny pochówek w krypcie Panteonu Narodowego

Henryk Zygalski

Powojenne losy

Źródła

https://www.theguardian.com/technology/2014/nov/14/how-did-enigma-machine-work-imitation-game

https://brilliant.org/wiki/enigma-machine/

https://www.history.co.uk/articles/the-polish-cryptographers-who-cracked-the-enigma-code

https://www.youtube.com/watch?v=3Jj0kMt-xn4

https://www.youtube.com/watch?v=OGEGjP8wdc8

https://www.youtube.com/watch?v=gc2NSljAMtc

https://www.youtube.com/watch?v=xshzDya8ZEk

https://gamma.im.uj.edu.pl/~blocki/enigma/inaug.pdf

https://www.youtube.com/watch?v=sOcTWaqFF3A&t=1075s

Dziękujemy za uwagę

Stanisław Boczarski, Dominik Dygas, Franciszek Gajownik, Karol Zaremba