Kryptolodzy z Uniwersytetu Poznańskiego i niemiecka maszyna szyfrująca Enigma

Wydział Matematyki i Informatyki UAM

Poznańska Fundacja Matematyczna

Projekt: Potęga matematyki – 2017

Magdalena Jaroszewska

Bartosz Naskręcki

Motto wykładu

Naród, który nie zna swoich dziejów,
zatraca swą tożsamość

św. Jan Paweł II

Plan wykładu

1. Wprowadzenie: Trzej kryptolodzy, Enigma.
2. Początki Uniwersytetu w Poznaniu i matematyki na Uniwersytecie
3. Kurs szyfrów na Uniwersytecie Poznańskim.
4. Trzej kryptolodzy, 1930-1939.
5. Kryptologia, szyfry podstawieniowe.
6. Historia Enigmy.
7. Enigma wojskowa – budowa, zasada działania.
8. Enigma a matematyka.
9. Urządzenia polskie wspomagające rozszyfrowywanie Enigmy.

Plan wykładu, cd.

10. Trzej kryptolodzy w czasie II wojny światowej.
11. Losy Mariana Rejewskiego i Henryka Zygalskiego po II wojnie światowej.
12. Kryptologia na WMiI UAM.
13. Pamięć o kryptologach, oddanie im czci.
14. Marian Rejewski „*Wspomnienia…..*”.
15. Znaczenie złamania Enigmy.
16. Źródła.

WPROWADZENIE. TRZEJ KRYPTOLODZY

Marian Rejewski
(1905-1980)
z Bydgoszczy

Jerzy Różycki
(1909-1942)
z Guberni Kijowskiej

Henryk Zygalski
(1908-1978)
z Poznania

WPROWADZENIE. ENIGMA WOJSKOWA

POCZĄTKI UNIWERSYTETU W POZNANIU I MATEMATYKI NA UNIWERSYTECIE

Zamek Cesarski w Poznaniu

Początki Uniwersytetu Poznańskiego i matematyki na UP

4.4.1919 - Wydział Filozoficzny,
pierwszy, i jedyny wówczas. W nim
- sekcja nauk matematyczno-przyrodniczych,
- dwie katedry matematyki

1919 - prof. Zdzisław Krygowski (ze Lwowa)
- prof. Franciszek Włodarski (z W-wy)

1924/25 - Wydział Mat-Przyrodniczy powstał z sekcji

1919-1939 - około 160 studentów matematyki, przeciętnie rocznie,

1936/37 - 77 kobiet i 82 mężczyzn

Każdego roku - około 20 osób uzyskiwało dyplom.

KURS SZYFRÓW NA UNIWERSYTECIE POZNAŃSKIM 1929/1930

Miejsce:

Budynek Komendy Miasta (obok Zamku,

2 razy w tygodniu, wieczorami).

Uczestnicy kursu, studenci matematyki, 26 osób, ich cechy: bdb wyniki w nauce, j. niemiecki, dobra intuicja, sumienność, cierpliwość, dokładność, przykładni obywatele RP.

Cel kursu (nieznany uczestnikom) – złamanie Enigmy.

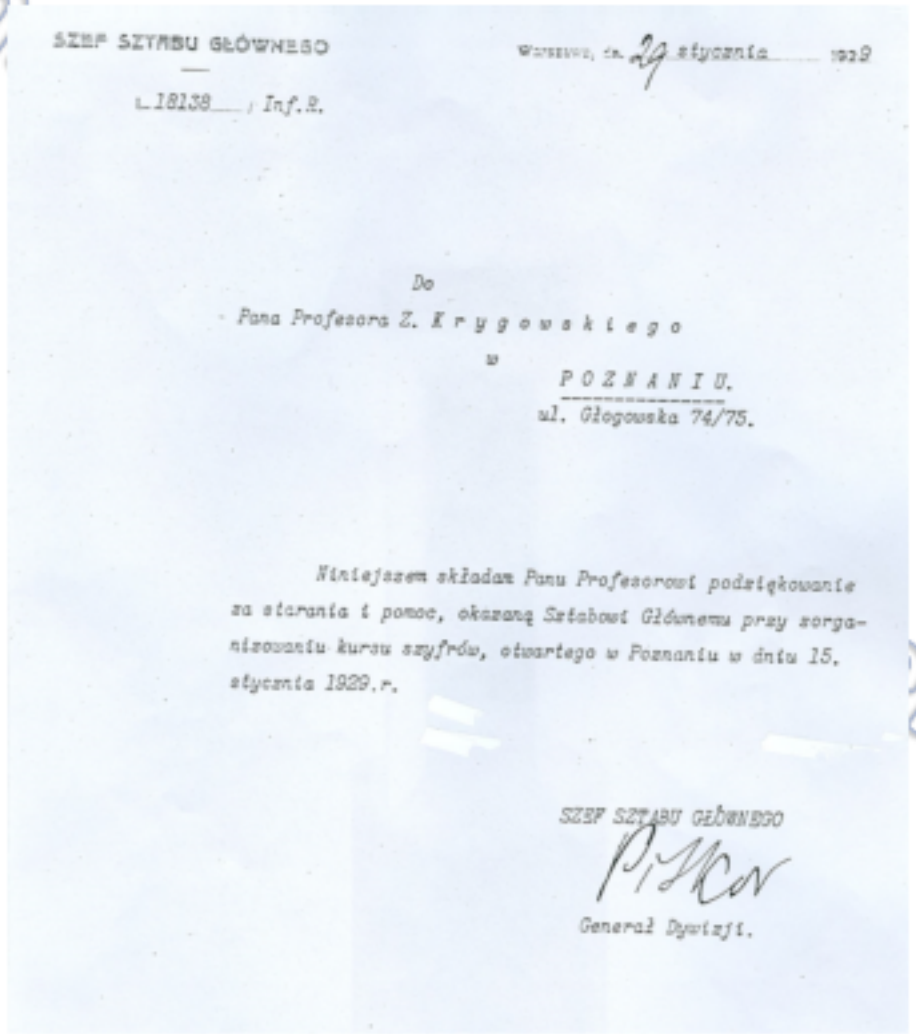
Kurs szyfrów na Uniwersytecie Poznańskim - kadra

kpt. Maksymilian Ciężki
1898-1951
ur. Szamotuły

płk Gwido Langer
1894-1948
ur. w Słowacji

inż. Antoni Palluth
1900-1944
ur. Pobiedziska

KURS SZYFRÓW NA UP, 1929/30, PODZIĘKOWANIE GENERAŁA TADEUSZA PISKORA



SZEF SZTABU GŁÓWNEGO

Warszawa, dn. 29 stycznia 1929

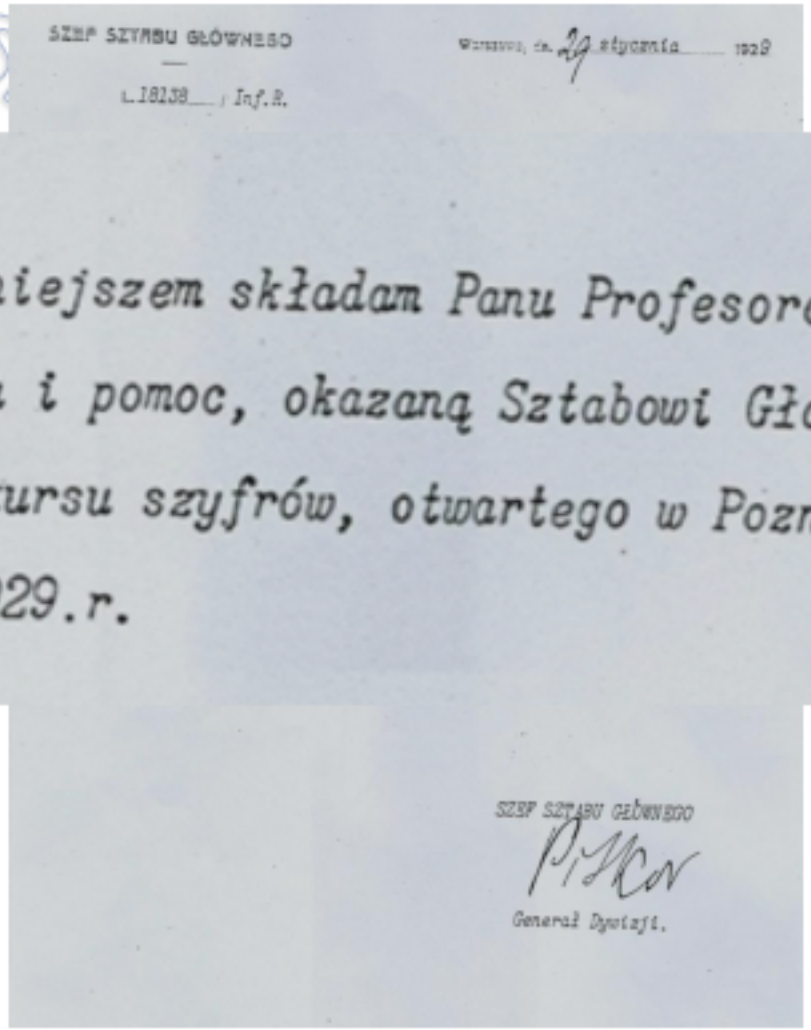
L. 18138 / Inf. R.

Do
Pana Profesora Z. K r y g o w s k i e g o
w
P O Z N A N I U.
ul. Głogowska 74/75.

Niniejszem składam Panu Profesorowi podziękowanie za starania i pomoc, okazaną Sztabowi Głównemu przy zorganizowaniu kursu szyfrów, otwartego w Poznaniu w dniu 15. stycznia 1929.r.

SZEF SZTABU GŁÓWNEGO
Piłsudski
Generał Dywizji.

Kurs szyfrów. Podziękowanie Gen Tadeusza Piskora szefa Sztabu Gł. WP



SZEF SZTABU GŁÓWNEGO

L.18138 Inf.R.

Warszawa, dn. 29 stycznia 1929

Niniejszem składam Panu Profesorowi podziękowanie za starania i pomoc, okazaną Sztabowi Głównemu przy zorganizowaniu kursu szyfrów, otwartego w Poznaniu w dniu 15. stycznia 1929.r.

SZEF SZTABU GŁÓWNEGO

Piskor

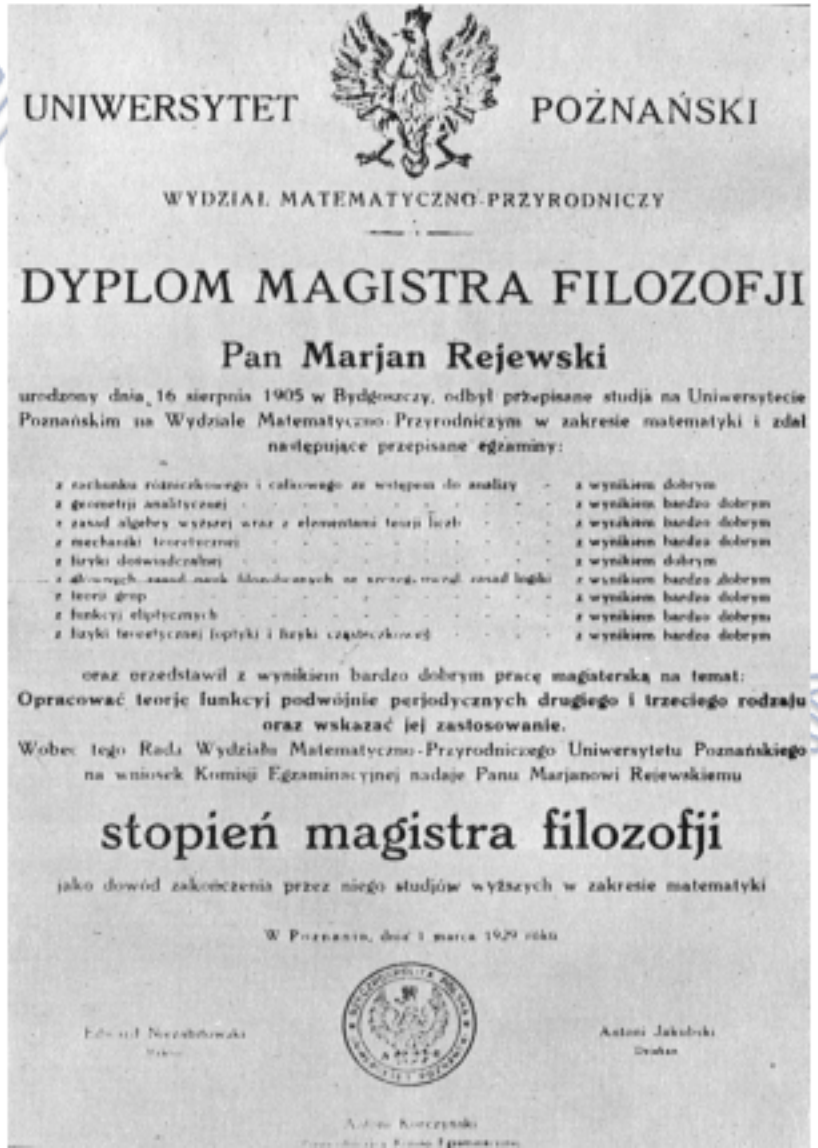
Generał Dywizji.

POCZĄTKI UNIWERSYTETU W POZNANIU I MATEMATYKI NA UNIWERSYTECIE

prof. Zdzisław Krygowski (1872-1955)

- **1919-1938 organizator, pionier matematyki na UP,**
- **kierownik katedry matematyki,**
- **dziekan,**
- **prorektor Uniwersytetu Poznańskiego,**
- **matematyka klasyczna: algebra, teoria Galois, krzywe eliptyczne.**

MARIAN REJEWSKI
DYPLOM STUDIÓW MATEMATYCZNYCH na UP



UNIWERSYTET POZNAŃSKI

WYDZIAŁ MATEMATYCZNO-PRZYRODNICZY

DYPLOM MAGISTRA FILOZOFJI

Pan Marjan Rejewski

urodzony dnia 16 sierpnia 1905 w Bydgoszczy, odbył przepisane studja na Uniwersytecie Poznańskim na Wydziale Matematyczno-Przyrodniczym w zakresie matematyki i zdał następujące przepisane egzaminy:

z rachunku różniczkowego i całkowego ze wstępem do analizy	z wynikiem dobrym
z geometrji analitycznej	z wynikiem bardzo dobrym
z zasad algebry wyższej wraz z elementami teorji liczb	z wynikiem bardzo dobrym
z mechaniki teoretycznej	z wynikiem bardzo dobrym
z fizyki doświadczalnej	z wynikiem dobrym
z ogólnych zasad nauk filozoficznych ze szczeg. uwzgl. zasad logiki	z wynikiem bardzo dobrym
z teorji grup	z wynikiem bardzo dobrym
z funkcyj eliptycznych	z wynikiem bardzo dobrym
z fizyki teoretycznej (optyki i fizyki cząsteczkowej)	z wynikiem bardzo dobrym

oraz przedstawił z wynikiem bardzo dobrym pracę magisterską na temat:
Opracować teorję funkcyj podwójnie perjodycznych drugiego i trzeciego rodzaju oraz wskazać jej zastosowanie.
Wobec tego Rada Wydziału Matematyczno-Przyrodniczego Uniwersytetu Poznańskiego na wniosek Komisji Egzaminacyjnej nadaje Panu Marjanowi Rejewskiemu

stopień magistra filozofji

jako dowód zakończenia przez niego studjów wyższych w zakresie matematyki

W Poznaniu, dnia 1 marca 1929 roku

Edward Nowakowski
Rektor

Antoni Jakubski
Dziekan

Antoni Kuczyński
Sekretarz Komisji Egzaminacyjnej

Marian Rejewski

dyplom studiów matematycznych na UP

UNIWERSYTET POZNAŃSKI

WYDZIAŁ MATEMATYCZNO-PRZYRODNICZY

z rachunku różniczkowego i całkowego ze wstępem do analizy	z wynikiem dobrym
z geometrji analitycznej	z wynikiem bardzo dobrym
z zasad algebry wyższej wraz z elementami teorji liczb	z wynikiem bardzo dobrym
z mechaniki teoretycznej	z wynikiem bardzo dobrym
z fizyki doświadczalnej	z wynikiem dobrym
z głównych zasad nauk filozoficznych ze szczególnem uwzgl. zasad logiki	z wynikiem bardzo dobrym
z teorji grup	z wynikiem bardzo dobrym
z funkcyj eliptycznych	z wynikiem bardzo dobrym
z fizyki teoretycznej (optyki i fizyki cząsteczkowej)	z wynikiem bardzo dobrym

stopień magistra filozofji

jako dowód zakończenia przez niego studjów wyższych w zakresie matematyki

W Poznaniu, dnia 1 marca 1929 roku

Edward Niezabitowski
Rektor

Antoni Jakubski
Dziekan

Trzej kryptolodzy, 1930-1939

- 1930-1932 praca w filii Biura Szyfrów w Poznaniu,
- 1932-1939 praca w Biurze Szyfrów przy Sztabie Głównym w dziale szyfrów niemieckich w Warszawie; Plac Saski, Las Kabacki (MR, JR, HZ),
- 1932 grudzień ostatnie dni Rejewski odtworzył wewnętrzną konstrukcję Enigmy i odczytał pierwsze zaszyfrowane nią depesze,
- zespół trzech kryptologów podjął wspólny atak na niemieckie szyfry maszynowe.

Jerzy Różycki - rozmowa z matką

Wanda Różycka matka Jerzego w 1935 roku w Warszawie zadała pytanie synowi:

„Z czego ty Jerzy żyjesz, gdzie pracujesz? Skąd masz pieniądze na drogie garnitury i kosztowne wczasy w Alpach francuskich?”

Odpowiedź Jerzego Różyckiego:

„Nie mogę ci mamo odpowiedzieć teraz, gdzie pracuję i u kogo, ale nie kradnę i nie zabijam nikogo, ale kiedyś, gdy się dowiesz co robię, to będziesz ze mnie bardzo, bardzo DUMNA! A może wręcz dumna będzie ze mnie nawet cała Polska !”

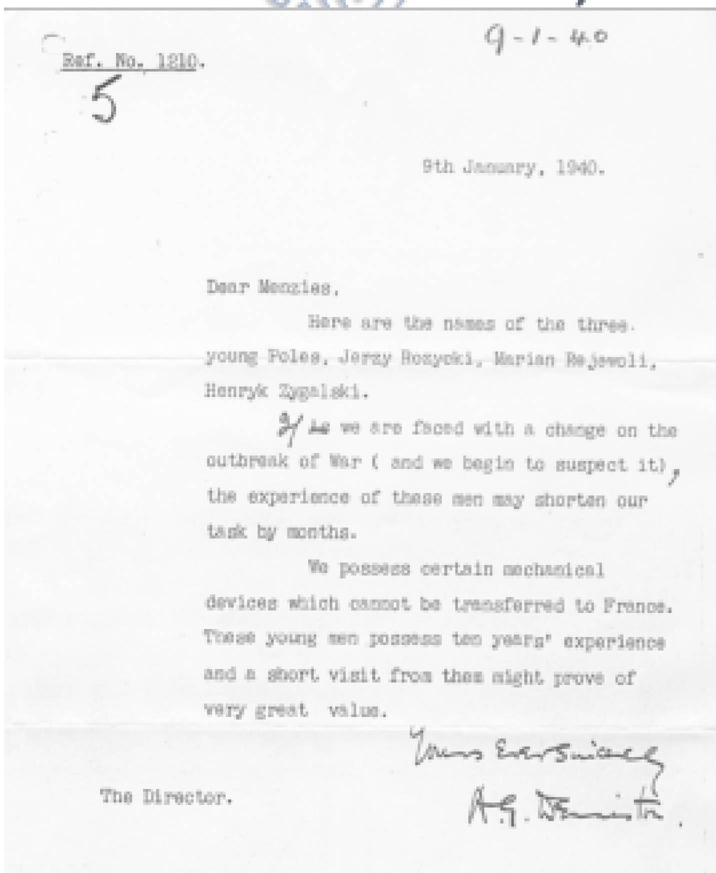
PRZEKAZANIE ALIANTOM TAJEMNICY

- 25-27 lipca 1939 roku przekazano Francji i Anglii, w Lesie Kabackim podczas zorganizowanej konferencji, dorobek polskich kryptologów:
  - skonstruowane w Polsce kopie Enigmy,
  - materiały dotyczące metod pracy, czyli szyfrowania i rozszyfrowywania depesz, m.in. metodę bomb, zegara, płacht i in.
- był to znaczący polski wkład do szybszego zwycięstwa aliantów w II wojnie światowej.

BLETCHLEY PARK, OŚRODEK DEKRYPTAŻU, WIELKA BRYTANIA

BRYTYJCZYCY CHCIELI MIEĆ U SIEBIE TRZECH NASZYCH KRYPTOLOGÓW,

Alastair Denniston, list do Stewarda Menziesa



9-1-40

Ref. No. 1210.

5

9th January, 1940.

Dear Menzies,

Here are the names of the three young Poles, Jerzy Rozycki, Marian Rejewoli, Henryk Zygalski.

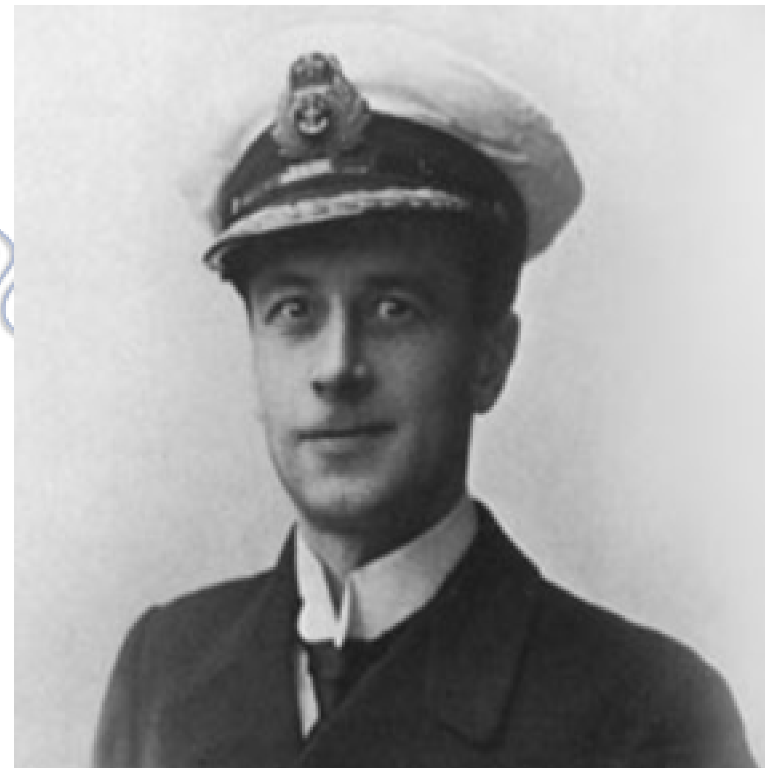
If ~~as~~ we are faced with a change on the outbreak of War (and we begin to suspect it), the experience of these men may shorten our task by months.

We possess certain mechanical devices which cannot be transferred to France. These young men possess ten years' experience and a short visit from them might prove of very great value.

Yours Ever Sincerely

A.G. Denniston.

The Director.



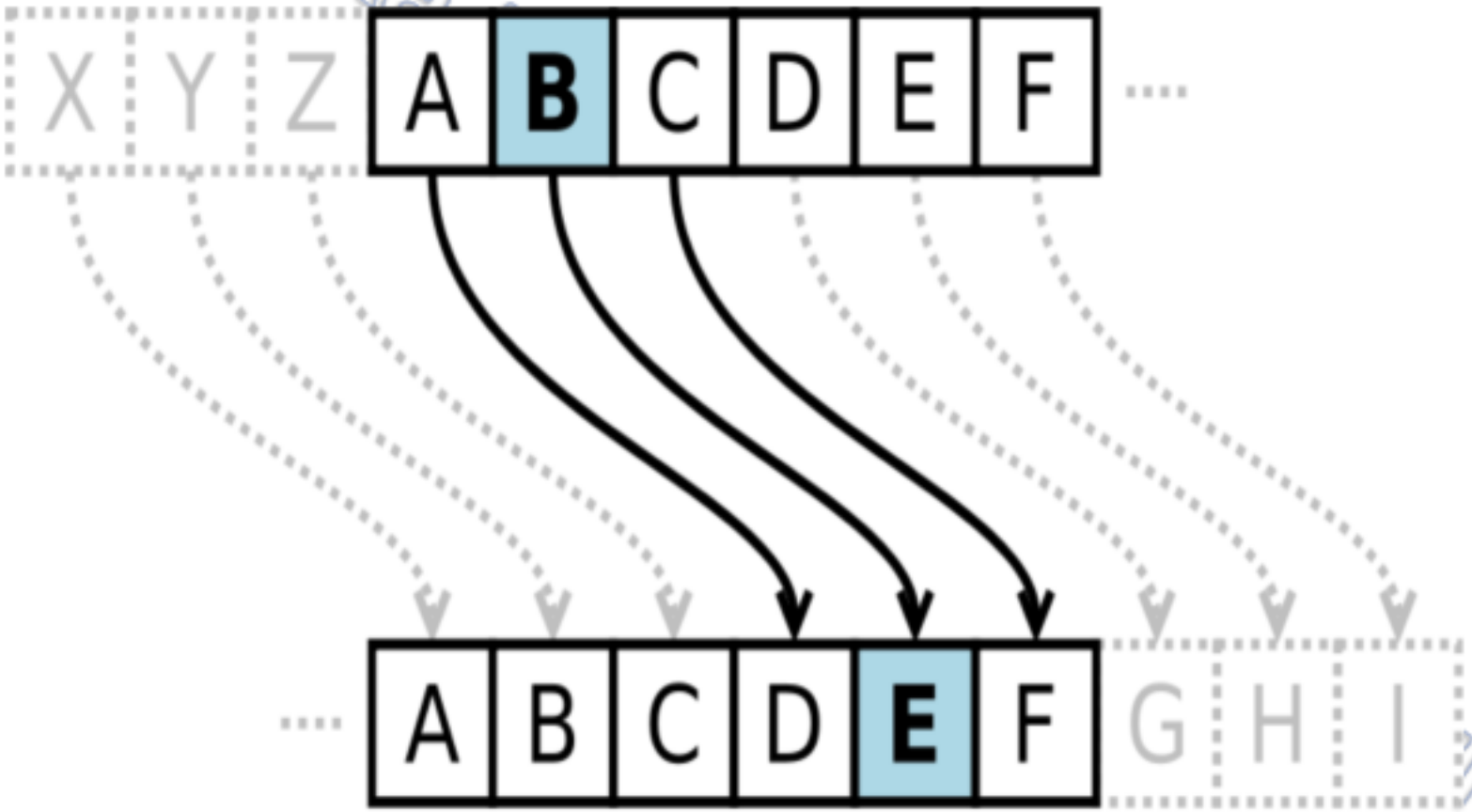
Genialny brytyjski matematyk Alan Turing (1912-1954)

KRYPTOLOGIA, SZYFRY PODSTAWIENIOWE

Kryptologia:

- **Kryptografia to opracowywanie metod utajniania wiadomości i konstrukcja szyfrów,**
- **Kryptoanaliza bada te metody pod kątem ich bezpieczeństwa oraz dostarcza metod służących do łamania szyfrów, to znaczy do odczytywania zaszyfrowanych wiadomości bez znajomości odpowiednich kluczy.**

SZYFR PODSTAWIENIOWY PRZYKŁAD - SZYFR CEZARA (I w. p.n.e.), diagram dwóch ciągów



SZYFROWANIE METODĄ CEZARA. PRZYKŁAD

Alfabet: ABCDEFGHIJKLMNOPRSTUWXYZ

Szyfr: DEFGHIJKLMNOPRSTUWXYZABC

tekst jawny: **E N I G M A**

tekst zaszyfrowany: **H R L J P D**

Historia Enigmy

1919 Hugo Koch holenderski wynalazca, opatentował projekt maszyny szyfrującej, później inżynier Arthur Scherbius spod Berlina zbudował prototypy maszyn szyfrujących. Były to maszyny typu handlowego dla instytucji wymagających tajnej korespondencji

Maszyna Scherbiusa to Enigma, zakupiły ją:

1926 Reichsmarine, później Kriegsmarine,

1929 Reichswehra, inne jednostki wojskowe.

ENIGMA WOJSKOWA, BUDOWA, ZASADA DZIAŁANIA

Skrzynka - 13 kg,
wymiary:
34 x 28 x 18 (cm);
po 26 liter alfabetu:
klawiatura -
wprowadz. depeszy,
szyfrowanie:
bębenki/wirniki -
mieszacz, łącznica
wtyczkowa, żarówki
(tekst zaszyfrowany)
bateria, instrukcja.

Schemat budowy Enigmy

Ustawienie wirników

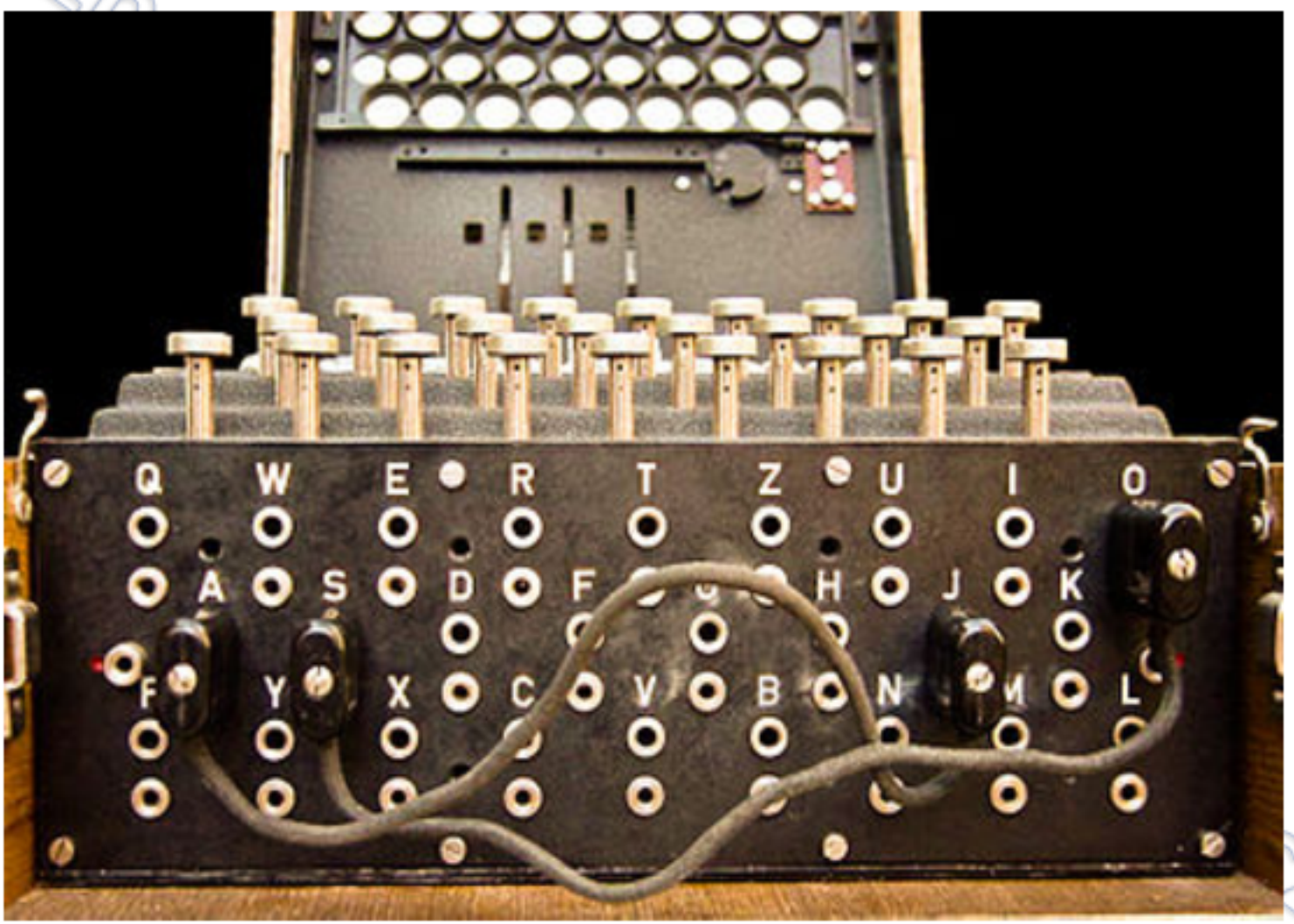
Pole wyświetlania zaszyfrowanych liter

Klawiatura szyfranta

Enigma, wirniki/bębenki

ŁĄCZNICA KABLOWA,

PRZEWODY ŁĄCZĄ DWIE PARY LITER: SO I JA



SZYFROWANIE DEPESZY

- Kolejność wirników: II – III – I
- Ustawienia pierścieni: BCD
- Ustawienie łącznicy: **A/P, B/L, C/Z, F/H, J/K, Q/U**
- Ustawienia wirników: SDK (19-04-11)
- Indywidualny klucz depeszy: HBN

  HBNHBN (podwójnie podany klucz)

  CAURAC (podwójny szyfr klucza)
- Szyfrujemy wiadomość:

  POZDROWIENIA Z FESTIWALU

- Przesyłamy wiadomość:

  CAURACWHTTEWDUTLPHRMXBRRAHOQ