

ZŁAMANIE SZYFRU ENIGMY



INSTYTUT
PAMIĘCI
NARODOWEJ

Autorzy wystawy:

Julia Kilanowska
dr Izabella Kopczyńska

Witold Sobócki

Koncepcja graficzna serii: Aleksandra Kaiper-Miszułowicz

Koncepcja plastyczna: dr Karolina Zielazek-Szeska

Korekta: Ilona Kaczmarek

Recenzja: dr Piotr Grzelczak, dr hab. Filip Musiał

Fotografie i dokumenty:

Archiwum Uniwersytetu im. Adama Mickiewicza w Poznaniu, Bundesarchiv,
Narodowe Archiwum Cyfrowe, Polona, Cryptomuseum.com,
Instytut Piłsudskiego w Londynie, zbiory p. Marii Bryszak
oraz p. Janiny Sylwestrzak

Autorzy składają serdeczne podziękowania pracownikom Centrum Szyfrów
Enigma w Poznaniu za okazaną pomoc podczas tworzenia wystawy.

Maszyna szyfrująca Enigma – widok klawiatury
Fot. Bundesarchiv, 183-2007-0705-502/Walther, 1943 r.

RADIOWYWIAD W NIEPODLEGŁEJ

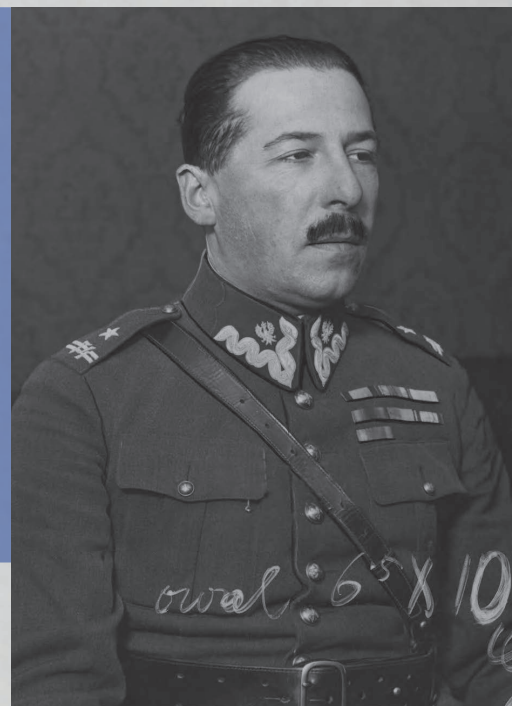
SZTAB GENERALNY.

Tylko do użytku służbowego.

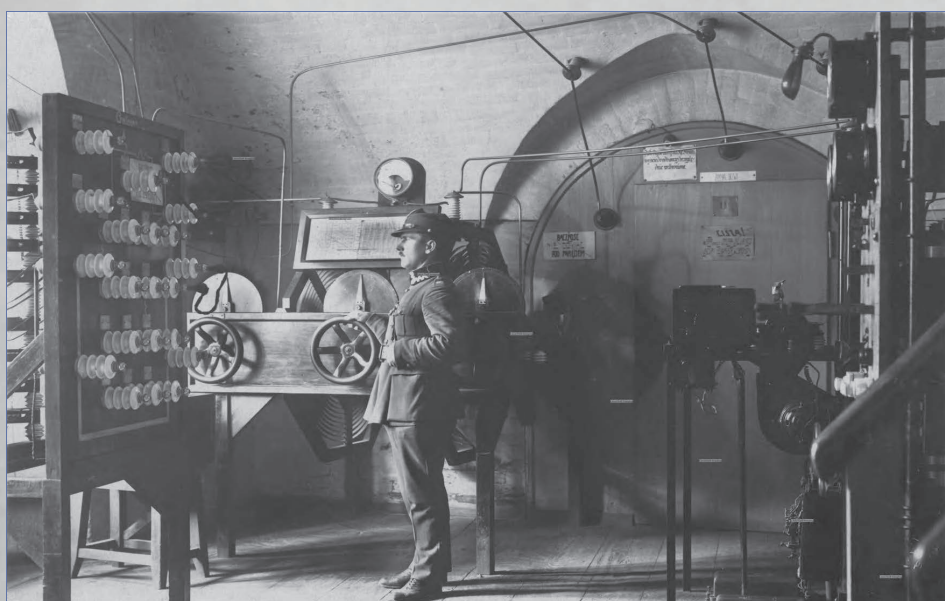
Radjotelegrafia

W Polsce, od momentu odzyskania niepodległości w 1918 r., Naczelne Dowództwo Wojska Polskiego stworzyło sieć stałych i polowych stacji radiotelegraficznych. Zajmowały się one nie tylko obsługą korespondencji własnej, ale także nasłuchem obcych sygnałów radiowych wszystkich sąsiadów Polski.

Sukces kryptologiczny porucznika Jana Kowalewskiego, jakim było złamanie sowieckiego szyfru podczas wojny polsko-bolszewickiej latem 1919 r., przyczynił się do pokonania bolszewików w 1920 r. oraz powstania w Sztabie Głównym Wojska Polskiego komórki zajmującej się kryptologią i radio-wywiadem: Biura Szyfrów. Kontynuowało ono pracę w czasie pokoju.



Jan Kowalewski w mundurze (1892-1965), fotografia portretowa
Fot. NAC



Wnętrze Centralnej Stacji Radiotelegraficznej na Cytadeli w Warszawie, ok. 1919 r.
Fot. NAC

Podczas wojny polsko-bolszewickiej używano radia nie tylko do poznania sowieckich zamiarów. W trakcie Bitwy Warszawskiej Polakom skutecznie udało się zagłuszyć łączność przeciwnika nadając tekst Pisma Świętego.

WARSZAWA.—1919.

NAKŁADEM KURSU OFICERÓW SZTABU GENERALNEGO.



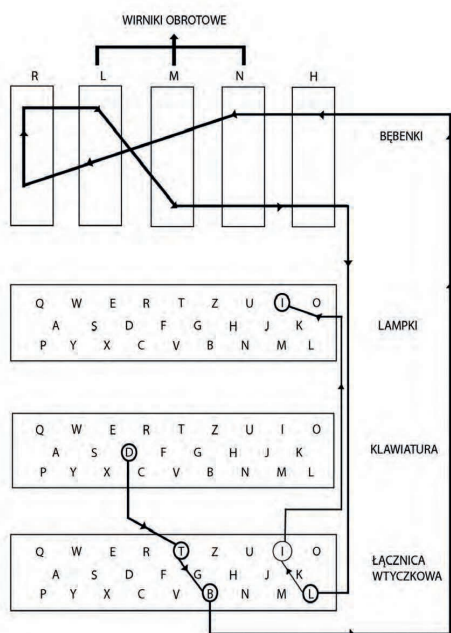
INSTYTUT
PAMIĘCI
NARODOWEJ

Okładka podręcznika *Radjotelegrafia*, 1919 r.
Fot. POLONA

PROBLEM ENIGMY



Schemat działania trózwirnikowej Enigmy wojskowej
Koncepcja: Witold Sobócki, rysunek: Karolina Zielazek-Szeska



Maszynowy szyfr generowany przez Enigmę uniemożliwiał w kryptoanalizie stosowanie metod lingwistycznych. Do odczytania depesz potrzebny był identyczny model maszyny z dokładnie takimi samymi, okresowo zmienianymi ustawieniami początkowymi. Samo urządzenie także ewoluowało: udoskonalono procedury jego używania oraz zmieniono konstrukcję. Wszystkie te zabiegi powodowały, że Enigma uważana była za maszynę nie do złamania.

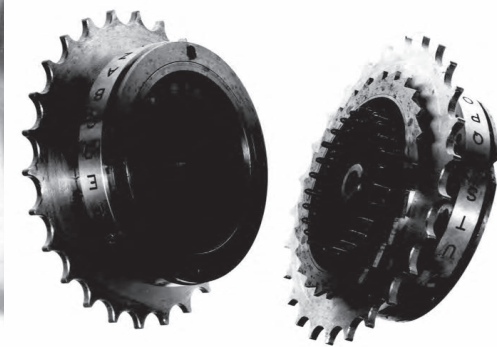
Niemiecka maszyna szyfrująca Enigma, opatentowana w 1918 r., pierwotnie była przeznaczona na rynek cywilny z myślą o utajnieniu korespondencji przez banki, urzędy pocztowe oraz duże przedsiębiorstwa. Działając w interesie bezpieczeństwa państwa, polski wywiad skutecznie rozpracowywał niemiecką militarną łączność radiową. Sytuację zmieniło wprowadzenie przez Niemców w drugiej połowie lat dwudziestych maszyny Enigma do użytku w marynarce wojennej oraz w wojskach lądowych. Wersje wojskowe maszyny różniły się od handlowego pierwowzoru znacznym skomplikowaniem algorytmu szyfrującego.



Model wojskowej Enigmy z widocznymi trzema wirnikami oraz łącznicą
Fot. Fot. United States Government Work, domena publiczna

PIERWSZE PRÓBY

Rozpracowaniem Enigmy, oprócz Polaków, zajmowały się bezskutecznie francuskie oraz brytyjskie służby wywiadowcze. Polscy kryptolodzy uciekali się do niestandardowych metod. Szyfrogramy przekazano m.in. do analizy słynnemu jasnowidzowi inż. Stefanowi Ossowieckiemu. Nieszablonowe podejście do problemu zaowocowało w przyszłości.



Worniki Enigmy
Fot. Instytut Piłsudskiego w Londynie

Podstawową trudnością stojącą przed kryptologiem usiłującym złamać szyfr Enigmy była nieznanomość wewnętrznych elementów maszyny: okablowania łącznicy, wałka wejściowego, poszczególnych wórków oraz reflektora. Dane na temat tych części były doskonale chronione przez Niemców.



Prof. Stefan Mazurkiewicz (1888-1945)
Fot. NAC

Jeszcze podczas wojny polsko-bolszewickiej polski wywiad współpracował w zakresie kryptoanalizy z warszawskimi matematykami – Stanisławem Leśniewskim, Stefanem Mazurkiewiczem oraz Wacławem Sierpińskim. Biuro Szyfrów postanowiło zwrócić się do nich o pomoc w sprawie Enigmy. Niestety matematycy nie potrafili sobie poradzić nawet z niemieckimi depeszami utajnionymi bez użycia maszyny.

Niemieccy żołnierze obsługujący Enigmę
Fot. Bundesarchiv, 183-L22303/ Mess, 1940 r.



KURS W POZNANIU

For Official Use Only

WAR DEPARTMENT
OFFICE OF THE CHIEF SIGNAL OFFICER
WASHINGTON

COURSE IN CRYPTOGRAPHY

By
GENERAL MARCEL GIVIERGE

Translated From the Original "Cours de Cryptographie"

DEREGISTERED
18 MAR 58

By
JOHN B. HURT, *Cryptanalyst Aide*

SIGNAL INTELLIGENCE SECTION
WAR PLANS AND TRAINING DIVISION



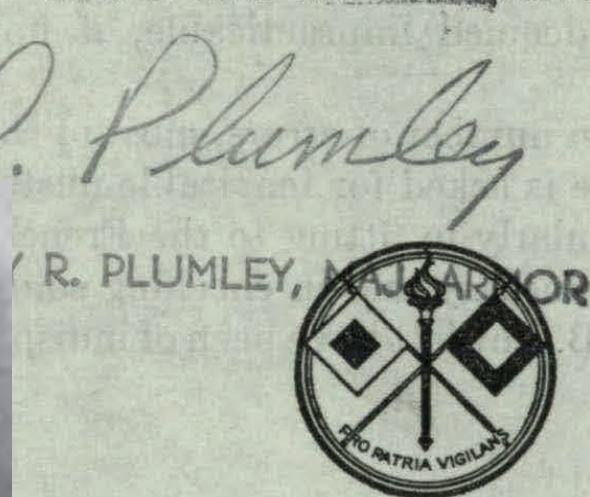
Zdzisław Krygowski (1872-1955)
Fot. Archiwum UAM

Profesor związany z lwowską szkołą matematyczną. Polski matematyk i kierownik Katedry Matematyki na Uniwersytecie Poznańskim.

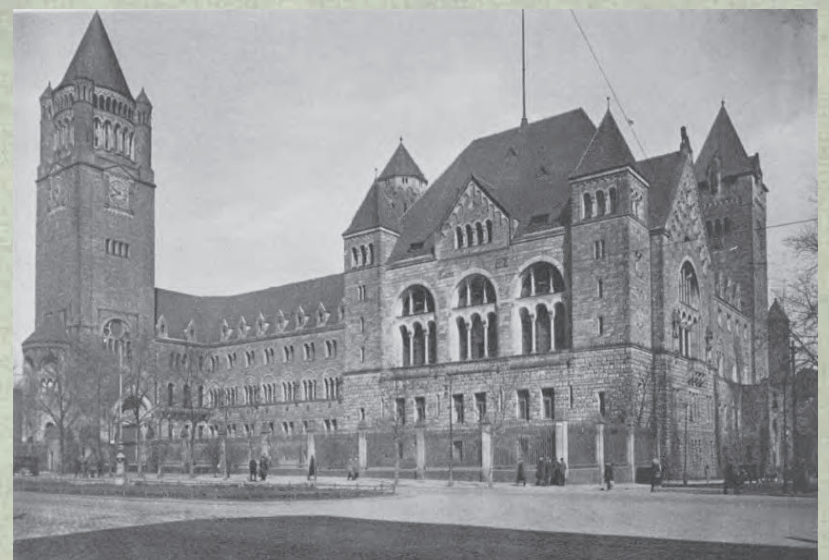


Maksymilian Ciężki (1898-1951)
Fot. Domena publiczna

Szef Sekcji Niemieckiej Biura Szyfrów, oficer wojsk łączności, powstaniec wielkopolski.



UNITED STATES
GOVERNMENT PRINTING OFFICE
WASHINGTON : 1934



Zamek Cesarski w Poznaniu
Fot. POLONA

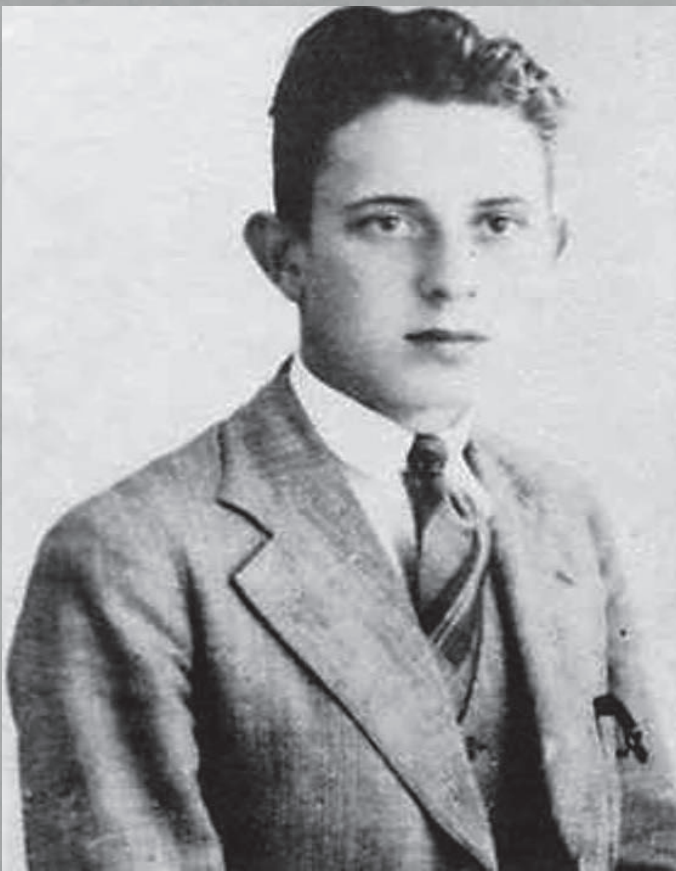
W 1929 r. oficerowie Biura Szyfrów postanowili ponownie zaangażować matematyków do złamania szyfru maszyny Enigma. Kurs kryptologiczny zorganizowano z inicjatywy Maksymiliana Ciężkiego dla studentów Wydziału Matematyczno-Przyrodniczego Uniwersytetu Poznańskiego. Na polecenie Oddziału II Sztabu Głównego, Zdzisław Krygowski miał zorganizować kurs i wyłonić najzdolniejszych studentów. Wybrano Poznań z uwagi na wysoki poziom nauczania i dobrą znajomość języka niemieckiego wśród studentów. W czasie kursu największy nacisk położono na łamanie szyfru podwójnego przestawienia.

Marcel Givierge, *Cours de Cryptographie*. Zakres i materiał kursu opierał się na wydanym w 1925 r. podręczniku *Cours de Cryptographie*. Na fotografii zaprezentowano wydanie amerykańskie tej publikacji.
Fot. Archive.org



INSTYTUT
PAMIĘCI
NARODOWEJ

NAJLEPSZE TRIO



Jerzy Różycki (1909-1942)
Fot. Domena publiczna



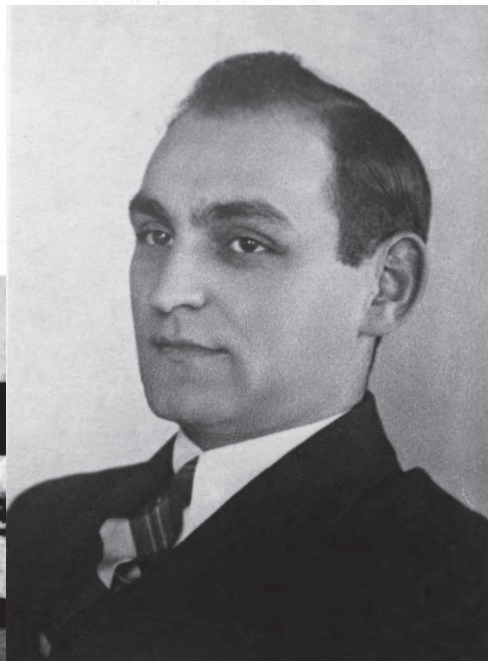
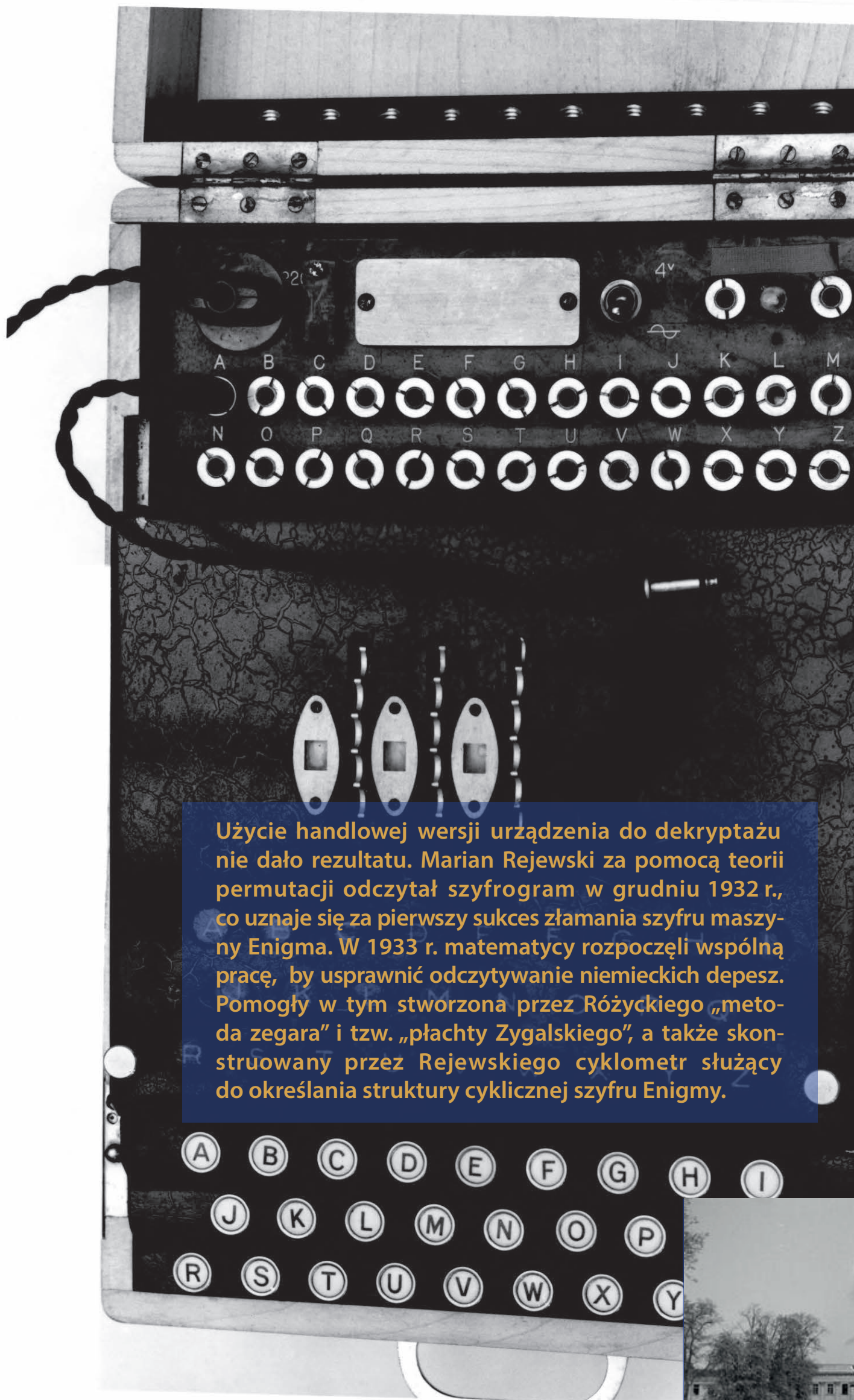
Henryk Zygalski (1908-1978)
Fot. Domena publiczna



W czasie kursu w Poznaniu wyłoniono trójkę najzdolniejszych studentów: Mariana Rejewskiego, Henryka Zygalskiego i Jerzego Różyckiego. Utworzony zespół został zatrudniony w Ekspozyturze Biura Szyfrów w Poznaniu, mieszczącej się przy dzisiejszej ulicy Św. Marcin. Po przeniesieniu do Warszawy grupa nadal pracowała nad powierzonym zadaniem. Poprzez pracę zespołową trzem matematykom udało się osiągnąć sukces, którym było złamanie szyfru maszyny szyfrującej Enigma.



POZNANIE TAJEMNIC



Antoni Palluth (1900-1944)
Fot. ze zbiorów p. Piotra Paluta

Jeden z wykładowców na kursie w Poznaniu w 1929 r. Pracował w Biurze Szyfrów w sekcji niemieckiej. Współtwórca Wytwórni Radiotechnicznej AVA, która stworzyła replikę maszyny szyfrującej Enigma oraz inne urządzenia ułatwiające złamanie niemieckich szyfrogramów.

Użycie handlowej wersji urządzenia do dekryptażu nie dało rezultatu. Marian Rejewski za pomocą teorii permutacji odczytał szyfrogram w grudniu 1932 r., co uznaje się za pierwszy sukces złamania szyfru maszyny Enigma. W 1933 r. matematycy rozpoczęli wspólną pracę, by usprawnić odczytywanie niemieckich depesz. Pomogły w tym stworzona przez Różyckiego „metoda zegara” i tzw. „płachty Zygałskiego”, a także skonstruowany przez Rejewskiego cyklometr służący do określania struktury cyklicznej szyfru Enigmy.



Pałac Saski
Fot. NAC

Siedziba Biura Szyfrów. Tutaj przeniesiono filię poznańskiego Biura. W tym miejscu kontynuowano prace kryptologiczne.



WIDMO WOJNY

We wrześniu 1938r. Niemcy zmienili sposób użycia Enigmy. Wówczas najważniejszym narzędziem ułatwiającym pracę polskich kryptologów była „bomba Rejewskiego” – połączenie sześciu maszyn Enigma. Z uwagi na ekspansywną politykę Adolfa Hitlera (zajęcie Czechosłowacji, roszczenia w stosunku do Polski oraz Anschluss) Biuro Szyfrów w lipcu 1939 r. postanowiło na konferencji w ośrodku kryptologicznym w Pyrach podzielić się ze stroną francuską i brytyjską swoją wiedzą i technikami łamania szyfrów. Do momentu spotkania w Pyrach kryptolodzy brytyjscy i francuscy używali metod, które były niewystarczające do odczytywania niemieckich szyfrów Enigmy.



Gustave Bertrand (1896-1976)

Fot. Domena publiczna

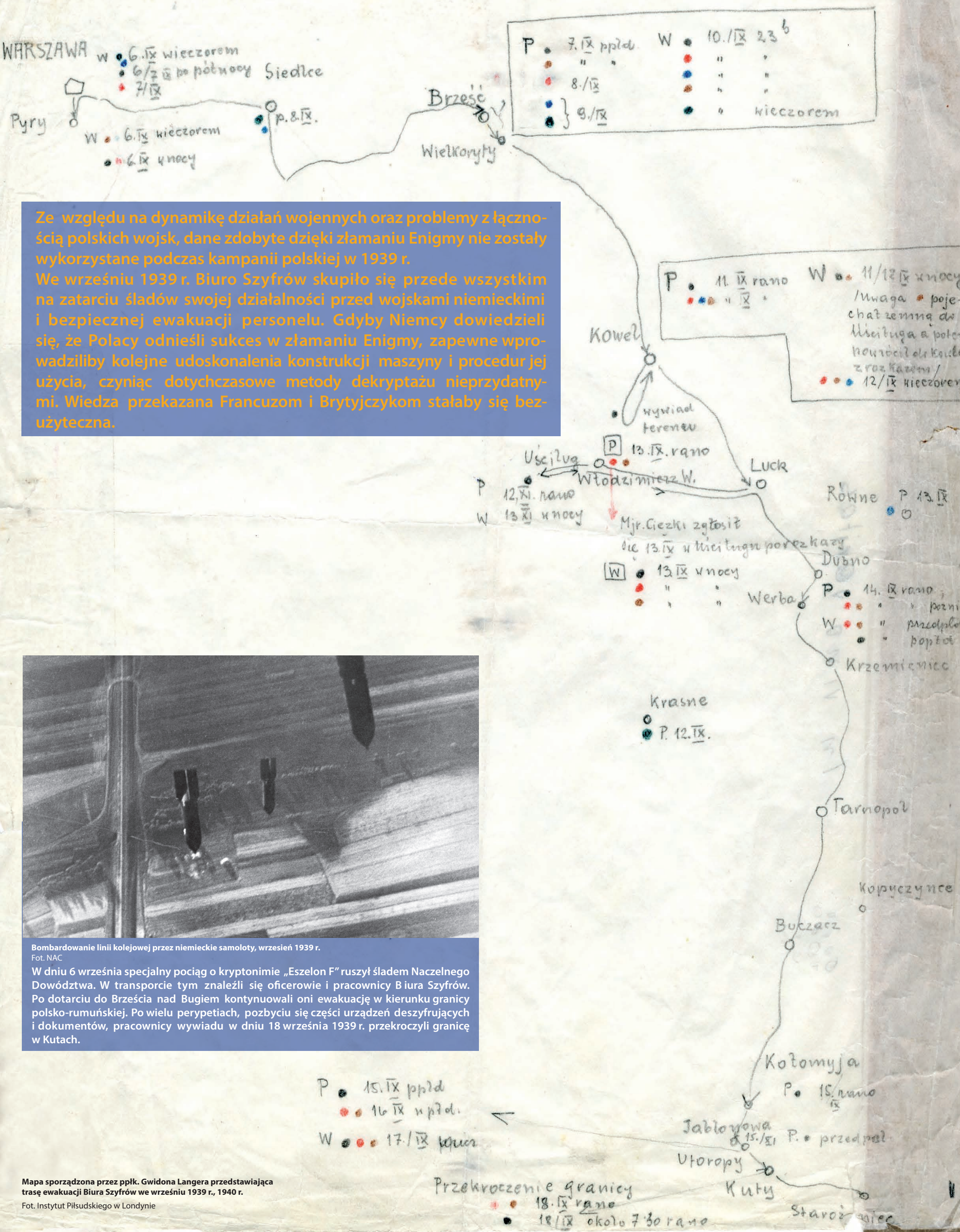
Szef sekcji D szyfrów francuskiego radiowywiadu. Przedstawiciel strony francuskiej w czasie konferencji w Pyrach. Na początku pracy polskich kryptologów przekazał im informacje na temat instrukcji użytkowania maszyny Enigma.



INSTYTUT
PAMIĘCI
NARODOWEJ

Rekonstrukcja wyglądu bomby kryptologicznej na podstawie szkiców ze wspomnień Mariana Rejewskiego
Rysunek: Szymon Pilecki, Szymon Dąbrowski. Licencja CC BY-SA 4.

OCALIĆ SEKRET



BRUNO – CADIX – – ALGIER

Chaotyczne pierwsze miesiące konfliktu zbrojnego nie sprzyjały wznowieniu prac nad odczytywaniem niemieckich depesz. Kluczowa dla powodzenia tych działań była wiedza polskich kryptologów, z czego doskonale zdawał sobie sprawę gen. Gustave Bertrand, usilnie zabiegający o ich obecność we Francji. Na podstawie umowy zawartej pomiędzy tworzącą się Armią Polską we Francji a francuskim dowództwem, Rejewski, Zygalski oraz Różycki znaleźli się najpierw w tajnym ośrodku kryptologicznym Bruno, a następnie w placówce Cadix, gdzie kontynuowali pracę nad dekryptażem.



Zespół pracujący w ośrodku Cadix; na zdjęciu m.in. M. Ciężki, G. Langer, H. Zygalski, J. Różycki, M. Rejewski
Fot. Domena publiczna

Ustronnie położona na obrzeżach miasta willa „Les Fouzes” zdawała się spełniać warunki niezbędne do rozpoczęcia tajnych prac kryptologicznych. Działający w południowej, nieokupowanej przez Niemców części Francji ośrodek Cadix służył przez niespełna dwa lata. W 1942 r. pojawiła się realna groźba dekonspiracji miejsca. Zasadom bezpieczeństwa szkodziło także zbytne zainteresowanie lokalnej ludności.



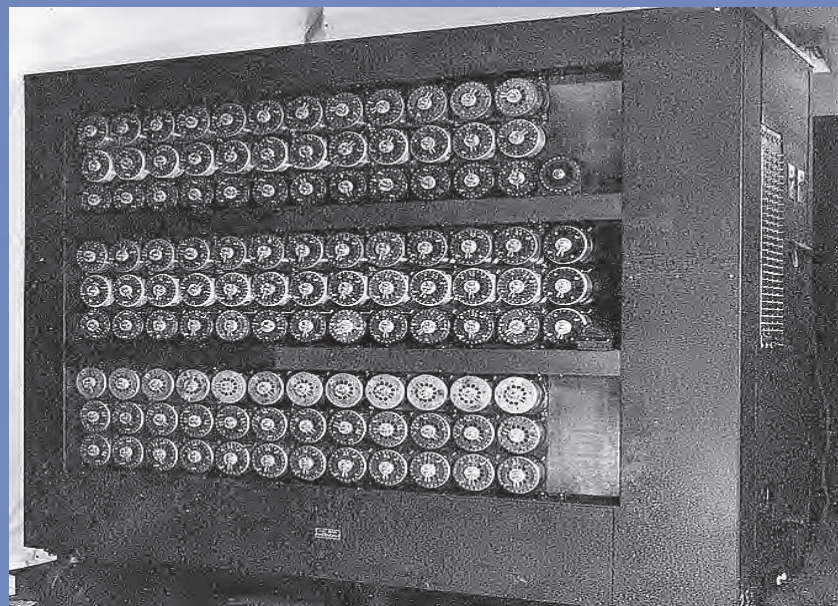
Statek Lamoricière
Fot. Kolekcja agencji Adhémair. Licencja CC BY-SA 4.0

W Algierii mieściła się filia ośrodka Cadix, którego załoga także zajmowała się przechwytywaniem tajnych depesz niemieckich. Skład osobowy zmieniał się tam co kilka miesięcy, dając polskim i francuskim kryptologom możliwość pracy w odmiennych warunkach. W 1942 r. z takiej propozycji skorzystał Jerzy Różycki, jednak zakończyła się ona dla niego tragicznie. W wyniku katastrofalnych warunków pogodowych statek Lamoricière, na którego pokładzie odbywał powrotny rejs, zatonął.



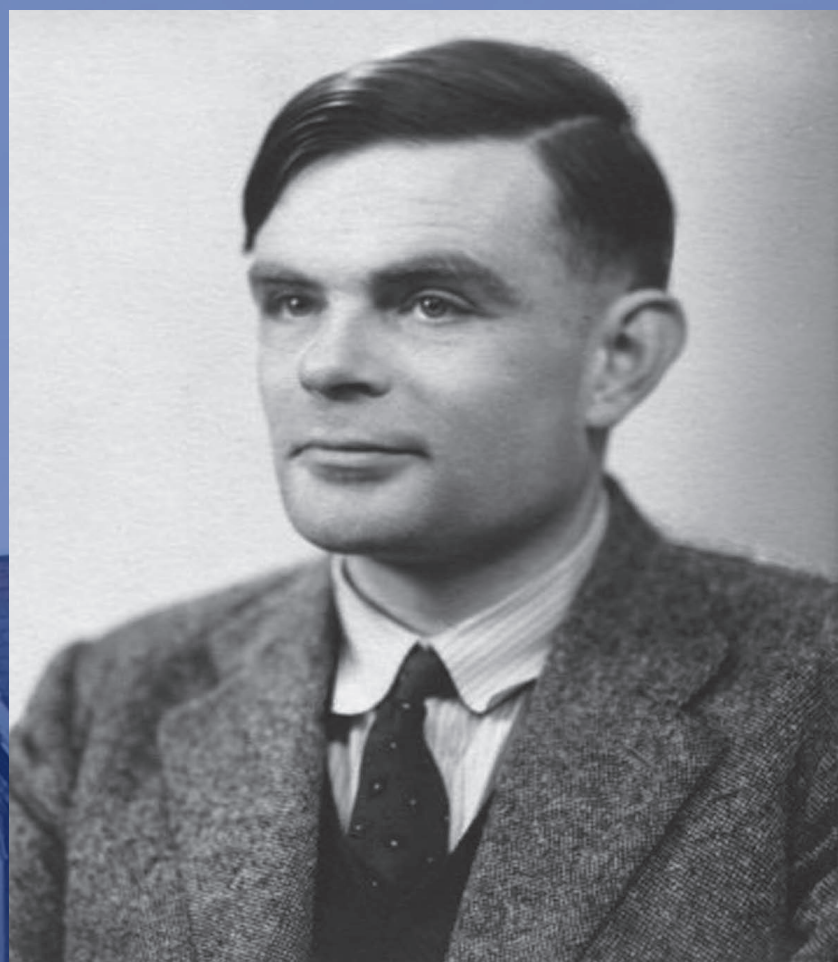
BLETCHLEY PARK

Początkowo sceptyczni wobec polskich dokonań Brytyjczycy wykorzystali wiedzę oraz doświadczenie przekazane podczas konferencji w Pyrach. W murach posiadłości położonej ok. 80 kilometrów od Londynu, Brytyjczycy stworzyli tajny ośrodek kryptologiczny Bletchley Park (Station X). Celem pracowników poszczególnych sekcji było rozpracowanie zarówno Enigmy, jak i innych szyfrów używanych m.in. przez wojska japońskie oraz włoskie. Dekryptaż w tym miejscu prowadzony był na skalę przemysłową. Bletchley Park stał się kryptologicznym centrum aliantów. Pomimo tego, że polscy kryptolodzy od sierpnia 1943 r. przebywali w Wielkiej Brytanii, do pracy w ośrodku nie zostali dopuszczeni.



Bomba Alana Turinga
Fot. Domena publiczna

Maszyna została skonstruowana przez Alana Turinga na podstawie badań i projektów sporządzonych przez Mariana Rejewskiego, choć w oparciu o odmienne założenia. Zdecydowanie przyspieszyła żmudny proces odnajdywania kluczy dziennych, wcześniej prowadzony głównie przy użyciu „płacht Zygalskiego”.

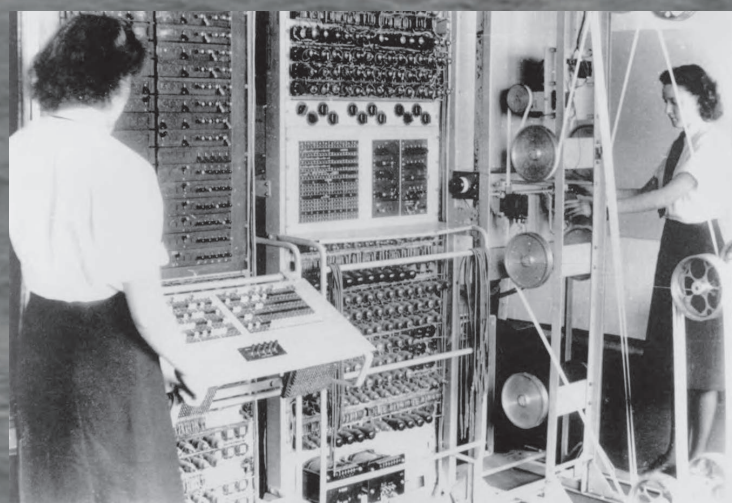


Alan Turing (1912-1954) na fotografii w 1951 r.
Fot. Elliott & Fry, domena publiczna

Jako wszechstronnie uzdolniony matematyk podjął pracę na stanowisku kryptoanalityka w Bletchley Park. Wieloletnia działalność naukowa, wypełniona innowacyjnymi projektami, przyniosła mu światową sławę. Określany mianem ojca sztucznej inteligencji, miał wielki wkład w rozwój informatyki. Niestety prywatne losy Turinga były tragiczne. Z powodu swojej orientacji seksualnej został skazany na przymusową terapię hormonalną. W 1954 r. popełnił samobójstwo. W 2013 r. został pośmiertnie ułaskawiony przez królową Elżbietę II.



OD KRYPTOLOGII DO INFORMATYKI

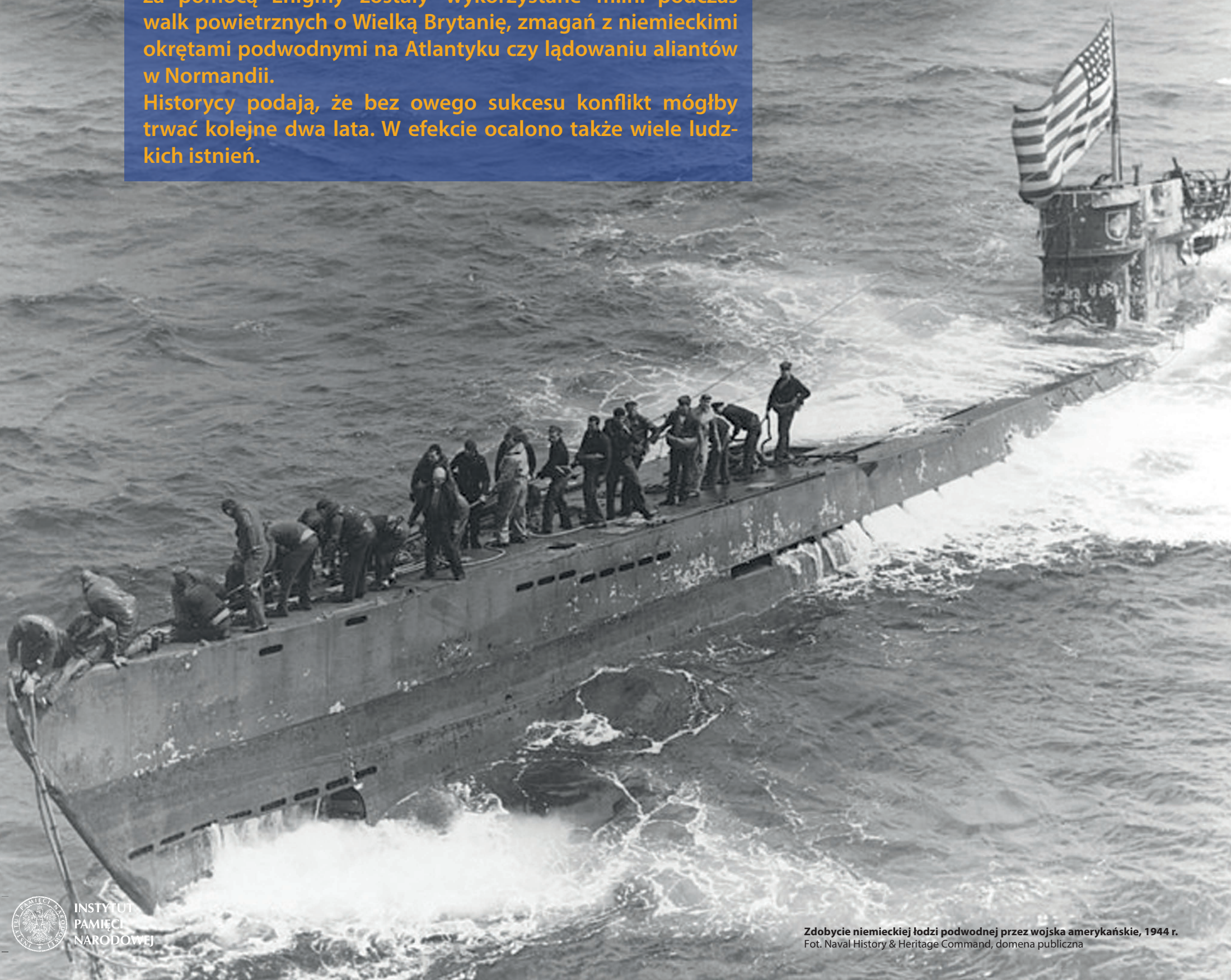


Maszyna Colossus Mark II, 1943 r.
Fot. Domena publiczna

W okresie wzmożonych działań zbrojnych nastąpił bardzo szybki rozwój technologii. Dzięki wykorzystaniu umiejętności zdobytych przez kryptologów oraz matematyków, możliwy stał się błyskawiczny postęp informatyki. Urządzenia przetwarzające dane, takie jak bomby kryptologiczne pomysłu Rejewskiego i Turinga, stały się zaczątkiem nowoczesnych komputerów.

Złamanie szyfru Enigmy oraz sprawny dekryptaż niemieckich depesz w znacznym stopniu przyczyniły się do szybszego zakończenia działań wojennych prowadzonych w latach 1939-1945. Dane pozyskane dzięki czytaniu depesz szyfrowanych za pomocą Enigmy zostały wykorzystane m.in. podczas walk powietrznych o Wielką Brytanię, zmagania z niemieckimi okrętami podwodnymi na Atlantyku czy lądowaniu aliantów w Normandii.

Historycy podają, że bez owego sukcesu konflikt mógłby trwać kolejne dwa lata. W efekcie ocalono także wiele ludzkich istnień.



Zdobycie niemieckiej łodzi podwodnej przez wojska amerykańskie, 1944 r.
Fot. Naval History & Heritage Command, domena publiczna



POWOJENNE LOSY

HENRYK ZYGALSKI

Minęło wiele dekad nim prawda o skali zasług polskich kryptologów trafiła do szerszego grona odbiorców. Brytyjczycy prowadzili narrację dotyczącą złamania szyfru Enigmy jednostronnie, marginalnie traktując wkład Polaków. Z drugiej strony sytuacja polityczna w PRL nie zachęcała byłych pracowników Biura Szyfrów do ujawnienia swojej przeszłości.

Na szczęście w ostatnich latach, dzięki działaniom podejmowanym przez instytucje, naukowców oraz zaangażowanych społeczników, pamięć o „Pogromcach Enigmy” jest coraz częściej należycie honorowana. Ich dzieje przybliżają kolejne publikacje, wystawy, pomniki oraz tablice pamiątkowe.



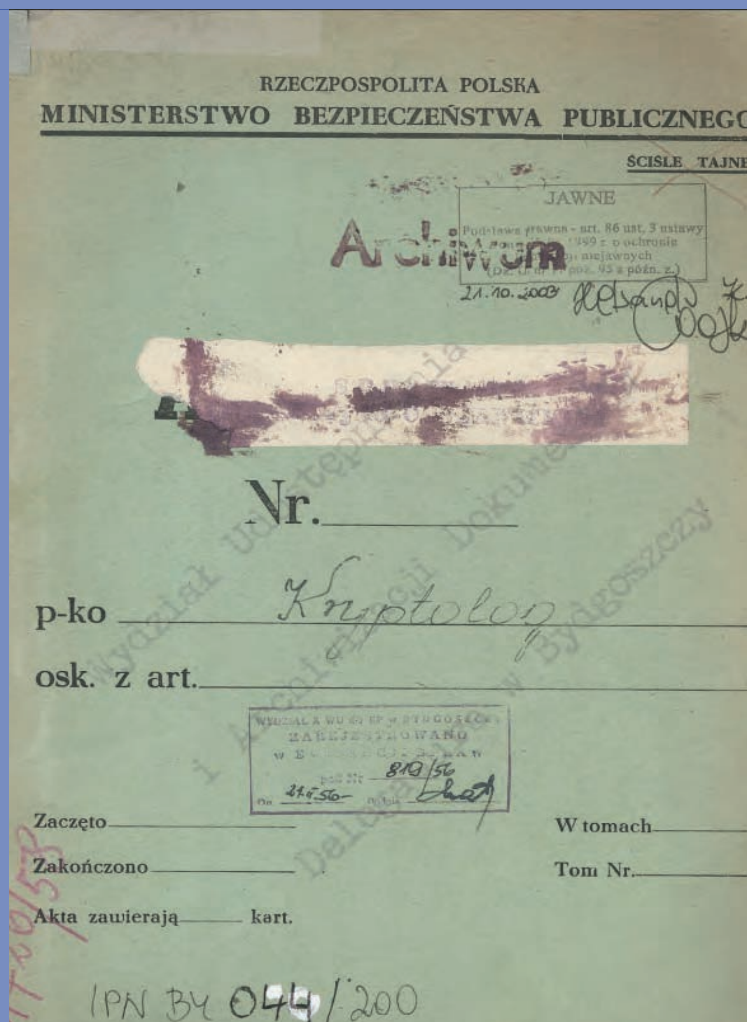
Fragment ekspozycji w Centrum Szyfrów Enigma w Poznaniu
Fot. Ł. Gdak/ Poznańskie Centrum Dziedzictwa

Centrum Szyfrów Enigma jest marką Poznańskiego Centrum Dziedzictwa, miejskiej instytucji kultury, która opowiada o Poznaniu i jego spuściźnie. Misją CSE jest budowanie świadomości, że złamanie szyfru niemieckiej maszyny szyfrującej Enigma było dziełem polskich matematyków: Mariana Rejewskiego, Henryka Zygalskiego i Jerzego Różyckiego, absolwentów Uniwersytetu Poznańskiego. CSE, podejmując także tematy historii kryptologii i świata cyfrowego, prowadzi zajęcia edukacyjne oraz kulturalno-naukowe, animujące społeczną aktywność w centrum miasta.



Henryk Zygałski z Berthą Blofield, 1955 r.
Fot. zbiory p. M. Bryschak (CS Enigma)

Henryk Zygałski po zakończeniu drugiej wojny światowej nie powrócił do ojczyzny. Pozostał na emigracji i podjął pracę jako wykładowca matematyki na Uniwersytecie Surrey. Prywatnie związał się z Berthą Blofield, z którą dzielił wspólne pasje do muzyki oraz podróży. W rodzinnych zbiorach zachowało się dużo fotografii, opatrzonych ciekawymi komentarzami kreślonymi przez Zygałskiego.



Teczka sprawy „Kryptolog” dot. rozpracowania Mariana Rejewskiego
Fot. AIPN Poznań

Marian Rejewski zdecydował się na powrót do Polski. Zamieszkał wraz z rodziną w Bydgoszczy, gdzie pracował jako urzędnik. Przez wiele lat skrywał sekret dotyczący złamania kodu Enigmy, obawiając się następstw, jakie mogło nieść ujawnienie przeszłości. Wojenna działalność poza granicami kraju skierowała na niego uwagę służb komunistycznych, które śledziły zarówno jego poczynania, jak i kontakty.



INSTYTUT
PAMIĘCI
NARODOWEJ

Pomnik kryptologów w Poznaniu, 2022 r.
Fot. J. Kilanowska

BILANS

Dienststelle: Stelle:

Spruch Nr.	Befördert am	193	Uhr durch
	Aufgenommen am	193	Uhr durch
	Erhalten am	193	Uhr

Fern-
Funk-
Blink-
Spruch Nr. von
an

Bemerkte:

Abfendende Stelle:	te Meldung	Ort	Tag Monat	Stunde Minuten
	Abgegangen			
Angekommen				
An				

Dane liczbowe

3×10^{114} wynosiła teoretyczna liczba kombinacji (stanów) wojskowej Enigmy w przypadku, gdy kryptolog atakujący szyfr nie znał budowy maszyny. Dzięki zastosowaniu zaawansowanej matematyki, Marian Rejewski zredukował tę liczbę do 105 456 kombinacji.

2 godziny zajmowało sześciu egzemplarzom „bomb Rejewskiego” przeanalizowanie wszystkich możliwych pozycji startowych maszyny.

10 000 osób zatrudniał ośrodek Bletchley Park w 1945 r.

200 000 ręcznie wycinanych otworów wymagało stworzenie kompletu „płacht Zygalskiego”.

8840 zaszyfrowanych niemieckich radiogramów odczytali podczas dziewięciu miesięcy (od października 1939 r. do czerwca 1940 r.) polscy kryptolodzy w ośrodku „Bruno”.

Od końca 1942 r. do maja 1945 r., głównie dzięki czytaniu depesz szyfrowanych za pomocą Enigmy, alianci zatopili na Atlantyku **692** niemieckie łodzie podwodne.

740528

PODSUMOWANIE

To tylko im należy się cała zasługa i chwała za doprowadzenie pod względem specjalistycznym do końca tej niewiarygodnej historii. Nastąpiło to dzięki ich wiedzy i uporczywości, niemających sobie równych w świecie! Pokonali trudności, które Niemcy uważali za „niemożliwe do przewyciężenia”.

(G. Bertrand, *Enigma ou la plus grande énigme de la guerre 1939-1945*, Paryż 1973 r.)

IEEE MILESTONE IN ELECTRICAL ENGINEERING AND COMPUTING

First Breaking of Enigma Code
by the Team of the Polish Cipher Bureau, 1932-1939

Polish Cipher Bureau mathematicians Marian Rejewski, Jerzy Różycki and Henryk Zygalski broke the German Enigma cipher machine codes. Working with engineers from the AVA Radio Manufacturing Company, they built the 'bomba' – the first cryptanalytic machine to break Enigma codes. Their work was a foundation of British code breaking efforts which, with later American assistance, helped to end World War II.

August 2014



Odznaczenie IEEE - "Kamień milowy" w rozwoju
inżynierii elektrycznej i obliczeniowej

Złamanie po raz pierwszy kodów Enigmy przez zespół
matematyków z polskiego Biura Szyfrów w latach 1932-1939

Polscy matematycy Marian Rejewski, Jerzy Różycki i Henryk Zygalski z krajowego Biura Szyfrów złamali kody maszyny szyfrującej Enigma. Pracując razem z inżynierami fabryki AVA w Warszawie zbudowali „bombę” – pierwszą maszynę deszyfrującą kody Enigmy. Ich osiągnięcia były podstawą do dalszych prac Brytyjczyków nad deszyfracją, które w okresie późniejszym z pomocą Amerykanów, przyczyniły się do zakończenia II-giej Wojny Światowej.

Sierpień 2014r



INSTYTUT
PAMIĘCI
NARODOWEJ

„Kamień milowy” honorujący dokonania poznańskich matematyków zajmujących się złamaniem szyfru Enigmy, znajdujący się przed Instytutem Matematycznym PAN im. Stefana Banacha w Warszawie
Fot. W. Sobócki