

ZŁAMANIE SZYFRU ENIGMY



INSTYTUT
PAMIĘCI
NARODOWEJ

**Materiały edukacyjne
do wystawy elementarnej**

ZŁAMANIE SZYFRU ENIGMY

Materiały edukacyjne
do wystawy elementarnej
Instytutu Pamięci Narodowej

Autorzy wystawy: Julia Moszczyńska, dr Izabella Kopczyńska, Witold Sobócki

Koncepcja graficzna serii: Aleksandra Kaiper-Miszułowicz

Koncepcja graficzna i skład wystawy: dr Karolina Zielazek-Szeska

Strefa edukacji: Witold Sobócki

Moduł edukacyjny: Julia Moszczyńska, Witold Sobócki

Korekta: Ilona Kaczmarek, Hanna Kwaśny

Recenzja: dr Katarzyna Maniewska, Magdalena Zapolska-Downar

Projekt graficzny i skład w oparciu o layout wystaw elementarnych:

Marcin Kucewicz

Fotografie i dokumenty ze zbiorów: Archive.org, Archiwum Uniwersytetu im. Adama Mickiewicza w Poznaniu, Marii Bryschak, Bundesarchiv, Centrum Szyfrów Enigma w Poznaniu, Cryptomuseum.com, Narodowego Archiwum Cyfrowego, Piotra Paluta, Polony, Instytutu Piłsudskiego w Londynie, Janiny Sylwestrzak.

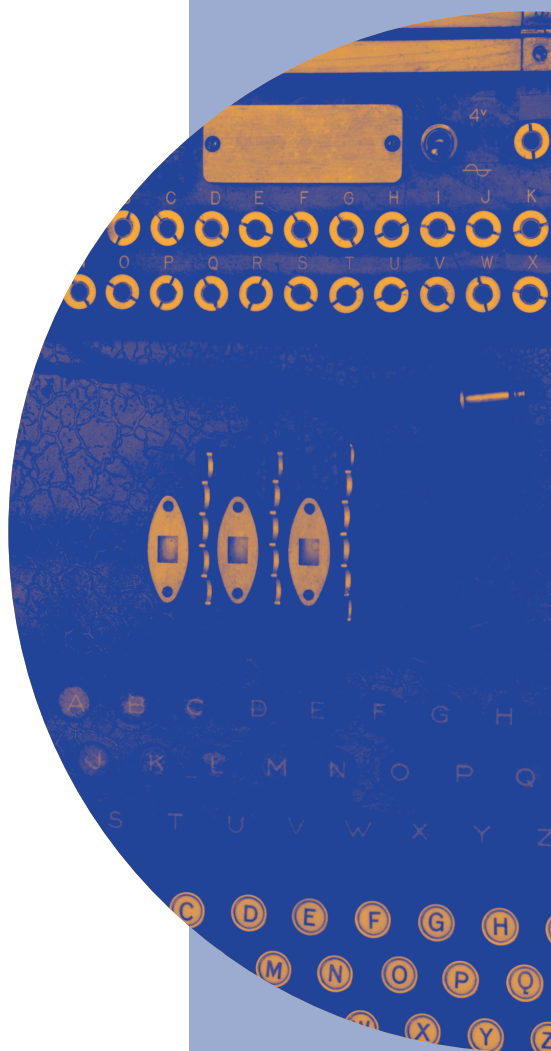
Autorzy składają serdeczne podziękowania Centrum Szyfrów Enigma w Poznaniu za okazaną pomoc podczas tworzenia wystawy.

ISBN: 978-83-8376-683-6 (druk) i 978-83-8376-684-3 (pdf)

© Instytut Pamięci Narodowej – Komisja Ścigania Zbrodni
przeciwko Narodowi Polskiemu Oddział w Poznaniu

Poznań 2026

Słowo wstępne	5
Radiowywiad w Niepodległej	6
Problem Enigmy	9
Pierwsze próby	12
Kurs w Poznaniu	14
Najlepsze trio	16
Poznanie tajemnic	18
Widmo wojny	20
Ocalić sekret	22
„Bruno” – „Cadix” – Algier	24
Bletchley Park	26
Od kryptologii do informatyki	28
Powojenne losy	30
Dekryptaż Enigmy w liczbach	32
Podsumowanie	33
Kalendarium	34
Moduł edukacyjny	39
Teksty źródłowe	47
Wybrana bibliografia	50
Słowniczek	51



SPIS TREŚCI



Kryptolodzy: Henryk Zygański, Jerzy Różycki i Marian Rejewski
podczas pobytu w ośrodku „Cadix”, 1940–1941 r.

Fot. domena publiczna

Szanowni Państwo,

poznański Oddział Instytutu Pamięci Narodowej po raz kolejny oddaje w Państwa ręce broszurę z materiałami edukacyjnymi do wystawy elementarnej. Tym razem dotyczą one ekspozycji zatytułowanej „Złamanie szyfru Enigmy”, przygotowanej przez Oddziałowe Biuro Edukacji Narodowej w Poznaniu w 2023 r.

Niniejsza publikacja, stanowiąca uzupełnienie wspomnianej wystawy, skierowana jest do nauczycieli oraz uczniów. Materiały składają się z dwóch zasadniczych części. W pierwszej z nich zamieszczono plansze wystawy poszerzone o „Strefę edukacji”. Znajdują się w niej wskazówki uwypuklające najważniejsze wątki podejmowane na każdej z plansz („Zwróć uwagę na...”), a także obszerniejszy tekst merytoryczny, który pozwala na zdobycie bardziej szczegółowej wiedzy z zakresu omawianego na planszy zagadnienia („Czy wiesz, że...”). Druga część, zatytułowana „Moduł edukacyjny”, zawiera ćwiczenia o różnym stopniu trudności oraz trzy teksty źródłowe z przypisanymi do nich pytaniami. Całość dopełniają kalendarium, słowniczek oraz wybrana bibliografia dotycząca tematyki złamania szyfru Enigmy.

Zachęcamy do korzystania z materiałów edukacyjnych zarówno w wersji drukowanej, jak i w wersji elektronicznej, zamieszczonej pod linkiem: <https://edukacja.ipn.gov.pl/edu/materiały-edukacyjne/zadania-i-cwiczenia-dla>

Mam nadzieję, że publikacja ta przyczyni się do upowszechnienia wiedzy o największym polskim osiągnięciu kryptologicznym – złamaniu szyfru Enigmy – które doprowadziło do skrócenia II wojny światowej, a także do rozwoju współczesnego cyfrowego świata.

Marta Szczesiak-Ślusarek
Naczelnik Biura Edukacji Narodowej
IPN Oddział w Poznaniu

RADIOWYWIAD W NIEPODLEGŁEJ

1

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.

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

Sukces kryptologiczny porucznika Jana Kowalewskiego, którym 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 radiowywiadem: Biura Szyfrów. Kontynuowało ono pracę również w czasie pokoju.



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

Fot. NAC

Zwróć uwagę na...

- ▶ rozwój wojskowej sieci radiotelegraficznej i nasłuchowej wraz z tworzeniem odrodzonego Wojska Polskiego;
- ▶ znaczenie złamania przez Polaków bolszewickich szyfrów podczas wojny z lat 1919–1920.

Por. Jan Kowalewski (1892–1965) w mundurze,
fotografia portretowa

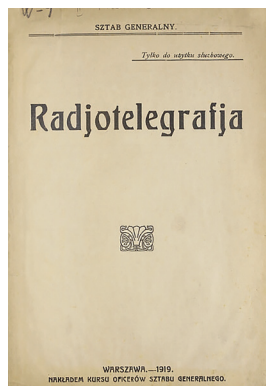
Fot. NAC



Czy wiesz, że...

- ▶ Podstawową formą łączności bezprzewodowej w ówczesnych czasach była radiotelegrafia, czyli nadawanie depesz drogą radiową za pomocą alfabetu Morse'a. Taki sposób przekazywania informacji nie wymagał stworzenia infrastruktury kablowej, ale z drugiej strony sprawiał, że komunikaty nadawane tą drogą były łatwe do przechwycenia (podśluchania).
- ▶ Gen. bryg. Jan Kowalewski (1892–1965) – oficer Wojska Polskiego, kryptolog, chemik. Podczas I wojny światowej był żołnierzem armii rosyjskiej. W sierpniu 1919 r. Kowalewskiemu, służącemu w II Oddziale Sztabu Wojska Polskiego (wywiadowczym), udało się złamać pierwszy bolszewicki szyfr. Jego sukces przyczynił się do powstania w II Oddziale Sztabu WP Referatu Radiowywiadu, w kolejnych latach przekształconego w Biuro Szyfrów.
- ▶ Podczas wojny polsko-bolszewickiej polscy kryptolodzy złamali ok. stu obcych szyfrów – nie tylko nadawanych przez Sowieców, lecz także przez „białych” Rosjan oraz Ukraińską Republikę Ludową.

▶ Okładka podręcznika
Radjotelegrafia, wydanego
w 1919 r.
Fot. POLONA



PROBLEM ENIGMY

2



▲ Model wojskowej Enigmy z widocznymi trzema wirnikami oraz łącznicą

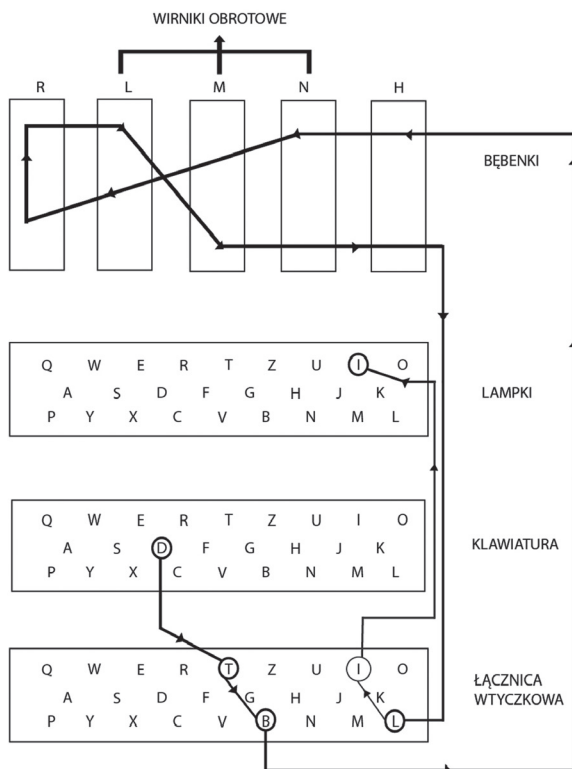
Fot. United States Government Work, domena publiczna

Opatentowana w 1918 r. niemiecka maszyna szyfrująca Enigma pierwotnie przeznaczona była na rynek cywilny z myślą o utajnianiu 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.

Zwróć uwagę na:

- ▶ początkowy brak zainteresowania niemieckiego wojska maszyną szyfrującą;
- ▶ nieskuteczność dotychczasowych metod kryptoanalitycznych w przypadku prób rozpracowania Enigmy typu wojskowego;
- ▶ różnice w budowie Enigmy w wersjach handlowych i wojskowych.



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

Maszynowy szyfr generowany przez Enigmę uniemożliwiał stosowanie w kryptoanalizie metod lingwistycznych. Do odczytania depesz potrzebny był identyczny model maszyny z dokładnie takimi samymi, okresowo zmienianymi, ustawieniami początkowymi. Samo urządzenie także ewoluowało – udoskonalano procedury jego używania oraz zmieniano konstrukcję. Wszystkie te zabiegi powodowały, że szyfr Enigmy uważany był za nie do złamania.

Czy wiesz, że...

- ▶ Elementami odpowiedzialnymi za procesy szyfrowania w wojskowej Enigmie były łącznica, walec wejściowy, obrotowe wirniki oraz reflektor. Przez każdy z tych elementów (oprócz reflektora) sygnał, który reprezentował daną literę szyfrogramu, przechodził dwukrotnie.
- ▶ Na ustawienia początkowe maszyny składały się: kolejność umieszczenia poszczególnych wirników w urządzeniu, ustawienia ich pierścieni oraz ich „pozycje startowe”, a także liczba i kombinacja połączeń w łącznicy. Dodatkowo każda depesza była zabezpieczana oddzielnym, trójszybnym kluczem nadawanym przez szyfranta.
- ▶ Budowa i sposób użycia maszyny generowały ogromną liczbę możliwych kombinacji szyfrujących, wobec których ówczesne techniki kryptograficzne były nieskuteczne.
- ▶ Różnice pomiędzy wersjami wojskowymi oraz handlowymi sprowadzały się do innego układu okablowania elementów odpowiedzialnych za szyfrowanie oraz dodania w wersji wojskowej łącznicy, która wprowadzała dodatkowe przekształcenia liter. Tak więc odczytanie za pomocą wariantu cywilnego depeszy nadanej przy użyciu wariantu wojskowego było niemożliwe.



3 PIERWSZE PRÓBY

Rozpracowaniem Enigmy, oprócz Polaków, bezskutecznie zajmowały się również francuskie oraz brytyjskie służby wywiadowcze.

Polscy kryptolodzy uciekali się do niestandardowych metod: szyfrogramy przekazano do analizy m.in. słynnemu jasnowidzowi – inż. Stefanowi Ossowieckiemu. Jak się okazało, ich nieszablonowe podejście do problemu zaowocowało w przyszłości.



Niemieccy żołnierze obsługujący Enigmę

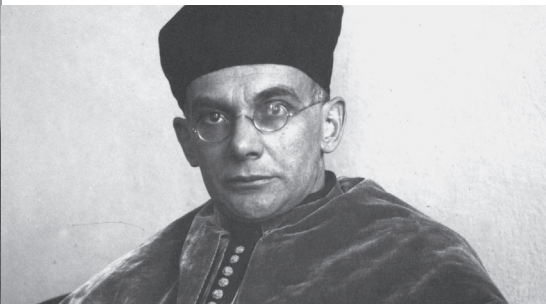
Fot. ze zbiorów Bundesarchiv, fotografia 183-L22303/Mess, 1940 r.

Zwróć uwagę na:

- ▶ zainteresowanie wywiadów Wielkiej Brytanii i Francji złamaniem szyfru Enigmy;
- ▶ konieczność dokładnego odtworzenia działania Enigmy oraz procedur jej używania w celu rozpracowania szyfru generowanego przez maszynę.

Czy wiesz, że...

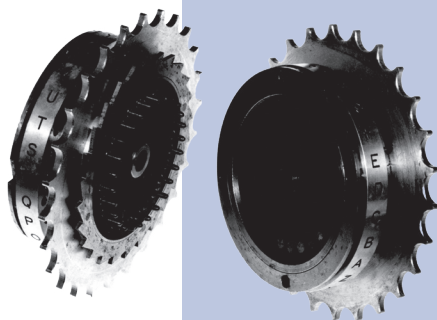
- ▶ W latach trzydziestych XX w. Brytyjczykom udało się złamać szyfr Enigmy używanej we włoskiej marynarce wojennej posługującej się jej handlowym modelem.



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 też postanowiło zwrócić się do nich o pomoc. Niestety, matematycy nie potrafili sobie poradzić nawet z niemieckimi depeszami utajnionymi bez użycia Enigmy



Wirniki Enigmy

Fot. ze zbiorów Instytutu Piłsudskiego w Londynie

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

KURS W POZNANIU

4

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



Zamek Cesarski w Poznaniu

Fot. POŁONA

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 68

By
JOHN B. HURT, *Cryptanalyst Aide*
SIGNAL INTELLIGENCE SECTION
WAR PLANS AND TRAINING DIVISION

Roy R. Plumley
ROY R. PLUMLEY, *Major*


UNITED STATES
GOVERNMENT PRINTING OFFICE
WASHINGTON: 1934



Marcel Givierge, *Cours de Cryptographie*. Na zdjęciu amerykańskie wydanie podręcznika. Zakres i materiał kursu opierał się na wydaniu podręcznika z 1925 r.

Fot. Archive.org

Zwróć uwagę na...

- ▶ nowatorski pomysł przeszkolenia, a następnie zatrudnienia wybitnych młodych matematyków;
- ▶ wybór Poznania jako miejsca odbywania kursu, uwarunkowanego znajomością języka niemieckiego i niemieckiej mentalności przez polskich mieszkańców terenów byłego zaboru pruskiego.

Czy wiesz, że...

- ▶ Szyfr podwójnego przedstawienia należał do szyfrów ręcznych, używanych przez Niemców jeszcze podczas I wojny światowej. W armii niemieckiej był stosowany pomimo wprowadzenia do użytku maszyny Enigma. Mimo tego, że istniały sposoby łamania tego szyfru, zapewniał on wysoki poziom zabezpieczenia informacji.
- ▶ W historii złamania szyfru Enigmy niebagatelną rolę odegrał prof. Zdzisław Krygowski. Pełniąc w 1929 r. funkcję kierownika Katedry Matematyki Uniwersytetu Poznańskiego, zgodził się na przeprowadzenie kursu kryptologicznego. Do udziału w nim wytypował najzdolniejszych studentów. Jego zainteresowania naukowe dotyczyły m.in. teorii permutacji. Właśnie tę dziedzinę matematyki skutecznie wykorzystał w złamaniu szyfru Enigmy jego uczeń – Marian Rejewski.



Maksymilian Ciężki (1898–1951)

Fot. domena publiczna

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



Zdzisław Krygowski (1872–1955)

Fot. ze zbiorów Archiwum UAM

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



5

NAJLEPSZE TRIO

W czasie kursu wyłoniono trzech najzdolniejszych studentów: Mariana Rejewskiego, Henryka Zygalskiego i Jerzego Różyckiego. Utworzony zespół został zatrudniony w Ekspozyturze Biura Szyfrów w Poznaniu, mieszczącej się przy dzisiejszej ul. 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.



Marian Rejewski (1905–1980)

Fot. ze zbiorów Janiny Sylwestrzak/Centrum Szyfrów Enigma



Henryk Zygański (1908–1978)

Fot. domena publiczna



Jerzy Różycki (1909–1942)

Fot. domena publiczna



Zwróć uwagę na...

- fakt, że ulokowanie Ekspozytury Biura Szyfrów zapewniało zachowanie przez matematyków konspiracji w pracach dla polskiego wywiadu.

Czy wiesz, że...

- Marian Rejewski (1905–1980) – urodzony w Bydgoszczy, absolwent Uniwersytetu Poznańskiego. W grudniu 1932 r. jako pierwszy na świecie złamał szyfr maszyny Enigma, posługując się zaawansowaną matematyką. Razem z pozostałymi kryptologami doskonał metody dekryptażu depesz szyfrowanych przy pomocy Enigmy. Jest twórcą maszyny kryptologicznej o nazwie „bomba Rejewskiego”. We wrześniu 1939 r. ewakuował się do Rumunii, a następnie trafił do Francji, gdzie kontynuował działalność kryptologiczną. Od 1943 r. przebywał w Wielkiej Brytanii i służył w Polskich Siłach Zbrojnych na Zachodzie. Po zakończeniu wojny zdecydował się na powrót do kraju. W Polsce Ludowej był inwigilowany przez Urząd Bezpieczeństwa, a po jego przekształceniu w Służbę Bezpieczeństwa – również przez nią. Marian Rejewski pracował na podrzędnych stanowiskach. Swoje dokonania kryptologiczne ujawnił dopiero w latach siedemdziesiątych XX w.
- Henryk Zygalski (1908–1978) – urodzony w Poznaniu, absolwent Uniwersytetu Poznańskiego. Jego największym wkładem w prace nad dekryptażem Enigmy było stworzenie zestawów perforowanych płacht, zwanych „płachtami Zygalskiego”, które pozwalały wyznaczyć początkowe ustawienia Enigmy. Podobnie jak Marian Rejewski, po wybuchu II wojny światowej trafił do Rumunii, a następnie do Francji oraz do Wielkiej Brytanii. Po wojnie zdecydował się na pozostanie na obczyźnie; w Wielkiej Brytanii kontynuował karierę matematyczną.
- Jerzy Różycki (1909–1942) – urodzony w Olszanie w guberni kijowskiej, absolwent Uniwersytetu Poznańskiego. Do złamania szyfru Enigmy przyczynił się, tworząc metodę zegara, która wykorzystywała statystykę i lingwistykę. Podczas II wojny światowej dzielił los Mariana Rejewskiego i Henryka Zygalskiego. Zginął w 1942 r. w katastrofie morskiej na Morzu Śródziemnym.
- Marian Rejewski, Henryk Zygalski oraz Jerzy Różycki w latach 1929–1932 zajmowali się łamaniem szyfru podwójnego przestawienia, którego działanie szczególnie wnikliwie omówiono podczas kursu kryptologicznego. Szyfr ten, obok szyfru tworzonego za pomocą Enigmy, był używany przez niemieckie wojsko głównie w niższych strukturach organizacyjnych.

POZNANIE TAJEMNIC

6

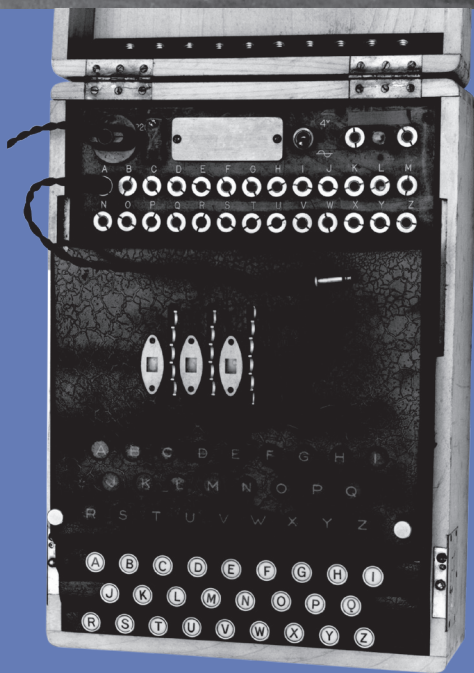
Użycie handlowej wersji urządzenia do dekryptażu nie dało rezultatu. Marian Rejewski za pomocą teorii permutacji odczytał szyfrogram w grudniu 1932 r., co uznaje się za pierwszy sukces w procesie łamania szyfru maszyny Enigma. W 1933 r. matematycy rozpoczęli wspólną pracę, by usprawnić odczytywanie niemieckich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



Pałac Saski w Warszawie

Fot. NAC

Siedziba Biura Szyfrów. Tutaj przeniesiono poznańską filię Biura i kontynuowano prace kryptologiczne



Kopia Enigmy

Fot. ze zbiorów Instytutu Piłsudskiego w Londynie

Zwróć uwagę na...

- ▶ fakt, że odczytanie pierwszych depesz przez Mariana Rejewskiego stanowiło początek procesu sprawnego dekryptażu;
- ▶ wsparcie techniczne udzielone pracownikom Biura Szyfrów przez Wytwórnię Radiotechniczną AVA, która produkowała kopie Enigmy oraz urządzenia wspomagające prace kryptologiczne.

Czy wiesz, że...

- ▶ W analizie matematycznej maszyny Rejewski posłużył się teorią permutacji. Analizując dziesiątki depesz, skupił się na pierwszych sześciu znakach każdej z nich, gdzie był podwójnie zaszyfrowany indywidualny klucz dla każdej wiadomości. Gdy zebrał odpowiednią liczbę depesz z danego dnia, udało mu się uchwycić cykliczność przekształceń. Cykle te wstawił w układ wielu równań.
- ▶ Skomplikowanym obliczeniom pomogła matematykowi także intuicja – założył alfabetyczny układ okablowania w walcu wejściowym (elemente szyfrującym pomiędzy łącznicą a pierwszym wirnikiem obrotowym). Pomocne w pracach okazały się materiały otrzymane od francuskiego wywiadu.
- ▶ Kopie maszyny Enigma wytworzone przez wytwórnię AVA powstały wyłącznie dzięki obliczeniom Rejewskiego – z dzisiejszego punktu widzenia proces ten można nazwać inżynierią wsteczną. Polskie maszyny odróżniały się od oryginałów innym umiejscowieniem łącznicy (z tyłu urządzenia) oraz alfabetycznym układem klawiatury.



Antoni Palluth (1900–1944)

Fot. ze zbiorów 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





WIDMO WOJNY

◀ **Gustave Bertrand (1896–1976)**

Fot. domena publiczna

Szef sekcji D szyfrów francuskiego radiowywiadu. Przedstawiciel strony francuskiej w czasie konferencji w Pyrach. Na początku pracy Polaków nad złamaniem szyfru Enigmy przekazał im informacje na temat instrukcji użytkowania maszyny

We wrześniu 1938 r. 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. na konferencji w ośrodku kryptologicznym w podwarszawskiej miejscowości Pyry postanowiło podzielić się ze stroną francuską i brytyjską swoją wiedzą i technikami łamania szyfrów. Do tego spotkania kryptolodzy brytyjscy i francuscy używali metod, które były niewystarczające do odczytania niemieckich szyfrów Enigmy.



▲ **Rekonstrukcja wyglądu bomby kryptologicznej na podstawie szkiców ze wspomnień Mariana Rejewskiego**

Rysunek: Szymon Pilecki, Szymon Dąbrowski.
Licencja CC BY-SA 4.0

Zwróć uwagę na...

- ▶ fakt, że podczas konferencji w Pyrach strona polska podzieliła się wszystkimi osiągnięciami w łamaniu szyfru Enigmy ze stronami francuską i brytyjską.

Czy wiesz, że...

- ▶ Podczas konferencji w Pyrach w lipcu 1939 r. strona polska przekazała Francuzom i Brytyjczykom wiedzę na temat metod potrzebnych do złamania szyfru Enigmy oraz kopie samej maszyny wraz z dokumentacją techniczną.
- ▶ Rozpracowanie przez Mariana Rejewskiego Enigmy wyłącznie dzięki dedukcji matematycznej, bez dostępu do egzemplarza maszyny, zrobiło szczególne wrażenie na stronie brytyjskiej. Kryptolog z tego państwa, Alfred Dillwyn „Dilly” Knox, zarzucał nawet Polakom nieszczerść – początkowo uważał, że rozpracowanie maszyny jest niemożliwe bez zdobycia urządzenia.
- ▶ Dokumentacja przekazana Polakom w 1932 r. przez Gustave'a Bertranda pochodziła od francuskiego szpiega Hansa-Thilo Schmidta z niemieckiego Biura Szyfrów (Chi-Stelle). Według Mariana Rejewskiego informacje tam zawarte znacznie ułatwiły prace. Bez dostępu do nich złamanie szyfru Enigmy byłoby możliwe, ale trwałoby dłużej. Gdy w latach siedemdziesiątych XX w. ukazały się wspomnienia gen. Bertranda, okazało się, że Rejewski nie otrzymał kompletu materiałów – decyzję o ich przekazaniu podejmował jego przełożony Maksymilian Ciężki, który ograniczając do nich dostęp, stymulował pomysłowość matematyka. Do całości dokumentacji mieli dostęp francuscy i brytyjscy kryptolodzy, jednak – w przeciwieństwie do Polaków – nie potrafili jej wykorzystać praktycznie.
- ▶ Bomba Rejewskiego oraz płachty Zygalskiego były najbardziej zaawansowanymi polskimi narzędziami dekryptażowymi. Dzięki tym wynalazkom udało się pokonać niemieckie udoskonalenia wprowadzane w Enigmie. Sukces ten jednak nie trwał długo – kolejne usprawnienia maszyny spowodowały, że Polakom coraz trudniej było czytać niemieckie depesze. Głównym problemem uniemożliwiającym sprawny dekryptaż były brak środków i personelu.

OCALIĆ SEKRET

8



6 września specjalny pociąg o kryptonimie „Eszelon F” ruszył śladem Naczelnego Dowództwa. To właśnie w tym transporcie znaleźli się oficerowie i pracownicy Biura Szyfrów. Po dotarciu do Brześcia nad Bugiem kontynuowali oni ewakuację w kierunku granicy polsko-rumuńskiej. Po wielu perypetiach, a także pozbyciu się części urządzeń deszyfrujących i dokumentów pracownicy wywiadu 18 września 1939 r. przekroczyli granicę w Kutach.

Ze względu na dynamikę działań wojennych oraz problemy z łącznością polskich wojsk dane zdobyte dzięki złamaniu szyfru Enigmy nie zostały wykorzystane podczas kampanii polskiej w 1939 r.

We wrześniu tr. Biuro Szyfrów skupiło się przede wszystkim na zatarciu śladów swojej działalności przed wojskami niemieckimi i bezpiecznej ewakuacji personelu. Gdyby Niemcy dowiedzieli się, że Polakom udało się złamać szyfr Enigmy, zapewne wprowadziliby kolejne udoskonalenia konstrukcji maszyny i procedur jej użycia, co prawdopodobnie sprawiłoby, że dotychczasowe metody dekryptaży byłyby nieprzydatne. Wiedza przekazana Francuzom i Brytyjczykom stałaby się więc bezużyteczna.



Bombardowanie linii kolejowej przez niemieckie samoloty, wrzesień 1939 r.

Fot. NAC

Zwróć uwagę na...

- sprawną ewakuację personelu, sprzętu i dokumentacji Biura Szyfrów.

Czy wiesz, że...

- Zespół polskich kryptologów, którzy byli cywilnymi pracownikami polskiego wywiadu, nie został internowany przez władze rumuńskie. Zwrócili się oni po pomoc do ambasady brytyjskiej, a następnie – francuskiej. Personel tej drugiej placówki był uprzedzony o możliwości pojawienia się polskich kryptologów, wobec czego błyskawicznie zorganizował wyjazd do Francji.

► Mapa sporządzona przez ppłk. Gwidona Langerę przedstawiająca trasę ewakuacji Biura Szyfrów we wrześniu 1939 r., 1940 r.

Fot. ze zbiorów Instytutu Piłsudskiego w Londynie



„BRUNO” – „CADIX” – ALGIER

9

Pierwsze miesiące konfliktu zbrojnego cechował chaos, co nie sprzyjało wznowieniu prac nad odczytywaniem niemieckich depech. 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 dekrypcją.



Kryptolodzy podczas pobytu
w ośrodku „Cadix”, 1940–1941 r.
Fot. domena publiczna

Zespół pracujący w ośrodku „Cadix”; na
zdjęciu m.in. Ciężki, Langer, Zygalski,
Różycki, 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 tego miejsca. Na zmianę siedziby wpłynęło także zbyt duże zainteresowanie lokalnej ludności



Zwróć uwagę na...

- ▶ kontynuowanie prac kryptologicznych przez polskich matematyków na terenie Francji w latach 1939–1942;
- ▶ śmierć Jerzego Różyckiego w katastrofie morskiej.

Czy wiesz, że...

- ▶ 17 stycznia 1940 r. z Wielkiej Brytanii do ośrodka „Bruno” przybył Alan Turing. Podczas wizyty polscy kryptolodzy zaprezentowali mu działanie płacht Zygalskiego, odczytując jedną z niemieckich depesz.
- ▶ Ośrodek „Cadix” był jednocześnie polską placówką wywiadowczą o kryptonimie „Ekspozytura 300”. Oprócz prac kryptologicznych zajmował się łącznością pomiędzy Wydziałem Wywiadowczym Oddziału II Sztabu Naczelnego Wodza w Londynie a „Ekspozyturą AFR” zlokalizowaną w Algierze. Placówka ta przekazała aliantom istotne informacje, które umożliwiły desant ich wojsk w listopadzie 1942 r. w Afryce Północnej.

Statek Lamoricière

Fot. Kolekcja agencji Adhémar. Licencja CC BY-SA 4.0

W Algierii mieściła się filia ośrodka „Cadix”, którego pracownicy także zajmowali się przechwytywaniem tajnych depesz niemieckich. Skład osobowy zmieniał się tam co kilka miesięcy, co dawało polskim i francuskim kryptologom możliwość pracy w odmiennych warunkach. W 1942 r. z takiej propozycji skorzystał Jerzy Różycki, jednak ta decyzja miała dla niego tragiczne skutki. W wyniku fatalnych warunków pogodowych statek Lamoricière, na którego pokładzie odbywał powrotny rejs, zatonął



S. S. LAMORICIÈRE
Paquebot de la Cie Transatlantique



BLETCHLEY PARK

10

Ośrodek Bletchley Park, 2005

Fot. Matt Crypto, domena publiczna

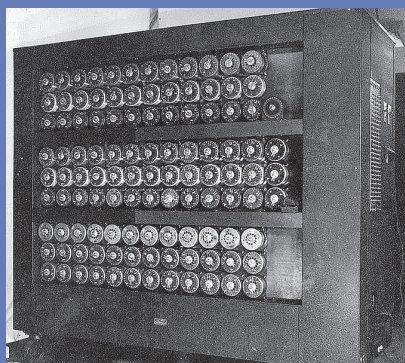
Początkowo sceptyczni wobec polskich dokonań Brytyjczycy wykorzystali wiedzę oraz doświadczenie przekazane podczas konferencji w Pyrach. W murach posiadłości położonej ok. 80 km od Londynu Brytyjczycy stworzyli tajny ośrodek kryptologiczny Bletchley Park („Station X”). Celem pracowników poszczególnych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



Bomba kryptologiczna 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



Zwróć uwagę na...

- ▶ twórcze zaadaptowanie i rozwój polskich metod łamania szyfru Enigmy przez Brytyjczyków w Bletchley Park;
- ▶ niedopuszczenie do prac w tym ośrodku zespołu polskich kryptologów.

Czy wiesz, że...

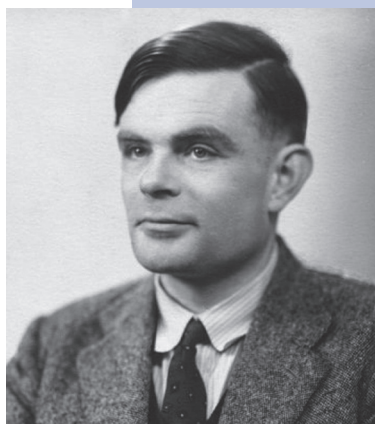
- ▶ W czasie II wojny światowej ustawienia początkowe maszyny były zmieniane nawet kilkukrotnie podczas doby. Każdy z rodzajów niemieckich sił zbrojnych miał własne sieci szyfrowe, w których posługiwano się innymi ustawieniami – bieżący dekryptaż, prowadzony w celu znajdowania nowych, skuteczniejszych sposobów łamania szyfru Enigmy, wymagał ogromnych nakładów kadrowych, finansowych oraz intelektualnych. Warunki te doskonale spełniali pracownicy ośrodka Bletchley Park, którzy rozwijali polskie pomysły i dokonania w tym zakresie.
- ▶ W maju 1940 r. Niemcy zrezygnowali z podwójnego szyfrowania klucza depeszy, a tym samym uszczelnili lukę w zabezpieczeniach Enigmy, którą z powodzeniem wykorzystali Polacy. Tymczasem Brytyjczycy dysponowali już bombą kryptologiczną Alana Turinga. Urządzenie to pozwoliło na znalezienie dziennych ustawień maszyny na podstawie analizy potencjalnych słów mogących pojawić się w szyfrogramie.



Alan Turing (1912–1954), 1951

Fot. Elliott & Fry, domena publiczna

Wszechstronnie uzdolniony matematyk, kryptoanalityk w Bletchley Park. Wieloletnia działalność naukowa, wypełniona innowacyjnymi projektami, przyniosła mu światową sławę. Jest określany mianem ojca sztucznej inteligencji, a jego wkład w rozwój informatyki jest nie do przecenienia. 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

11

Złamanie szyfru Enigmy oraz sprawny dekryptaż niemieckich depesz w znacznym stopniu przyczyniły się do szybszego zakończenia działań wojennych. Dane pozyskane dzięki czytaniu depesz szyfrowanych za pomocą Enigmy zostały wykorzystane m.in. podczas walk powietrznych o Wielką Brytanię, zmagających z niemieckimi okrętami podwodnymi na Atlantyku czy lądowania aliantów w Normandii. Historycy podają, że bez owego sukcesu konflikt mógłby trwać kolejne dwa lata. W efekcie ocalono wiele ludzkich istnień.



Zdobycie niemieckiego okrętu podwodnego przez wojska amerykańskie, 1944

Fot. Naval History & Heritage Command; domena publiczna

Zwróć uwagę na...

- ▶ wykorzystanie przez aliantów informacji zdobytych dzięki dekryptażowi szyfrów Enigmy podczas walk z Niemcami w okresie II wojny światowej;
- ▶ związek pomiędzy pracą kryptologów podczas tego konfliktu zbrojnego a rozwojem informatyki.

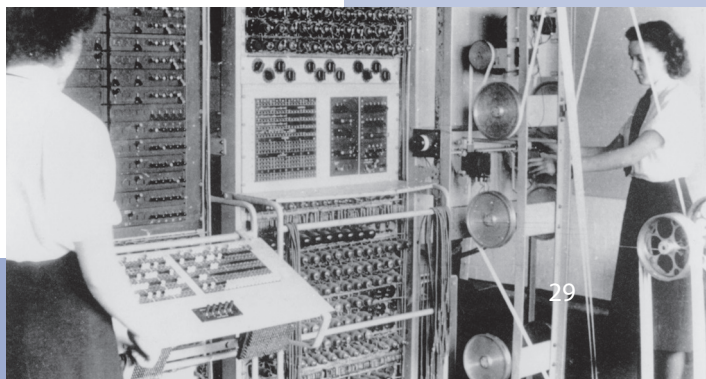
Czy wiesz, że...

- ▶ Brytyjska operacja wykorzystania informacji pochodzących z dekryptażu nosiła kryptonim „Ultra”. Istotne dane wywiadowcze pochodzące z tego źródła były przekazywane wojskom alianckim, ale dla bezpieczeństwa fakt łamania szyfru Enigmy ukrywano nawet przed oficerami własnej armii, wskazując, że udostępniane informacje pochodzą od agentów bądź wywiadu lotniczego.
- ▶ Maszyna Colossus, skonstruowana na podstawie projektu Alana Turinga, służyła do rozpracowania niemieckiej maszyny szyfrującej Lorenza, którą szyfrowano łączność najwyższych ogniw organizacyjnych wojsk niemieckich.

Maszyna Colossus Mark II, 1943

Fot. domena publiczna

W okresie wzmózonych 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. Poniższa fotografia prezentuje przykładową programowalną maszynę cyfrową



12 POWOJENNE LOSY

Minęło wiele dekad, nim prawda o skali zasług polskich kryptologów trafiła do szerszego grona odbiorców. Przez wiele lat Brytyjczycy wkład Polaków w złamanie szyfru Enigmy traktowali marginalnie. Z drugiej strony sytuacja polityczna w Polskiej Rzeczypospolitej Ludowej nie zachęcała byłych pracowników Biura Szyfrów do ujawniania swojej przeszłości.

W ostatnich latach działania podejmowane przez instytucje, naukowców oraz zaangażowanych społeczników świadczą o tym, że pamięć o „Pogromcach Enigmy” jest wciąż kultywowana. Ich dzieje przybliżają kolejne publikacje, wystawy, pomniki oraz tablice pamiątkowe.

Fragment ekspozycji w Centrum Szyfrów Enigma w Poznaniu

Fot. Ł. Gdąk/ Poznańskie Centrum Dziedzictwa

Centrum Szyfrów Enigma jest marką Poznańskiego Centrum Dziedzictwa, miejskiej instytucji kultury, która zachowuje pamięć o Poznaniu i jego spuściznie. Misją CSE jest budowanie świadomości, że złamanie szyfru niemieckiej maszyny szyfrującej Enigma było dziełem polskich matematyków: Mariana Rejewskiego, Henryka Żygalskiego 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



▲ Pomnik kryptologów w Poznaniu, 2022
Fot. ze zbiorów Witolda Sobóckiego



Zwróć uwagę na...

- powojenne losy Mariana Rejewskiego oraz Henryka Zygalskiego.

Czy wiesz, że...

- Po powrocie do Polski Marian Rejewski był inwigilowany przez organy bezpieczeństwa Polskiej Rzeczypospolitej Ludowej. Funkcjonariusze Urzędu Bezpieczeństwa, a następnie Służby Bezpieczeństwa, nie poznali jego faktycznych zasług w zakresie złamania szyfru Enigmy. Rejewski publicznie ujawnił swoje dokonania w r. 1967, składając wspomnienia w Wojskowym Instytucie Historycznym w Warszawie.



Henryk Zygalski z Berthą Blofield, 1955

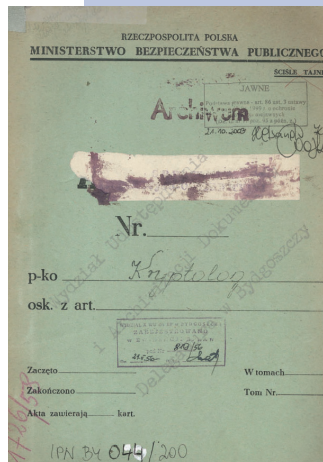
Fot. ze zbiorów p. Bryszak (CS Enigma)

Henryk Zygalski po zakończeniu II 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 Zygalskiego



Teczka sprawy obserwacyjno-ewidencyjnej kryptonim „Kryptolog” dot. rozpracowania Mariana Rejewskiego
Fot. ze zbiorów AIPN Poznań

Marian Rejewski zdecydował się na powrót do Polski. Zamieszkał wraz z rodziną w Bydgoszczy, gdzie pracował na stanowiskach związanych z księgowością i rachunkowością. Przez wiele lat skrywał sekret dotyczący złamania szyfru 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 jego kontakty



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

Vermerke:

Absendende Stelle:	te Meldung	Ort	Tag Monat	Stunde Minuten
	Abgegangen			
	Angesommen			
	An			

- ▶ Gdy kryptolog atakujący szyfr nie znał budowy Enigmy, teoretyczna liczba kombinacji (stanów) wojskowej maszyny szyfrującej wynosiła 3×10^{114} . Dzięki zastosowaniu zaawansowanej matematyki Marian Rejewski zredukował tę liczbę do 105 456 kombinacji.
- ▶ 6 egzemplarzom bomb Rejewskiego przeanalizowanie wszystkich możliwych pozycji startowych maszyny zajmowało 2 godziny.
- ▶ Stworzenie kompletu płacht Zygalskiego wymagało wyprodukowania 200 000 ręcznie wycinanych otworów.
- ▶ Polscy kryptolodzy podczas 9 miesięcy (od października 1939 r. do czerwca 1940 r.) w ośrodku „Bruno” odczytali 8840 zaszyfrowanych niemieckich radiogramów.
- ▶ Od końca 1942 r. do maja 1945 r., głównie dzięki czytaniu depesz szyfrowanych za pomocą Enigmy, alianci zatopili na Atlantyku 692 niemieckich okrętów podwodnych.
- ▶ Ośrodek Bletchley Park w 1945 r. zatrudniał 10 000 osób.

13 DEKRYPTAŻ ENIGMY W LICZBACH

Pusty formularz szyfrogramu używany przy obsłudze Enigmy
Fot. Cryptomuseum.com, domena publiczna

PODSUMOWANIE

14

„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 przezwyciężenia»”.

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

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



Odnaczenie 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



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

KALENDARIUM

1918

- ▶ **II 1918** – niemiecki inżynier Artur Scherbius złożył patent dotyczący wirnikowej maszyny szyfrującej, na bazie której powstała Enigma.

1919

- ▶ **VIII 1919** – ppor. Jan Kowalewski złamał bolszewicki szyfr „Delegat”.

1923

- ▶ **1923** – firma Scherbius&Ritter wprowadziła na niemiecki rynek maszyny Enigma w wersji handlowej.

1926

- ▶ **1926** – wojskowe wersje Enigmy zostały wprowadzone do użytku w niemieckiej marynarce wojennej.

1928

- ▶ **1928** – Enigma została wprowadzona do użytku w niemieckich wojskach lądowych.
- ▶ **15 VII 1928** – polskie stacje nasłuchowe przechwyciły pierwsze szyfrogramy sporządzone przy pomocy Enigmy.

1929

- ▶ **15 I – 22 III 1929** – w tym czasie trwał kurs kryptologiczny dla wybranych studentów matematyki Uniwersytetu Poznańskiego. Najlepsi z nich zostali zatrudnieni w ekspozyturze Biura Szyfrów.

- ▶ **01 IX 1929 – 31 VIII 1932** – działalność ekspozytury Biura Szyfrów w Poznaniu, podczas której łamane były niemieckie szyfry ręczne dzięki metodom omówionym na kursie kryptologicznym. W tej komórce zostali zatrudnieni Marian Rejewski, Jerzy Różycki oraz Henryk Żygalski.
- ▶ **IX 1929** – miał miejsce pierwszy samodzielny sukces trójki poznańskich kryptologów: złamanie czteroliterowego kodu niemieckiej marynarki.
- ▶ **31 XII 1929** – Marian Rejewski za pomocą teorii permutacji odszyfrował pierwszy szyfrogram sporządzony przy pomocy Enigmy.

1930

- ▶ **wiosna 1930** – na podstawie matematycznych obliczeń Mariana Rejewskiego firma AVA stworzyła kopie maszyny Enigma, niezbędne do sprawnego dekrzyptażu.
- ▶ **I 1930** – do Mariana Rejewskiego dołączyli Jerzy Różycki i Henryk Żygalski, od tej pory w trójkę opracowywali metody łamania szyfru Enigmy.

1932

- ▶ **X–XII 1932** – Marianowi Rejewskiemu powierzono zadanie samodzielnego złamania szyfru Enigmy. Kpt. Gustave Bertrand przekazał Polakom zdobyte dzięki pracy wywiadowczej dokumenty dotyczące Enigmy.
- ▶ **01 IX 1932** – została zlikwidowana Ekspozytura Biura Szyfrów w Poznaniu. Personel został przeniesiony do Pałacu Saskiego w Warszawie.
- ▶ **koniec XII 1932** – Marian Rejewski za pomocą teorii permutacji odszyfrował pierwszy szyfrogram sporządzony przy pomocy Enigmy.

1934

- ▶ **1 VIII 1934** – Enigma została wprowadzona do niemieckich sił powietrznych – Luftwaffe.

1936

- ▶ **od II 1936** – Niemcy wprowadzili szereg zmian w konstrukcji maszyny Enigma i procedurach z nią związanych.

1937

- ▶ **1937** – został utworzony tajny ośrodek kryptologiczny w Pyrach k. Warszawy, gdzie zostali przeniesieni polscy kryptolodzy.

1938

- ▶ **15 IX 1938** – Niemcy wprowadzili zmianę w procedurze szyfrowania polegającą na odmiennym dla każdej depeszy ustawieniu pierścieni szyfrujących, co spowodowało poważne utrudnienia w pracy polskich kryptologów.
- ▶ **X 1938** – w odpowiedzi na niemieckie modyfikacje maszyny Enigma Marian Rejewski opracował bombę kryptologiczną, a Henryk Zygałski – płachty Zygałskiego. Oba te narzędzia pomagały w sprawnym dekrypcie niemieckich depesz.

1939

- ▶ **I 1939** – Niemcy wprowadzili dwa kolejne wirniki szyfrujące. Strona polska jedynie sporadycznie była w stanie odszyfrować niemieckie depesze.
- ▶ **25–27 VII 1939** – w Pyrach k. Warszawy miało miejsce spotkanie przedstawicieli Francji, Wielkiej Brytanii i Polski. Polacy przekazali swoim sojusznikom wiedzę, urządzenia i opracowane przez siebie metody łamania szyfru Enigmy.
- ▶ **koniec VIII 1939** – w Wielkiej Brytanii został uruchomiony ośrodek Bletchley Park, gdzie Brytyjczycy adaptowali i rozwijali polskie metody dekrypcy.
- ▶ **1 IX 1939** – wybuchła II wojna światowa.
- ▶ **6 IX 1939** – rozpoczęła się ewakuacja personelu Biura Szyfrów w ślad za Naczelnym Wodzem. Podczas ewakuacji personel Biura Szyfrów zadbał o zatarcie wszelkich śladów dotyczących polskich sukcesów w zakresie łamania szyfrów Enigmy.
- ▶ **17 IX 1939** – personel Biura Szyfrów przekroczył granicę polsko-rumuńską.
- ▶ **X 1939** – na terenie Francji został uruchomiony ośrodek „Bruno”, w którym pracował m.in. polski personel Biura Szyfrów ewakuowany z Rumunii.

1940

- ▶ **17 I 1940 r** – Alan Turing odwiedził w ośrodek „Bruno”, w tym czasie polscy kryptolodzy zademonstrowali łamanie szyfru Enigmy przy pomocy płacht Zygałskiego.
- ▶ **IV 1940** – zespół z Bletchley Park i ośrodka „Bruno”, współpracując ze sobą na bieżąco, łamał depesze szyfrowane za pomocą Enigmy podczas kampanii norweskiej.
- ▶ **VI 1940** – z powodu agresji Niemiec na Francję nastąpiła ewakuacja zespołu pracującego w ośrodku „Bruno” do Afryki Północnej.
- ▶ **IX 1940** – personel ośrodka „Bruno” powrócił z Afryki Północnej do Francji, prace kryptologiczne zostały wznowione w nowo zorganizowanym ośrodku „Cadix” w okolicach miejscowości Uzes, w nieokupowanej części Francji – Republice Vichy. Polscy kryptolodzy i oficerowie służbowo podlegali Oddziałowi II Naczelnego Wodza, organizacyjnie zaś – płk. Gustave'owi Bertrandowi.

1941

- ▶ **I 1941** – Gustave Bertrand utworzył filię ośrodka „Cadix” w Algierze.
- ▶ **III 1941** – na pokładzie niemieckich okrętów Brytyjczycy zdobyli egzemplarz Enigmy, zestaw bębneków i książ z ustawieniami maszyny używanej w niemieckiej marynarce wojennej. Materiały te pozwoliły kryptologom z Bletchley Park odczytywać depeche używane w niemieckiej marynarce wojennej.
- ▶ **VI 1941** – Brytyjczycy złamali szyfr Enigmy używanej we włoskiej marynarce oraz prowadzili skuteczny dekryptaż depech niemieckich nadawanych podczas ataku III Rzeszy na Związek Sowiecki.

1942

- ▶ **9 I 1942** – miała miejsce katastrofa morska statku Lamoricière, w której zginęła część personelu Biura Szyfrów: Jerzy Różycki, kpt. Jan Graliński oraz Piotr Smoleński.
- ▶ **II 1942** – niemiecka marynarka wojenna wprowadziła do użytku czterowirnikową wersję maszyny Enigma.
- ▶ **X 1942** – Brytyjczycy na pokładzie niemieckiego okrętu U-559 zdobyli egzemplarz czterowirnikowej Enigmy – od tego momentu pracownicy Bletchley Park byli w stanie znów prowadzić skuteczny dekryptaż.
- ▶ **XI 1942** – miało miejsce wkroczenie wojsk niemieckich i włoskich do Republiki Vichy i likwidacja ośrodka „Cadix” oraz chaos organizacyjny związany z nieudanymi próbami ewakuacji jego personelu.

1943

- ▶ **I-II 1943** – podczas ewakuacji polskich kryptologów przez granicę francusko-hispańską Marian Rejewski i Henryk Zygański zostali aresztowani przez hispańską policję i osadzeni w więzieniu. Maksymilian Cieżki, Gwido Langer i Antoni Palluth z kolei zostali zatrzymani przez Francuzów, a następnie trafili do niemieckiej niewoli.
- ▶ **VIII 1943** – Marian Rejewski i Henryk Zygański zostali zwolnieni z więzienia i trafili do Wielkiej Brytanii, gdzie otrzymali stopnie wojskowe i do końca wojny służyli w Kompanii Radiowywiadowczej Batalionu Łączności Sztabu Naczelnego Wodza.

1944

- ▶ **18 IV 1944** – Antoni Palluth zginął podczas bombardowania fabryki Heinkla, w której pracował jako więzień obozu koncentracyjnego w Sassenhausen.

1945

- ▶ **V 1945** – Maksymilian Ciężki został uwolniony przez wojska alianckie i trafił do Wielkiej Brytanii.

1946

- ▶ **XI 1946** – Marian Rejewski powrócił do Polski.

1967

- ▶ **IV 1967** – Marian Rejewski złożył w Wojskowym Instytucie Historycznym *Wspomnienia z mej pracy w Biurze Szyfrów Oddziału II Sztabu Głównego w latach 1930–1945*.

1973

- ▶ **1973** – we Francji ukazała się książka Gustave'a Bertranda, *Enigma, ou la plus grande énigme de la guerre 1939–45*, w której po raz pierwszy ujawniono tajemnicę złamania szyfru Enigmy.

1974

- ▶ **1974** – Marian Rejewski złożył w Wojskowym Instytucie Historycznym uzupełnienia do swoich wspomnień.

1980

- ▶ **13 II 1980** – miała miejsce śmierć Mariana Rejewskiego.

MODUŁ EDUKACYJNY

1. Znajdź poniższe wyrazy na wykreślanie i je skreśl. Słowa zostały umieszczone poziomo, pionowo lub ukośnie, niektóre z nich mogą być zapisane wspak:

CYKLOMETR, REJEWSKI, ENIGMA, KRYPTOLOGIA, WYWIAD, WIRNIKI

Następnie, opierając się o treść wystawy, wyjaśnij ich znaczenie.

Ł	X	I	Ż	J	D	Ń	P	Z	Ó	D	I	M	G
D	T	G	Ż	S	W	Y	W	I	A	D	L	V	Y
Ę	D	A	Ż	V	O	V	Ł	Ń	Ę	L	J	L	E
M	V	Y	I	G	A	W	I	R	N	I	K	I	L
D	P	M	Ł	G	I	T	L	Ą	J	I	B	Ł	H
S	O	G	Ć	Ś	O	G	Ś	M	N	W	Z	Z	C
Z	L	Y	C	Y	K	L	O	M	E	T	R	V	T
Ł	I	W	T	U	K	C	O	Ł	H	Ą	K	X	E
N	B	T	T	I	U	A	P	T	X	W	C	Ż	L
Ą	I	Ś	Ż	Z	E	Ł	Ł	Ł	P	V	J	Ó	B
L	U	Ż	A	M	G	I	N	E	X	Y	Ż	Ł	Ń
Z	S	R	D	U	K	J	V	L	Ó	F	R	Ó	H
Ń	Z	Ę	S	V	R	R	E	J	E	W	S	K	I
Ó	K	Ć	H	Ż	J	K	Ż	J	T	W	B	N	R

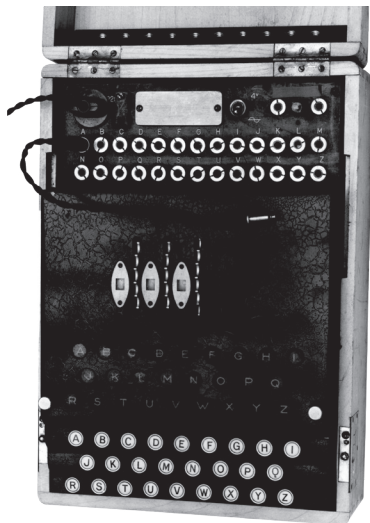
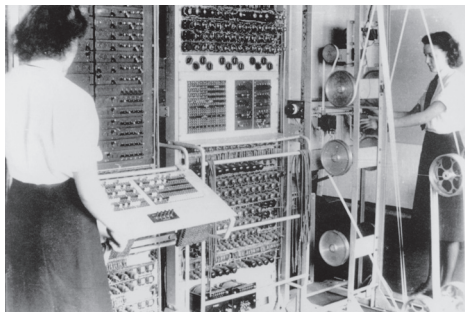
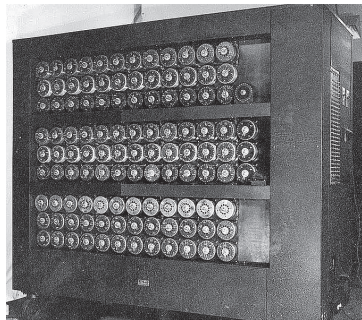
2. W oparciu o informacje z wystawy wskaż zdania prawdziwe (P) oraz fałszywe (F).

- ☐ Wojskowe wersje maszyny szyfrującej Enigma były takie same jak te przeznaczone na rynek cywilny.
- ☐ Rozpracowywaniem szyfru Enigmy zajmowały się służby wywiadowcze brytyjskie, francuskie oraz polskie.
- ☐ Dane dotyczące układu okablowania poszczególnych elementów odpowiedzialnych za szyfrowanie w Enigmie typu wojskowego były powszechnie dostępne.
- ☐ Maksymilian Ciężki był współwłaścicielem firmy radiotechnicznej AVA.
- ☐ Jerzy Różycki stworzył metodę zegara.
- ☐ Konferencja polsko-brytyjsko-francuska w Pyrach odbyła się w r. 1939.
- ☐ Zespół polskich kryptologów we wrześniu 1939 r. dostał się do niemieckiej niewoli.
- ☐ Jerzy Różycki zginął tragicznie w 1942 r.
- ☐ Kryptonim ośrodka w Bletchley Park brzmiał: „Station I”.
- ☐ Marian Rejewski powrócił do Polski po zakończeniu II wojny światowej.
- ☐ Enigma generowała 3×100 kombinacji.

3. Podane wydarzenia ułóż w kolejności chronologicznej. Przy najwcześniejszym wydarzeniu zapisz „1”, a przy najpóźniejszym – „7”.

- ☐ Przybycie zespołu kryptologów do Wielkiej Brytanii.
- ☐ Złamanie szyfru Enigmy przez Mariana Rejewskiego.
- ☐ Utworzenie w Poznaniu kursu kryptologicznego dla studentów matematyki.
- ☐ Ewakuacja Biura Szyfrów przez granicę polsko-rumuńską.
- ☐ Wynalezienie bomby Rejewskiego.
- ☐ Praca polskich kryptologów na terenie Francji.
- ☐ Przekazanie przez Polaków wiedzy na temat łamania szyfru Enigmy Francuzom i Brytyjczykom.

4. Odnajdź fotografie na wystawie i podpisz je:



5. Uzupełnij luki podanymi w ramce wyrażeniami tak, by tekst stanowił spójną informację.

Alan Turing, AVA, „Cadix”, „Bruno”, Zdzisławem Krygowskim, matematyki, Marian Rejewski, permutacji, Jerzy Różycki, Bletchley Park, Henryk Zygałski

Historia złamania przez Polaków szyfru niemieckiej maszyny Enigma rozpoczęła się w Poznaniu. W 1929 r. oficerowie polskiego wywiadu wojskowego wraz z profesorem Uniwersytetu Poznańskiego zorganizowali kurs kryptologiczny dla najlepszych studentów Na zajęciach tych szkolono studentów w zakresie wiedzy o szyfrach. Trzech najlepszych kursantów po zakończeniu szkolenia zostało zatrudnionych w ekspozyturze Biura Szyfrów w Poznaniu. W 1932 r. zostali oni przeniesieni do Warszawy. W grudniu tego samego roku wykorzystał matematyczną teorię zrekonstruował działanie i budowę niemieckiej maszyny Enigma i odczytał pierwszy szyfrogram. Jego obliczenia matematyczne posłużyły firmie radiotechnicznej do stworzenia kopii Enigmy, które służyły do czytania depeesz. Prace nad sprawnym dekryptażem wymagały zaangażowania pozostałych dwóch matematyków.

Skomplikowany algorytm szyfrujący maszyny, a także wprowadzone przez Niemców zmiany w samej jej konstrukcji i procedurach spowodowały, że zespół kryptologów musiał opracowywać nowe sposoby łamania szyfrów. Tymczasem zbliżała się II wojna światowa. W ośrodku kryptologicznym w Pyrach pod Warszawą w dniach 25–26 lipca 1939 r. odbyła się tajna konferencja, podczas której Polacy przekazali kryptologom z Francji i Wielkiej Brytanii metody łamania szyfru Enigmy. Po wybuchu wojny personel Biura Szyfrów ewakuował się do Rumunii. Polscy kryptolodzy i oficerowie następnie przedostali się do Francji, gdzie kontynuowali pracę. W tym kraju utworzono ośrodek który po ataku Niemiec na Francję w 1940 r. został przeniesiony na południe kraju i otrzymał kryptonim Filia tego ośrodka znajdowała się w Algierze. 9 stycznia 1942 r. w katastrofie morskiej zginął..... W listopadzie 1943 r. placówkę rozwiązano, a kryptolodzy trafili do Wielkiej Brytanii. Zostali tam skierowani do jednostki radiowywiadowczej przy Sztapie Naczelnego Wodza, gdzie służyli do końca II wojny światowej. Jeden z nich, po wojnie pozostał w Wielkiej Brytanii, drugi zaś powrócił do Polski.

Jeszcze przed wybuchem II wojny światowej w Wielkiej Brytanii utworzono ośrodek w którym zaadaptowano i rozwinięto osiągnięcia polskiego Biura Szyfrów. Miejsce to stało się kryptologicznym centrum aliantów, gdzie łamano szyfr powstający przy użyciu Enigmy i inne szyfry używane przez III Rzeszę oraz jej sojuszników. Pozyskane w ten sposób informacje były wykorzystywane przeciwko Niemcom na wielu frontach II wojny światowej. Jednym z najsłynniejszych pracowników tego ośrodka był – matematyk uważany za twórcę komputera.

6. Odnajdź na wystawie lata życia podanych osób. Do każdego nazwiska dopasuj krótką charakterystykę postaci – wpisz do tabeli odpowiadającą jej cyfrę (1–6).

Imię i nazwisko	Lata życia	Charakterystyka
Maksymilian Ciężki		
Antoni Palluth		
Marian Rejewski		
Zdzisław Krygowski		
Gustave Bertrand		
Alan Turing		

Charakterystyki do dopasowania:

1. Pracownik Biura Szyfrów, jeden z wykładowców na kursie kryptologicznym, współzałożyciel firmy AVA.
2. Brytyjski matematyk, pracownik Bletchley Park, konstruktor bomby kryptologicznej.
3. Polski kryptolog, matematyk. Jako pierwszy na świecie złamał szyfr Enigmy, wykorzystując matematyczną teorię permutacji.
4. Profesor matematyki, współorganizator kursu kryptologicznego odbywającego się w Poznaniu w 1929 r.
5. Francuski oficer wywiadu, uczestnik konferencji w Pyrach, przekazał Polakom dokumenty dotyczące Enigmy.
6. Szef sekcji niemieckiej Biura Szyfrów, inicjator stworzenia kursu kryptologicznego dla poznańskich studentów matematyki.

7. Krótki kurs szyfrowania

Jak już wiesz z treści wystawy, w 1929 r. w Poznaniu rozpoczął się kurs kryptologiczny dla studentów matematyki. Kursanci nie mieli nigdy wcześniej styczności z szyframi, zatem musieli się nauczyć wielu sposobów ich używania oraz poznać metody ich łamania.

Spróbujmy podążać ich śladem – przed Tobą kilka prostych szyfrów.

SZYFR CEZARA

W szyfrze Cezara daną literę zamieniamy na inną, oddaloną od niej w alfabecie o trzy pozycje w prawo. Aby stworzyć szyfrogram, należy zastąpić literę jawną (górny wiersz tabeli) odpowiadającą jej literą z wiersza dolnego. Deszyfrowanie z kolei polega na operacji odwrotnej – zastępujemy literę w szyfrogramie z dolnego wiersza odpowiadającą jej literą z wiersza górnego.

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
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Słowo ENIGMA zaszyfrowane w ten sposób przybierze postać: HQLJPD.

SZYFR POLIBIUSZA

W szyfrze Polibiusza poszczególnym literom alfabetu przyporządkowane są pary cyfr. Aby zaszyfrować literę, należy odszukać ją w poniższej tabeli i zapisać w ją; pierwsza cyfra odpowiada numerowi kolumny, a druga – wiersza.

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Słowo ENIGMA zaszyfrowane w ten sposób
przybierze postać: 51 33 42 22 23 11.

SZYFR POLIALFABETYCZNY TABLICOWY

Szyfr ten tworzy alfanumeryczna tablica, składająca się z dziewięciu kolumn i dziewięciu wierszy. W pierwszej kolumnie znajduje się słowo-klucz, w tym wypadku: PILSUDSKI. Komórki kolejnych kolumn wypełniają kolejne litery alfabetu, występujące po danej literze ze słowa kluczowego. Jeżeli w pierwszej komórce pierwszej kolumny znajduje się litera P, to w kolejnej komórce wiersza znajdzie się litera Q, po niej R, S, T itd. Zasada ta jest powtórzona w kolejnych komórkach.

Używając tego szyfru, poszczególne litery zapisuje się w formie par cyfr jak w szyfrze Polibiusza (numer kolumny i numer wiersza). Zapis rozpoczynamy od pierwszego wiersza, w którym dana litera występuje. Gdy ta sama litera pojawi się w wiadomości po raz drugi, korzystamy na następnego wiersza z daną literą. W przypadku, gdy dotrzemy do ostatniego wiersza z daną literą, zapisujemy ją znów „od góry”. Podobnie jak w poprzednich przypadkach – deszyfrowanie polega na wykonaniu operacji odwrotnej. Jak zapewne już zauważyłeś – ta sama litera może być zapisana za pomocą różnych cyfr. Słowo ZAGADKA zapisane tym szyfrem przybierze postać: 84 94 46 75 16 32 97.

	1	2	3	4	5	6	7	8	9
1	P	Q	R	S	T	U	V	W	X
2	I	J	K	L	M	N	O	P	Q
3	L	M	N	O	P	Q	R	S	T
4	S	T	U	V	W	X	Y	Z	A
5	U	V	W	X	Y	Z	A	B	C
6	D	E	F	G	H	I	J	K	L
7	S	T	U	V	W	X	Y	Z	A
8	K	L	M	N	O	P	Q	R	S
9	I	J	K	L	M	N	O	P	Q

Ten sposób szyfrowania (oczywiście z innymi słowami kluczowymi) był stosowany przez struktury Polskiego Państwa Podziemnego.

Używając wymienionych wyżej szyfrów, spróbuj odczytać poniższy szyfrogram:

52 43 33 42 51 31

ZRMQB

URCZRM

12 62 36 72 31 38 94 51 77 39 19

Prawidłowe rozwiązanie składa się z dwóch wyrażений związanych z historią złamania szyfru Enigmy. Uzasadnij, w jaki sposób łączą się one z tym ważnym sukcesem polskich kryptologów.

Nauczyciel dzieli klasę na kilkoosobowe grupy. Każda z nich otrzymuje arkusz papieru i flamastry lub kredki. Uczniowie zapisują na środku arkusza frazę „Złamanie szyfru Enigmy”, a następnie podają własne skojarzenia związane ze wskazanym zagadnieniem – mogą być one zapisane w formie haseł lub rysunków. Poszczególne elementy naniesione przez zespoły powinny stanowić układ wzajemnych powiązań. Przedstawiciele każdej z grup objaśniają stworzone w ten sposób mapy mentalne.

9. W oparciu o plansze wystawy „Problem Enigmy” (w broszurze s. 9–11) oraz „Poznanie tajemnic”(w broszurze s. 18–19) i swoją wiedzę na temat rozwoju ówczesnej techniki oceń, czy złamanie szyfru Enigmy przez Mariana Rejewskiego było proste. Jakimi narzędziami mogli posługiwać się kryptolodzy w okresie międzywojennym, a z jakich mogliby korzystać obecnie? Odpowiedź uzasadnij.

10. W oparciu o planszę wystawy „Od kryptologii do informatyki” (w broszurze s. 28) wskaż, w jaki sposób złamanie szyfru Enigmy wpłynęło na przebieg II wojny światowej oraz jakie inne, długofalowe skutki niosło ze sobą to wydarzenie.

Tekst źródłowy nr 1

Fragment elaboratu ppłka Ludwika Sadowskiego *Oddział II Sztabu Generalnego.*

Rezultaty pracy i przygotowania do wojny sporządzonego w 1941 r.

Prace kryptologiczne w dziedzinie szyfrów niemieckich były postawione na ogół bardzo wysoko, zdaje się, że wyżej niż w odpowiednich komórkach sztabu francuskiego czy angielskiego. Szyfry transpozycyjne były rozwiązywane, używane jednak przez Niemców w niewielkiej ilości. Niemiecka maszyna szyfrowa „Enigma” została na kilka lat przed wojną rozwiązana, przy czym opracowano system techniczny ułatwiający odczytywanie zaszyfrowanych tą maszyną depesz niemieckich.

Na ogół, do 1938 r. praca radiowywiadu i szyfrów niemieckich stanowiła cenny wkład rozpoznania rozbudowy sił zbrojnych Niemiec przez Wydział Studiów Oddziału II, zwłaszcza w następujących dziedzinach:

- niemiecka łączność radiowa (ustalenie miejsca postoju niemieckich stacji radio, podział na kategorię, przydziały)
- ustalenie OdeB¹ wojska i floty niemieckiej (często bardzo cenne wiadomości dotyczące identyfikacji nowych mas nieznanymi jednostek)
- obserwacja ćwiczeń i manewrów, kiedy to działalność radiostacji była szczególnie intensywna.

Dużo pożytecznego materiału dostarczył radiowywiad niemiecki przed i po aneksji Austrii. Udało się odczytać ponadto szereg cennych wiadomości z dziedziny uzbrojenia i przemysłu uzbrojeniowego.

Nie umniejszając wartości rezultatów pracy szyfrów niemieckich, trzeba stwierdzić jednak, iż charakter tych wiadomości był fragmentaryczny i przypadkowy. Niestety, wprowadzenie modyfikacji do niemieckiej maszyny szyfrowej przerwało w okresie sudeckim odczytywanie depesz tymi maszynami szyfrowanych i ograniczyło je jedynie do rzadkich wypadków kiedy w użyciu tej maszyny zbiegały się znane nam elementy. Studia i prace techniczne nad rozwiązaniem tego zagadnienia trwały do wybuchu wojny, dla przyspieszenia ich nawiązano kontakt i wymianę ze sztabem francuskim i angielskim (tuż przed wojną).

Źródło: L. Sadowski, *Oddział II Sztabu Generalnego. Rezultaty pracy i przygotowania do wojny*, wstęp A. Suchitz, opracowanie M. Sobieraj, Łódź 2014, s 56–57.

1

OdeB – skrót od: *Orde de bataillie* (fr. ‘porządek bitewny’) – schemat organizacyjny wojsk.

Pytania do tekstu

- 1) Jak autor opracowania ocenia pracę polskiej komórki odpowiedzialnej za łamanie szyfrów niemieckich na tle analogicznych komórek sztabu francuskiego oraz angielskiego?
- 2) Czego dotyczyły informacje na temat Niemiec zdobyte dzięki złamaniu szyfru Enigmy przez polski wywiad? Co sądzą o nich autor?
- 3) Ostatnie zdanie przytoczonego fragmentu tekstu dotyczy współpracy kryptologicznej pomiędzy Polakami, Brytyjczykami i Francuzami. Korzystając z wystawy, wskaż przełomowe wydarzenie dotyczące tej współpracy.

Tekst źródłowy nr 2

Fragment memorandum Mariana Rejewskiego *Kilka uwag na temat trudności, w jakich znajduje się w chwili obecnej dział szyfrów niemieckich, 20 X 1944 r.*

Przed wybuchem wojny istniała w dziedzinie szyfrów współpraca polsko-angielsko-francuska, w czasie trwania której, należy to z całym naciskiem podkreślić, stroną dającą i to hojnie dającą, była wyłącznie strona polska. Byłoby wskazaniem przypomnieć obecnie Anglikom o długu wdzięczności, jaki wobec polskiego Biura Szyfrów zaciągnęli, przypomnieć, że bez pomocy Polaków nie byłiby w czasie kampanii norweskiej i francuskiej oraz później odczytać ani jednego szyfrogramu niemieckiego i domagać się od nich, by współpracowali z Polakami równie lojalnie, jak Polacy pracowali i pracują z nimi. Nie ulega wątpliwości, że ze strony władz polskich odpowiednie zabiegi były już, i to może niejednokrotnie, robione. Tym niemniej wydaje się celowym jeszcze raz sprecyzować, czego się polscy kryptolodzy od swoich angielskich kolegów spodziewają i domagają. Należałoby przede wszystkim zażądać od nich zwrotu darowanej im w swoim czasie przez Polaków niemieckiej maszyny Enigma. Maszyna ta jest polskim kryptologom potrzebna, jeżeli nie do innych celów, to choćby do celów archiwalnych. Wypada, by ci, którzy maszynę zrekonstruowali byli w posiadaniu choć jednego jej egzemplarza.

Następnie należałoby wymóc na nich, by zechcieli się podzielić doświadczeniami poczynionymi przez nich w ciągu ostatnich pięciu lat w dziedzinie szyfrów niemieckich, najlepiej przez bezpośrednie skontaktowanie się zainteresowanych kryptologów polskich i angielskich.

I wreszcie należałoby spróbować nakłonić ich, by zechcieli dostarczać swój materiał podsłuchowy. W tej dziedzinie polskie możliwości są bardzo ograniczone i pomoc angielska byłaby niezmiernie cenną.

Źródło: E. Maresch, *Kompania radiowywiadowcza w Anglii*, [w:] *Marian Rejewski 1905–1980. Życie Enigmą pisane*, wstęp: Z. Brzeziński, zespół red. J.S. Ciechanowski et al., Bydgoszcz 2005, s. 199.

Pytania do tekstu:

- 1) Dlaczego, zdaniem Mariana Rejewskiego, Polacy mają prawo żądać pomocy od Anglików w zakresie łamania szyfrów niemieckich?
- 2) Jak ta pomoc powinna wyglądać?

Tekst źródłowy nr 3

List Mariana Rejewskiego do Ministerstwa Obrony Narodowej Polskiej Rzeczypospolitej Ludowej w sprawie swojej przeszłości kryptologicznej

Bydgoszcz, dnia 29 kwietnia 1956 r.

Do
Ministerstwa Obrony Narodowej
w Warszawie

Jako były pracownik Biura Szyfrów Oddziału II Sztabu Głównego w Warszawie w okresie lat 1932–1939, a następnie jako żołnierz przydzielony do roku 1946 do Oddziału Radio Sztabu N.W. Polskich Sił Zbrojnych za granicą zapytuję się uprzejmie, czy nabyta ongiś przeze mnie wiedza fachowa i praktyka w rozwiązywaniu szyfrów niemieckich, może być jeszcze w jakikolwiek sposób władzom wojskowym przydatna.

Pomimo, że wróciłem do kraju już w roku 1946, to jednak do tej pory z podobnym zapytaniem jeszcze się nie zwracałem, wychodząc z założenia, prawdopodobnie uzasadnionego, że propozycję moją przyjęłoby z nieufnością.

Być może, że chwila obecna jest bardziej sprzyjająca dla składania tego rodzaju ofert.

Źródło: Archiwum IPN, IPN BU 2602/3259, 29 IV 1956 r., k. 32.

Pytania do tekstu:

- 1) Co oferuje Marian Rejewski władzom wojskowym Polskiej Rzeczypospolitej Ludowej?
- 2) Odwołując się do wiedzy na temat historii Polski w latach 1944–1989, odpowiedz, dlaczego dopiero po 10 latach przebywania w kraju autor postanowił wyjawić swoją kryptologiczną przeszłość?

WYBRANA BIBLIOGRAFIA

- Garliński J., *Enigma. Tajemnica drugiej wojny światowej*, Londyn 1980.
- Grajek M., *Enigma. Bliżej prawdy*, Poznań 2007.
- *Marian Rejewski 1905–1980. Życie Enigmą pisane*, wstęp Z. Brzeziński, zespół red. J. S. Ciechanowski et al., Bydgoszcz 2005.
- Piper F., Murphy S., *Kryptografia. Krótki kurs*, Warszawa 2022.
- Rejewski M., *Wspomnienia z mej pracy w Biurze Szyfrów Oddziału II Sztabu Głównego w latach 1930–1945*, Poznań 2021.
- Turing D., XYZ. *Prawdziwa historia złamania szyfru Enigmy*, Poznań 2019.

Dekryptaż – proces ustalania klucza szyfrowego bez jego znajomości, inaczej kryptoanaliza, rozwiązywanie lub łamanie szyfrów.

Deszyfrowanie – odczytywanie zaszyfrowanych wiadomości przy pomocy klucza szyfrowego.

Kod – sposób zapisywania informacji polegający na przekształcaniu poszczególnych wyrazów lub wyrażeń na inne znaki lub symbole w sposób znany nadawcy i odbiorcy. Powszechnie stosowanym kodem są znaki drogowe. Do odmian kodu należą kryptonimy oraz pseudonimy.

Klucz szyfrowy – informacja która określa sposób przekształcenia tekstu podczas szyfrowania i deszyfrowania. W przypadku maszyny Enigma w skład klucza wchodziły ustawienia początkowe maszyny wraz z indywidualnym hasłem nadawanym podczas szyfrowania.

Kryptologia – dziedzina wiedzy zajmująca się sposobami utajniania informacji przy pomocy kodów i szyfrów. Obejmuje kryptoanalizę (zob. dekryptaż) oraz kryptografię zajmującą się opracowywaniem nowych kodów lub szyfrów.

Szyfr – sposób utajniania informacji polegający na przekształcaniu poszczególnych znaków pisma (np. liter alfabetu) na inne znaki (np. cyfry) według określonego systemu znanego nadawcy i odbiorcy przy pomocy klucza szyfrowego.

Teoria permutacji – dział matematyki zajmujący się badaniem przestawień elementów w danym zbiorze w określonej kolejności. Za pomocą permutacji można przykładowo określić, na ile sposobów możemy rozmieścić osoby w kolejce. Wykorzystując tę gałąź matematyki, Marianowi Rejewskiemu udało się w grudniu 1932 r. odczytać depezę sporządzoną przy użyciu Enigmy.



INSTYTUT
PAMIĘCI
NARODOWEJ