

# Maszyna szyfrująca ENIGMA

## H i s t o r i a   r o z w i ą z a n i a

Poniższy tekst powstał w oparciu o materiały książkowe, między innymi o popularyzatorską, lecz solidnie opracowaną pozycję Davida Kahn *Seizing the Enigma: The Race to Break the German U-Boat Codes, 1939-1943* (Wydawnictwo.: Houghton Mifflin, Boston, 1991) oraz o książkę Krzysztofa Gaja *Szyfr Enigmy. Metody złamania*.

Wszelkie uwagi oraz zapytania dotyczące poniższego tekstu, również jego rozpowszechniania, proszę kierować do [Autora](#).

1. Wprowadzenie Enigmy na wyposażenie Armii Niemieckiej.
2. Biuro Szyfrów, jego pracownicy i ich pierwsze osiągnięcia.
3. Zastosowanie wyższej matematyki do rozwiązania szyfru.
4. Współpraca wywiadu francuskiego z polskim Biurem Szyfrów.
5. Odczytywanie przez polskich kryptologów depesz kodowanych Enigmą.
6. Przekazanie materiałów rozwiązywanej przez wywiad polski zagadki Enigmy wywiadom Francji i Anglii.

Po stopniowym, powolnym i trwającym aż do dzisiaj odtajnianiu archiwów II wojny światowej, historycy badający dostępne materiały zgodnie stwierdzają, że rozwiązanie zagadki Enigmy stanowiło rolę przysłowiowego jęczyczka u wagi przeważającego szale zwycięstwa sił alianckich nad Niemcami.

Operacje odczytywania niemieckich meldunków w czasie II wojny światowej również przez wiele lat powojennych osłonięte były największą tajemnicą. Tym bardziej nie znany był wkład Polaków w rozwiązanie kodu Enigmy. Pierwszą publikacją wyłaniającą na światło dzienne fakt przedwojennego odczytywania kryptogramów Enigmy, była książka Władysława Kozaczuka *Bitwa o tajemnice. Służby wywiadowcze Polski i Rzeszy Niemieckiej 1922-1939*, wydana w Warszawie w 1967 roku. Na potwierdzenie tej rewelacyjnej wówczas tezy należało czekać sześć lat, kiedy to ukazała się we Francji publikacja generała Gustawa Bertrand *Enigma czyli największa zagadka wojny 1939-1945*.

Od tej pory ukazało się co najmniej kilkadziesiąt, bardziej lub mniej poważnych prac, omawiających próby rozwiązania - wielokrotnie udoskonalanego przez Niemców - szyfru znanego pod postacią Enigma. Pomijając kilka merytorycznie absurdalnych książek, wiele z tych prac cechuje lekkie podejście do tematu, często graniczące z fikcją, sporo jednak pozycji przedstawia historię rozwiązania szyfru w świetle dokumentalnym.

Oto [przykład wybranych pozycji literatury przedmiotowej](#).

(Mówiąc o opracowaniach, w których nierzetelnie - bądź wcale - korzystano z materiałów źródłowych, warto wspomnieć o książce brytyjskiego pułkownika lotnictwa F. W. Winterbotham *The Ultra Secret*. Książka ta jest warta wzmianki z tego względu, iż rozpowszechniła błędną i krzywdzącą tezę o pierwszeństwie Anglików w rozwiązaniu zagadki Enigmy. Teza ta, już dawno przez historyków zarzucona, całkiem mocno wbiła się w świadomość wielu Brytyjczyków i do dnia dzisiejszego [można znaleźć jej ślady](#).)

Czymże jednakże była Enigma, jak doszło do jej rozwiązania i w jaki sposób doszło do wymiany informacji pomiędzy służbami wywiadowczymi Francji, Polski i Anglii?

## **1. Wprowadzenie ENIGMY na wyposażenie Armii Niemieckiej.**

Cofnijmy się do roku 1918, kiedy to niemiecki wynalazca Arthur Scherbius opatentował maszynę szyfrującą, nazwaną później Enigma. Planowanymi użytkownikami tej maszyny miały być głównie korporacje, wielkie firmy chcące chronić swoją korespondencję, poczty, oraz inne instytucje państwowe. Początkowo armia niemiecka nie była zbyt zainteresowana wprowadzeniem maszyn szyfrujących na miejsce powszechnego w tym czasie kodu ręcznego, jednakże plany remilitaryzacji Republiki Weimarskiej, a także odkrycie faktu, iż służby Królestwa Brytyjskiego regularnie czytały depesze niemieckie w czasie I wojny światowej spowodowały, że dowództwo niemieckie zdecydowało się na wprowadzenie kodu maszynowego, stanowiącego gwarancję zachowania bezpieczeństwa przekazywanych informacji.

Ulepszona wersja Enigmy po raz pierwszy pojawiła się na wyposażeniu niemieckiej armii w 1926 roku, najpierw w marynarce wojennej, a w dwa lata później w siłach lądowych. Była to cały czas zmieniona wersja odmiany cywilnej, którą można było wtenczas bez utrudnień nabyć na rynku. Przypuszcza się, iż celowo dowództwo armii niemieckiej, nabywając cywilną Enigmę i adaptując ją do potrzeb wojskowych, nie dążyło do wycofania jej z rynku, aby nie zwrócić uwagi służb specjalnych innych krajów jej nagłym zniknięciem.

Przełom w stopniu komplikacji maszyny nastąpił w 1930 roku, kiedy to dla potrzeb rozrastającej się Reichswehry opracowano nową, bardziej rozbudowaną wersję Enigmy, wzbogaconą o tzw. centralkę, która w niepomiaralny sposób zwiększała liczbę kombinacji szyfrów.

W kolejnych latach, podczas których Niemcy coraz intensywniej przygotowywały się do działań wojennych, maszyna szyfrująca Enigma przechodziła kilkakrotne modyfikacje, często bardzo znacznie zmniejszające szanse ewentualnego jej dekryptażu.

## **2. Biuro Szyfrów, jego pracownicy i ich pierwsze osiągnięcia.**

Krótko po odzyskaniu niepodległości, w formującej się armii polskiej zaistniała potrzeba zorganizowania komórki, której zadaniem byłoby przechwytywanie i czytanie meldunków armii sąsiadujących krajów. Właściwym człowiekiem do wykonania tego zadania okazał się 27-letni porucznik Jan Kowalewski, utalentowany inżynier, znający wiele języków obcych. Uformowane przez niego Biuro Szyfrów, działające w ramach tzw. Wydziału Drugiego, czyli wywiadu wojskowego, czekało potężne wyzwanie w postaci odradzających się w Niemczech ruchów narodowościowych i wzrostu znaczenia armii niemieckiej, a następcę Kowalewskiego, majora Franciszka Pokornego czekało trudne zadanie obserwowania zarówno wschodniego jak i zachodniego sąsiada. W tych warunkach stałego zagrożenia Kraju z obu stron, dalekowzroczna polityka

dowódców wojskowych, jak i bieżące potrzeby, zintensyfikowały prace nad przechwytywaniem i odczytywaniem meldunków polityczno-wojskowych obydwu sąsiadów. Z początku nie sprawiało to większego kłopotu: w okresie do 1926 roku, regularnie odczytywano kody niemieckie, jak również - tak samo nieskomplikowane w tym czasie - szyfry i kody sowieckie. Żadne państwo nie stosowało jednak dotychczas kodów maszynowych. Sytuacja uległa pogorszeniu w roku 1926, kiedy to niemiecka marynarka wojenna zaczęła stopniowo szyfrować meldunki maszynowo. W lipcu 1928 roku również meldunki niemieckich sił lądowych stały się dla polskich służb specjalnych nierozwiązalną zagadką. Słusznie przypuszczając, że ta dramatyczna zmiana łączyła się z wprowadzeniem maszyny szyfrującej tekst, zakupiono - dostępną na wolnym rynku w Niemczech - handlową wersję Enigmy. Po przewiezieniu maszyny do Kraju, intensywne jej oględziny i próby rozwiązania przechwyconych meldunków, prowadzone m.in. przez kapitana Maksymiliana Ciężkiego i porucznika Wiktora Michałowskiego, nie przyniosły żadnych pozytywnych rezultatów. Problem ten należało zaatakować z innej strony. W sytuacji tej, w styczniu 1929 roku, na zlecenie Sztabu Głównego Wojska Polskiego w Instytucie Matematyki Uniwersytetu Poznańskiego zorganizowano kurs kryptologii. Kurs ten, prowadzony przez majora Pokornego, kapitana Ciężkiego i inżyniera Antoniego Pallutha miał za zadanie wyłowić wyróżniających się w tym kierunku studentów matematyki. Podczas jednego z wieczornych zajęć, kapitan Ciężki dał adeptom kryptologii zadanie rozwiązania - rozwiązane już wcześniej przez niego samego - transpozycyjnego kodu niemieckiego. W ciągu kilku godzin trzech studentów: Marian Rejewski, Jerzy Różycki i Henryk Zygalski, prawidłowo odczytało ukryty tekst. Wyłowione w trakcie tego kursu talenty: ośmiu studentów, w tym dwóch z trzech najbardziej się wyróżniających, podjęli w zaadaptowanym pomieszczeniu Komendy Miasta w Poznaniu prace nad niemieckimi szyframi. Trzeci z uczestników kursu: Marian Rejewski opuścił zespół i udał się na Uniwersytet w Getyndze na specjalizację w statystyce matematycznej. Warunki ekonomiczne zmusiły go jednak do powrotu do Kraju i od jesieni 1930 roku i on dołączył do zespołu kryptologów. W początkowej fazie materiały do dekryptażu pochodziły głównie ze stacji nasłuchowej pod Poznaniem, chociaż często pracowano nad materiałami z innych stacji: w Warszawie, Starogardzie (Gdańskim) i Krzeszawicach pod Krakowem. Placówka Biura Szyfrów w Poznaniu, pomyślana jako tymczasowa, została rozwiązana, a trzem najbardziej wyróżniającym się: Rejewskiemu, który w tym czasie wykładał matematykę na Uniwersytecie Poznańskim, oraz świeżo upieczonym absolwentom tej uczelni: Różyckiemu i Zygalskiemu, zaproponowano stałą pracę w Biurze Szyfrów Sztabu Głównego Wojska Polskiego w Warszawie. Tym samym rozpoczął się nowy okres w boju z Enigmą.

### **3. Zastosowanie wyższej matematyki do rozwiązania szyfru.**

Pierwszy sukces grupa młodych kryptologów odniosła odczytując czteroliterowy kod niemieckiej marynarki wojennej, jakkolwiek cały czas droga do odczytywania meldunków szyfrowanych maszynowo, wydawała się bardzo daleka. Dostrzegając jednak ogromne możliwości tej grupy, szefowie Biura Szyfrów postanowili w takiej sytuacji sprawdzić kryptologów w najtrudniejszej walce. Najstarszemu z trójki: Marianowi

Rejewskiemu udostępniono zbierane w ostatnich latach szyfrowane maszynowo niemieckie meldunki i zlecono ich przeanalizowanie. Z pewnością nie liczone wtedy na szybkie rozwiązanie zagadki, jednak wierzone, że może istnieć jakaś trudno zauważalna własność, która pomogłaby w rozwiązaniu szyfru.

Rejewski, dysponujący handlową wersją Enigmy i depezbami niemieckimi, zauważył występowanie pewnych charakterystycznych cech, które ujął w postać układu równań permutacyjnych. I mimo, iż ilość niewiadomych wykluczała rozwiązanie równań, to sam fakt wykorzystania wyższej matematyki stał się pierwszym w tym czasie i przełomowym elementem w rozwiązywaniu problemów szyfrów maszynowych, czyniąc Rejewskiego "ojcem" nowoczesnych ataków kryptograficznych.

Widząc ogromne możliwości dalszych postępów w próbie rozwiązania szyfru Enigmy, nowy kierownik Biura Szyfrów: major Gwidon Langer, przekazał Rejewskiemu cztery dokumenty zdobyte przez wywiad francuski. Były to: zdjęcie wojskowej odmiany Enigmy, instrukcja obsługi Enigmy oraz dwie, nieaktualne od roku tabele kluczy. Jak obecnie stwierdzają historycy, informacje zawarte w tych dokumentach nie były wystarczające do odkrycia największej zagadki Enigmy: wewnętrznych połączeń wirników, jednak w znacznym stopniu pomogły Rejewskiemu w zlikwidowaniu kilku niewiadomych z równań permutacyjnych.

#### 4. Współpraca wywiadu francuskiego z polskim Biurem Szyfrów.

Warto w tym miejscu zatrzymać się na chwilę i wspomnieć o współpracy jaka występowała pomiędzy wywiadem francuskim i polskim. Otóż Gustave Bertrand, wówczas kapitan, szef Służby Wywiadowczej (*Service de Renseignements*) zauważając niezdolność francuskich służb kryptograficznych do rozwiązania szyfru maszynowego, nawiązał w 1931 roku kontakt z wywiadem polskim. Już podczas pierwszej swojej wizyty w Warszawie przekazał on wspomniane wyżej dokumenty Polakom. Dokumenty te, oraz kolejne materiały przekazywane w przyszłości, pochodziły od płatnego szpiega, noszącego pseudonim Ashe. Kim był ów tajemniczy informator wywiadu francuskiego? Ashe, czyli Hans-Thilo Schmidt, pochodzący z szacownej niemieckiej rodziny, pracował jako urzędnik w niemieckim Centrum Szyfrów (*Chiffrierstelle*), zajmując się niszczeniem zdezaktualizowanych tabeli kluczy. Za największy paradoks w historii wywiadu uznać można fakt, iż osoba, która przyjęła Hans-Thilo Schmidt do pracy na tym stanowisku, był jego rodzony brat: major Rudolf Schmidt, wówczas kierownik *Chiffrierstelle*. (Rudolf Schmidt, późniejszy generał, wydalony został z Armii po wykryciu działalności prowadzonej przez brata. Hans-Thilo skazany został na śmierć i stracony).

Ashe sprzedał wywiadowi francuskiemu wiele, mniej lub bardziej ważnych dokumentów, z których część przekazana została szefom polskiego Biura Szyfrów: Langerowi i Ciężkiemu. Jednakże - co okazuje się niezwykle zaskakujące - ŻADEN z późniejszych dokumentów nie został udostępniony Rejewskiemu i zespołowi kryptologów. Czym tłumaczyć fakt ukrycia posiadanych tabeli kluczy? Przypuszcza się, że strategia kierownictwa Biura wiązała się z potrzebą wyrobienia silnego zespołu kryptologów, który mógłby odnosić sukcesy z niemieckimi szyframi również w przypadku, gdyby nagle zabrakło materiałów wywiadowczych (w tym przypadku liczone się z nagłym

przerwaniem działalności Asche, jak i z możliwością zrezygnowania Francji ze współpracy z wywiadem polskim). W kontekście tych faktów tym bardziej znaczące stają się osiągnięcia Rejewskiego i reszty polskich kryptologów.

Największym osiągnięciem Rejewskiego było wydedukowanie połączeń wewnętrznych jednego z wirników Enigmy. Mimo tego jednak zagadka działania całej maszyny ciągle nie miała swego rozwiązania. W tym momencie można mówić o szczęściu polskiego zespołu kryptologów: jeden z dostarczonych przez wywiad francuski kluczy umożliwił odgadnięcie połączeń drugiego wirnika. Z niewielką trudnością znaleziono również i połączenia trzeciego wirnika. Tym samym - przy znajomości połączeń wewnętrznych wirników - możliwe stało się odczytywanie depeesz niemieckich.

## 5. Odczytywanie przez polskich kryptologów depeesz kodowanych Enigmą.

Od pierwszych dni stycznia 1933 roku Biuro Szyfrów było w stanie czytać niemal wszystkie depeesz niemieckie kodowane maszynowo. Polska była jedynym krajem na świecie, który w tym czasie posiadał taką możliwość. Szacuje się, że do grudnia 1938 roku odczytano kilka tysięcy meldunków kodowanych Enigmą.

W połowie grudnia 1938 roku Niemcy dodali do zestawu dwa dodatkowe wirniki (mimo, iż maszyna dalej używała tylko trzech wirników), co spowodowało, iż do rozwiązywania szyfru Polacy potrzebowali dziesięć razy więcej tzw. bomb. Bombami nazywano specjalnie zaprojektowane przez Jerzego Różyckiego i skonstruowane w warszawskich zakładach AVA, maszyny-cyklometry, które pracując równolegle znajdowały pierwotne położenie wirników. Wykonanie sześćdziesięciu *Bomb* przekraczało zarówno techniczne jak i finansowe możliwości Biura Szyfrów, tym bardziej, że równocześnie należałoby wykonać co najmniej 60 tzw. *placht Zygalskiego*, bardzo pracochłonnych w wykonaniu arkuszy perforowanych pomagających w ustaleniu kolejności wirników.

Można zadać sobie pytanie dlaczego inne kraje z wielkimi tradycjami zespołów kryptoanalitycznych, nie były w stanie rozwiązać zagadki Enigmy. Po sukcesach kryptologów francuskich w latach 1914-1918 i regularnym czytaniu kodów co najmniej dziesięciu krajów w latach dwudziestych, Francja nie była zainteresowana przyłączeniem do zespołów młodych matematyków, co - jak się okazało na przykładzie Rejewskiego i polskich kryptoanalityków - było warunkiem rozwiązania kodu maszynowego.

Anglia, również mimo posiadania wielkich tradycji, jak i takich językowych słów kryptoanalitycznych jak Dillwyn Knox, mimo wielkich wysiłków nie była w stanie złamać szyfrów Enigmy. W przypadku Wielkiej Brytanii istotny był jeszcze jeden czynnik: za największego wroga traktowano flotę japońską, nie zaś Niemcy i przez to wysiłki rozwiązania Enigmy nie uważano za priorytetowe.

Obok tego wszystkiego, brak wizji i silnej woli Francji i Wielkiej Brytanii spowodowały, że tylko Polska i polscy kryptoanalitycy byli w stanie wydrzeć tajemnicę Niemcom. Tak więc - bez pomocy Polski - dwa wielkie mocarstwa zaczynałyby wojnę bez żadnych możliwości czytania depeesz największego wroga i najsilniejszej armii świata.

## 6. Przekazanie rozwiązanej przez wywiad polski zagadki Enigmy wywiadowi Francji i Anglii.

Pomimo nieustannych udoskonaleń Enigmy polscy kryptolodzy nadążali z ustaleniem dokonywanych przez Niemców zmian. Niestety, polityczne uwarunkowania w Europie: zajęcie przez Niemców Austrii i Czechosłowacji i agresywne wypowiedzi Hitlera, nie wróżyły Polsce długiej przyszłości. Oczekując najgorszego, kierownictwo Biura Szyfrów zdecydowało się na zaaranżowanie spotkania z szefami wywiadów Francji i Wielkiej Brytanii. Do pierwszego spotkania doszło w styczniu 1939 w Paryżu, jednak dopiero podczas drugiego spotkania, które odbyło się w dniach 24-26 lipca 1939 roku w Warszawie, Polacy ujawnili aliantom mocno strzeżoną przez tyle lat tajemnicę rozwiązania zagadki Enigmy.

Na drugie trójstronne, lipcowe spotkanie przybyli ze strony francuskiej: Gustave Bertrand i kapitan Henri Braquenie, ze strony angielskiej: szef *Government Code and Cypher School* komandor Alistair Denniston, główny kryptolog Alfred D. Knox oraz specjalista nasłuchu radiowego, komandor Humphrey Sandwith. Przed odkryciem tajemnicy, goście zabawiali w restauracji Hotelu Bristol: szef Biura Szyfrów, Stefan Mayer, major Gwidon Langer i kapitan Ciężki oraz trzech kryptologów: Rejewski, Różycki i Zygalski. Po milej rozmowie (prowadzonej po niemiecku, gdyż był to jedyny język znany wszystkim trzem stronom) goście i gospodarze udali się do ośrodka w Pyrach gdzie w biurze kryptologów leżały na stole, przykryte materiałem, przygotowane przez Polaków maszyny. Gdy wszyscy zebrali się wokół stołu, major Langer bez słowa zdjął z maszyn pokrowce. Po chwili ciszy, która była wynikiem zaskoczenia i zadziwienia, generał Bertrand spytał pierwszy: "Skąd to wzięliście?" na co Langer odpowiedział: "Zrobiliśmy to sami." Na stole leżały kopie Enigmy, wykonane przez warszawską wytwornię AVA. Brytyjczycy zadawali najwięcej pytań, a Denniston chciał natychmiast dzwonić do Londynu, aby przysłano kreślarza i elektryka, którzy wykonaliby szkice maszyny. Major Langer miał jednak więcej do pokazania: goście przeszli do następnego pokoju, w którym zademonstrowano polskie wynalazki: *bomby* i *plachty Zygalskiego*. Francuscy i angielscy goście nie mieli słów uznania i podziękowania za ujawnienie tajemnicy, a Denniston ponownie chciał telefonować do Londynu. Zupełnie jednak nie uwierzył swym uszom, gdy usłyszał, że Polacy przygotowali gościom po jednej kopii Enigmy i komplet wszystkich materiałów. Był to pierwszy - acz nie ostatni - wkład Polaków w walkę przeciw wspólnemu wrogowi.

16 sierpnia Bertrand, wraz z brytyjskim kurierem dyplomatycznym, przewiózł jeden egzemplarz Enigmy z Paryża do Londynu, gdzie osobiście wręczył ją szefowi brytyjskiego wywiadu pułkownikowi Steward Menzies.

Za niecałe dwa tygodnie wojska niemieckie napadły na Polskę. Polskie Biuro Szyfrów i jego pracownicy ewakuowali się do Rumunii, skąd kryptolodzy przewiezieni zostali do Francji, gdzie ponownie zajęli się rozszyfrowywaniem Enigmy.

A w brytyjskim ośrodku dekryptażu Bletchley Park, największe głowy matematyczne, w tym genialny Alan Turing, korzystając z polskich odkryć mogły podjąć - jeszcze kilka dni temu beznadziejną - walkę kryptologiczną z Niemcami.

*Opracował: Lech Maziakowski*

Copyright ©1996-2000 Lech Maziakowski