Jak Polacy sprawili, że niemożliwe stało się możliwe

Sukces, który skrócił wojnę

Złamanie szyfru Enigmy było gigantycznym osiągnięciem polskiej kryptologii. Czas skuteczniej opowiedzieć tę historię światu.

dr Karol
Nawrocki
prezes Instytutu Pamięci Narodowej

Wczesnym rankiem 30 sierpnia 1942 roku z portu w Tarencie wyszedł włoski tankowiec „San Andrea". Zadanie było jasne: dostarczyć paliwo do Afryki Północnej, gdzie wojska Osi dowodzone przez niemieckiego feldmarszałka Erwina Rommla zaczynały właśnie kolejną ofensywę przeciwko Brytyjczykom. „San Andrea" nie dopłynęła do celu. Jeszcze tego samego dnia została zatopiona przez brytyjskie samoloty. Na początku września jej los podzielił inny włoski tankowiec „Picci Fassio".

Wściekły Rommel podejrzewał włoskich sojuszników o zdradę. Dziś wiadomo, że o ruchach statków wroga na Morzu Śródziemnym, ale też w innych miejscach działań wojennych Brytyjczycy byli informowani dzięki przechwyconym niemieckim depeszom. Szyfrowane przy pomocy słynnej Enigmy – maszyny, której kody uchodziły za niemożliwe do złamania – w tym czasie już od miesięcy były regularnie czytane przez kryptologów z ośrodka Bletchley Park pod Londynem. Historycy wojskowości są zdania, że skróciło to II wojnę światową nawet o kilka lat i uratowało życie milionów ludzi. Wielki udział w tym sukcesie mieli młodzi polscy matematycy.

Korzeni tej historii trzeba szukać w roku 1929, gdy na Uniwersytecie Poznańskim ruszył kurs kryptologii, zorganizowany przez Biuro Szyfrów Oddziału II Sztabu Głównego Wojska Polskiego, dla najzdolniejszych studentów. Trzej wyróżniający się kursanci – Marian Rejewski, Jerzy Różycki i Henryk Zygalski – znaleźli wkrótce zatrudnienie w Biurze Szyfrów: najpierw w jego poznańskiej ekspozyturze, a od września 1932 roku w warszawskiej centrali.

Po przeprowadzce do stolicy 27-letni Rejewski otrzymał nowe zlecenie: pracę nad złamaniem maszynowego szyfru Enigmy. Korzystając z matematycznej teorii permutacji, błyskawicznie poradził sobie z wyzwaniem, tak że jeszcze przed końcem 1932 roku możliwe stało się odczytanie pierwszych niemieckich depesz. „Był to niewątpliwie niemały sukces – wspominał po latach – zwłaszcza jeżeli weźmie się pod uwagę, że ani francuskie, ani angielskie biura szyfrów (...) pomimo długoletnich tradycji i doświadczeń w dziedzinie kryptologii i daleko większych niż polskie Biuro Szyfrów zasobów ludzkich i materialnych, nawet w roku 1938 jeszcze nie były w posiadaniu metody rozwiązania szyfru Enigma".

Lata 1932–1939 to „nieustanny pojedynek pomiędzy niemieckim i polskim biurem szyfrów, z którego stale wychodziliśmy zwycięsko" – jak zapamiętał Rejewski. Niemcy wciąż wprowadzali w swojej maszynie ulepszenia i zmieniali stosowane procedury. Polscy kryptolodzy nie pozostawali jednak w tyle, tworząc takie wynalazki jak zegar Różyckiego, płachta Zygalskiego, cyklometr i tzw. bomba Rejewskiego.

U progu wojny, w lipcu 1939 roku, Polacy podzielili się swoją wiedzą i sprzętem z Brytyjczykami i Francuzami. We wrześniu tego samego roku, w obliczu niemieckiej i sowieckiej agresji, zespół Biura Szyfrów ewakuował się na Zachód, gdzie dalej wspierał naszych sojuszników. Wiedza o wkładzie polskich kryptologów w złamanie szyfru Enigmy przez lata była nieznana, a i dziś jest za granicą słabo rozpowszechniona. Najwyższy czas opowiedzieć tę historię światu.

Klucz do Enigmy

TRZECH POLAKÓW PRZECIW MASZYNIE

Połączyły ich niesamowite, poparte doskonałym wykształceniem umiejętności matematyczne, praca dla polskiego wywiadu oraz trudy wojennej tułaczki. Znani są przede wszystkim z rozszyfrowania tajemnicy niemieckiej maszyny Enigma.

Witold
Sobócki
OBEN IPN W POZNANIU

Jako pierwszy z problemem Enigmy zetknął się, pochodzący z Bydgoszczy, Marian Rejewski. Praca nad chaotycznym ciągiem liter wymagała dyskrecji – na tyle posuniętej, że nawet koledzy z Biura Szyfrów nie mogli zostać wtajemniczeni.

Lider kryptologii

Rejewski przeanalizował ogromną liczbę depesz, a także pochodzące od francuskiego wywiadu fotokopie instrukcji Enigmy i nieaktualne zestawy początkowych ustawień maszyny. Genialnemu matematykowi udało się odnaleźć pewne prawidłowości. Pierwszych sześć znaków każdej depeszy było podwójnie zaszyfrowanym kluczem indywidualnie nadawanym do każdej wiadomości. Zabieg ten miał jeszcze bardziej utrudnić potencjalny atak na szyfr, jednak dzięki geniuszowi Rejewskiego udało się go wykorzystać przeciwko użytkownikom maszyny. Matematyk zauważył cykliczność klucza, dającą się matematycznie opisać za pomocą teorii permutacji. Sukces ten, połączony z trafną intuicją, pozwolił na ustalenie matematycznego modelu elementów Enigmy, odpowiedzialnych za kolejne przekształcenia szyfru: okablowania wirników, łącznicy, walca wejściowego i odwracającego. Wreszcie w grudniu 1932 r. Marian Rejewski skutecznie odczytał pierwszy szyfrogram.

Do prac włączono pozostałą dwójkę matematyków: Jerzego Różyckiego i Henryka Zygalskiego. Wkrótce potem powstało jedno z największych osiągnięć polskiej myśli naukowo-technicznej – za pomocą matematycznej rekonstrukcji maszyny udało się wykonać jej kopię. Sukces ten jest wart docenienia, tym bardziej że zarówno matematycy, jak i związani z polskim wywiadem inżynierowie z firmy radiotechnicznej AVA nigdy nie widzieli wojskowej Enigmy czy poszczególnych jej elementów.

Model wojskowej Enigmy wyposażonej w trzy wirniki i łącznicę. Fot. Domena publiczna

Wydawałoby się, że historia mogłaby się tu zakończyć, jednak możliwości komplikacji szyfru Enigmy powodowały, że problem sprawnego odczytywania niemieckich depesz dopiero zaczął nabierać rumieńców. Metoda Rejewskiego była pracochłonna, należało ją zatem udoskonalić.

Zegar z Kresów i płachty z Poznania

Zespół kryptologów postanowił skupić się na automatyzacji pracy. Powstał cyklometr – dzięki niemu stworzono katalog charakterystyk możliwych cykli. O ogromie pracy zespołu włożonego w opracowanie tego wykazu świadczy fakt, że mimo wspierania się maszyną, katalog powstawał niemal rok.

Praca nad sprawnym dekryptażem wymagała wciąż opracowywania nowych metod. Urodzony w roku 1909 na Kresach najmłodszy z całej grupy – Jerzy Różycki – sformułował „metodę zegara", która pozwoliła na odnalezienie tzw. szybkiego wirnika maszyny. Uczestniczył też w dalszych pracach kryptologicznych, Enigmą zajmował się do końca życia – w 1942 r. zginął w wyniku zatonięcia statku pasażerskiego „Lamoriciére" na Morzu Śródziemnym.

Pochodzący z Poznania Henryk Zygalski z kolei wynalazł nowatorski system odnajdywania pozycji startowej i kolejności wirników Enigmy. Składał się z on z zestawu płacht, które nakładane na siebie w odpowiedni sposób eliminowały fałszywe rozwiązania.

Najbardziej zaawansowanym narzędziem, usprawniającym prace polskiego zespołu, była bomba kryptologiczna, zwana od nazwiska pomysłodawcy „bombą Rejewskiego". Historia pochodzenia nazwy tego urządzenia ma dwie anegdotyczne wersje: w pierwszej nawiązuje do bomby – ulubionego deseru Mariana Rejewskiego, a drugiej zaś słowo

INSTYTUT PAMIĘCI NARODOWEJ

Jerzy Różycki – matematyk, Marian Rejewski – matematyk, lider trójki poznańskich kryptologów, Henryk Zygalski – matmatyk. Fot. Domena publiczna

„bomba" wynikało ze specyficznego tykania maszyny podczas pracy, przypominającej odgłos bomby zegarowej.

Rywalizacja intelektów

Stworzenie polskiej kopii Enigmy, cyklometru oraz bomby kryptologicznej było przełomem w kryptologii. Po raz pierwszy w dziejach do łamania szyfrów wykorzystano skomplikowane metody matematyczne, których rezultatem było wykorzystanie maszyny przeciwko innej maszynie.

W miarę zbliżania się II wojny światowej Niemcy coraz częściej modyfikowali Enigmę, jak też sposoby jej używania. Pomiędzy Niemcami a Polakami trwał swojego rodzaju wyścig intelektualny, którego rezultatem były opisane wyżej metody i urządzenia. Matematycy dotrzymywali kroku niemieckim oficerom, jednak dystans zaczął się niebezpiecznie zwiększać. Nie wynikał on z braków intelektualnych absolwentów Uniwersytetu Poznańskiego, raczej ze spraw bardziej prozaicznych – stworzenie kolejnych egzemplarzy bomb i płacht przewyższało możliwości finansowe Biura Szyfrów. Postanowiono wreszcie podzielić się osiągnięciami z zaprzyjaźnionymi brytyjskimi oraz francuskimi służbami wywiadowczymi. W lipcu 1939 roku doszło do spotkania w ośrodku kryptologicznym w Pyrach pod Warszawą, podczas którego Polacy przekazali swoim kolegom z Francji i Wysp Brytyjskich wiedzę o Enigmie, metody jej dekryptażu, a także kopie płacht Zygalskiego oraz zrekonstruowane egzemplarze Enigmy.

Przekazanie tajemnicy

Po wybuchu II wojny światowej kryptolodzy trafili do Francji, gdzie pracowali w ośrodku P.C Bruno w Gretz-Armainvilliers. Po kapitulacji Francji latem 1940 r. przenieśli się na południe kraju i kontynuowali pracę nad niemieckimi szyframi w ośrodku Cadix. Wobec groźby zdekonspirowania tego miejsca Rejewski i Zygalski przedostali się do Wielkiej Brytanii, po drodze trafiając do hiszpańskiego więzienia.

Po raz pierwszy w dziejach do łamania szyfrów wykorzystano skomplikowane metody matematyczne, których rezultatem było wykorzystanie maszyny przeciwko innej maszynie.

Tymczasem od spotkania w Pyrach Brytyjczycy zaczęli pracę nad stworzeniem własnego ośrodka kryptologicznego. Wybór padł na posiadłość Bletchley Park, położoną na północ od Londynu. Tam, korzystając z dokonań Polaków, doskonalono pracę nad Enigmą i innymi maszynami szyfrującymi. Miejsce to stało się wywiadowczym mózgiem aliantów, zatrudniającym w szczytowym momencie 10 tys. osób. Żadna z większych operacji alianckich nie mogła zakończyć się powodzeniem, gdyby nie dane poznane dzięki łamaniu niemieckich depesz. Wgląd w zamierzenia III Rzeszy m.in. uratował Brytyjczyków podczas bitwy o Wielką Brytanię, pomógł rozprawić się z U-Bootami podczas walk na Atlantyku, a także doskonale przygotował sprzymierzonych do lądowania w Normandii. Niektórzy historycy podkreślają, że złamanie Enigmy skróciło o kilka lat II wojnę światową. Z Bletchley Park pochodziły koncepcje stworzenia używanego dziś powszechnie komputera. Polacy nie zostali dopuszczeni do prac w tym ośrodku. Marian Rejewski po wojnie powrócił do Polski, dopiero w 1967 roku ujawnił swoje dokonania w spisanych wspomnieniach. Henryk Zygalski z kolei pozostał w Wielkiej Brytanii, gdzie kontynuował karierę matematyczną. ■

Oficerowie Biura Szyfrów. Lata 20. XX wieku Od lewej: Jakub Plezia, Jerzy Suryn, Paweł Misiurewicz, Franciszek Pokorny, Maksymilian Ciężki. W środku Yamawaki Masataka, japoński attaché, porucznik Cesarskiej Marynarki Japonii. Fot. Domena publiczna

Nie tylko matematycy...

BIURO SZYFRÓW PRZEJMUJE INICJATYWĘ

Gdy mówimy o wielkim sukcesie, jakim było rozpracowanie maszyny szyfrującej Enigma, pierwsze przychodzą na myśl trzy nazwiska: Mariana Rejewskiego, Henryka Zygalskiego oraz Jerzego Różyckiego. Warto sobie jednak uświadomić, że genialni polscy matematycy nie działali w próżni; zaangażowanie ich do prac kryptologicznych było zasługą oficerów polskiego wywiadu, którzy współpracowali z władzami Uniwersytetu Poznańskiego.

Witold
Sobócki
OBEN IPN W POZNANIU

Korzeni Biura Szyfrów, polskiej komórki wywiadowczej zajmującej się kryptologią, należy szukać w lecie 1919 roku. Ówczesny polski radiowywiad zdążył już zorganizować sieć nasłuchową przejmującą depesze sowieckie. Samo ich przechwycenie nie gwarantowało sukcesu – te najważniejsze były wszak szyfrowane.

Egdar Alan Poe, grzebień i polski wywiad

Przełom przyszedł niespodziewanie: podczas jednego z nocnych dyżurów w Sztabie Generalnym porucznikowi Janowi Kowalewskiemu udało się złamać pierwszy z sowieckich szyfrów. Bohater tej historii nie był zawodowym kryptologiem, w celu odczytania depesz oparł się z jednej strony na lekturze opowiadania „Złoty Żuk" Edgara Alana Poe, a z drugiej, za pomocą grzebienia z odpowiednio wyłamanymi zębami udało mu się zidentyfikować literę „i" w rosyjskim słowie „dywizja". Stąd była już krótka droga do poznania klucza szyfru. Kowalewskiemu powierzono stworzenie pierwszej polskiej komórki zajmującej się kryptoanalizą: Wydziału II Radiowywiadu Biura Szyfrów.

Jeszcze podczas wojny polsko-bolszewickiej do łamania kolejnych szyfrów zaangażowano także matematyków, późniejszych profesorów: Stanisława Leśniewskiego, Stefana Mazurkiewicza oraz Wacława Sierpińskiego. Naukowcy umiejętnie łączyli metody matematyczne z lingwistycznymi. „Cud nad Wisłą" stał się dzięki pracy kryptologów cudem realnym – wgląd w tajną, sowiecką korespondencję walnie przyczynił się do zwycięskiej rozprawy z najeźdźcą.

Problem Enigmy

Od drugiej połowy lat 20. XX wieku polski radiowywiad przechwytujący depesze niemieckie natrafiał na wiadomości przesyłane nowym szyfrem. Wkrótce okazało się, że siły zbrojne Republiki Weimarskiej wprowadziły

do użytku maszynę szyfrującą Enigma. Polakom znana była budowa handlowej wersji tej maszyny, jednak jej militarny odpowiednik był znacznie zmodyfikowany. Szyfr Enigmy wojskowej uważany był za niepokonany, teoretyczna liczba możliwych kombinacji była większa od liczby atomów w widzialnym wszechświecie. Na arenę musiały wejść zaawansowane metody matematyczne.

Dlaczego Poznań?

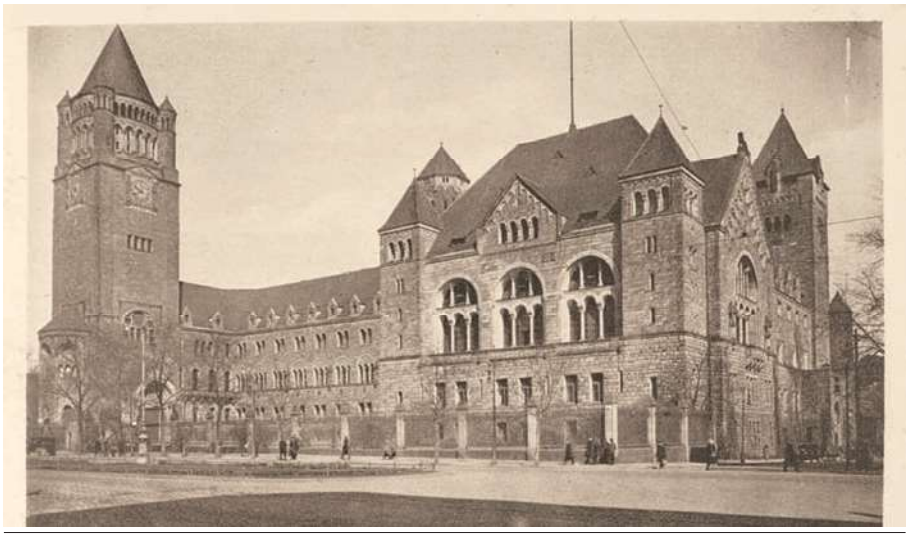
Stając przed problemem Enigmy oficerowie polskiego wywiadu uciekali się do niestandardowych metod: szyfrem tym bezskutecznie zajmował się znany międzywojenny jasnowidz inż. Stefan Ossowiecki. Powrócono do pomysłu wykorzystania kadry naukowej Uniwersytetu Warszawskiego. Okazało się jednak, że dawni kryptolodzy, zasłużeni w wojnie polsko-bolszewickiej, nie radzą sobie z niemieckimi depeszami szyfrowanymi nawet bez użycia Enigmy. Porucznik Maksymilian Ciężki, szef Sekcji Niemieckiej Biura Szyfrów, weteran powstania wielkopolskiego, zaproponował zorganizowanie kursu kryptologicznego dla najzdolniejszych studentów matematyki Uniwersytetu Poznańskiego. Za lokalizacją kursu w stolicy Wielkopolski przemawiało kilka czynników, m.in. ten, że Uniwersytet był wówczas młodą placówką, ze świeżym podejściem do rozwiązywania naukowych problemów, a w poznańskiej cytadeli znajdowała się radiostacja bezpośrednio nasłuchująca niemiecki ruch radiowy. Nie bez znaczenia było również to, że przyszły kryptolog zajmujący się Enigmą musiał, oprócz matematycznych zdolności, doskonale znać język niemiecki, wręcz umieć myśleć w tym języku. Więc gdzie jeśli nie w Poznaniu można było spotkać studentów z biegłą znajomością tego języka? Ale być może decydował lokalny patriotyzm pracowników Biura Szyfrów – oprócz Ciężkiego w biurze tym pracowało jeszcze dwóch innych Wielkopolan: Antoni Palluth oraz Wiktor Michałowski. Wszystkie te argumenty przekonały ich przełożonego, majora Franciszka Pokornego do postawienia karty na stolicę Wielkopolski.

Kurs kryptologiczny

Na początku roku 1929 r. oficerowie Biura Szyfrów skontaktowali się z profesorem Zdzisławem Krygowskim, szefem Katedry Matematyki na Wydziale Matematyczno-Przyrodniczym Uniwersytetu Poznańskiego. Profesor wytypował 26 najzdolniejszych studentów, którzy wzięli udział w kilkumiesięcznych zajęciach o tematyce kryptologicznej. Zajęcia prowadzone przez oficerów Biura Szyfrów odbywały się poza godzinami zajęć uniwersyteckich – najpierw w poznańskim Zamku Cesarskim, ówczesnej siedzibie Wydziału Matematyczno-Przyrodniczego, a następnie poznańskiej Cytadeli. Kursanci poznawali podstawy kryptologii, stopniowo wtajemniczano ich w coraz trudniejsze techniki łamania szyfrów. Trójkę najlepszych: Mariana Rejewskiego, Henryka Zygalskiego oraz Jerzego Różyckiego zatrudniono w Ekspozyturze Biura Szyfrów. Komórka ta była zorganizowana w budynku Intendentury Wojskowej, mieszczącej się po drugiej stronie ulicy Wały Kościuszki, naprzeciw poznańskiego Zamku. Absolwenci kursu mogli więc dyskretnie połączyć pracę na uniwersytecie z zadaniami stawianymi przez polski wywiad.

Wkrótce po zakończeniu kursu przygodę z szyframi na rok zawiesił Marian Rejewski. Planując jeszcze karierę statystyka w branży ubezpieczeniowej, udał się on na wymarzony staż do Getyngi. Ówczesna „mekka matematyki" bardzo mocno go rozczarowała. Niepocieszony powrócił do Poznania, gdzie przypomniał sobie o kolegach – kryptologach i dołączył do pracowników Biura Szyfrów. Niedługo potem Ekspozyturę przeniesiono do Warszawy. Zespół odniósł pierwszy sukces – złamano kod niemieckiej marynarki. Następnie, najpierw Marianowi Rejewskiemu, a potem pozostałej dwójce wyznaczono najważniejsze zadanie: rozpracowanie szyfru Enigmy. ■

Pałac Saski w Warszawie. W gmachu tym do 1937 r. mieściła się siedziba Biura Szyfrów. Fot. NAC



Zamek Cesarski w Poznaniu, w okresie międzywojennym w budynku tym mieściła się Katedra Matematyki. Fot. Polona