



Służba w cieniu dla Polski

Elektromechaniczna maszyna szyfrująca, wykorzystująca zarówno właściwości prądu elektrycznego, jak i elementy mechaniczne do szyfrowania polialfabetycznego. Jej najważniejszymi elementami były obracające się na jednej osi wirniki szyfrujące.

Decydujące znaczenia dla powstania Enigmy miało zakupienie w 1928 r. przez Artura Scherbiusa - niemieckiego inżyniera, konstruktora, współzałożyciela wytwórni urządzeń elektrotechnicznych - Scherbius & Ritterwas - własnej wirnikowej maszyny szyfrującej i praw patentowych do innej wirnikowej maszyny szyfrującej, opracowanej dziewięć lat wcześniej przez holenderskiego inżyniera Hugona Kocha. Transakcja ta zrewolucjonizowała rynek sprzętu szyfrującego oraz samą kryptologię. Enigma bardzo szybko zyskała uznanie nabywców, co zaowocowało licznymi zamówieniami i trafiła do masowej produkcji.

Sukces komercyjny oraz skuteczność Enigmy - wykorzystywanej wówczas głównie do szyfrowania niemieckiej korespondencji handlowej - sprawiły, że zainteresowały się nią również niemieckie wojsko oraz służby wywiadowcze, które po bolesnej porażce w czasie I wojny światowej pracowały nad stworzeniem idealnego urządzenia szyfrującego. Po zmodyfikowaniu jej konstrukcji i zasad działania instytucje te wprowadziły ją do użytku w swojej łączności szyfrowej. Od tego momentu kraje sąsiadujące utraciły możliwość rozszyfrowywania niemieckich komunikatów.

Brytyjscy i francuscy kryptolodzy wielokrotnie starali się złamać niemiecki kod, jednak ich wysiłki za każdym razem kończyły się fiaskiem. Zrażeni ciągłymi niepowodzeniami ostatecznie zaprzestali dalszych prób, uznając Enigmę za maszynę niemożliwą do rozpracowania.

Początek prac nad złamaniem niemieckich szyfrów

Polaków, w odróżnieniu od innych nacji, obawy przed ekspansywną polityką Niemiec, motywowały do pracy nad systemem szyfrowym tego państwa oraz przede wszystkim napełniały wiarą w to, że dzięki pomysłowości, inteligencji i wysiłkowi złamanie wykorzystywanego w nim klucza jest możliwe. Przez stulecia powszechne było przekonanie, że najlepszymi specjalistami w tym zakresie są językoznawcy i osoby z predyspozycjami lingwistycznymi. Ekspert z Polski postanowili jednak zastosować niestandardowe metody pracy oparte na wiedzy i zdolnościach matematycznych wybranych absolwentów polskich uczelni znających język niemiecki. Na początku 1929 r. wywiad II RP, poszukujący utalentowanych kandydatów na tajny kurs kryptologiczny, zwrócił się do wykładowcy Instytutu Matematyki Uniwersytetu Poznańskiego profesora Zdzisława Krygowskiego z prośbą o pomoc w ich wytypowaniu (nieprzypadkowo wybrano uczelnię w zaborze pruskim, gdzie powszechna była znajomość języka niemieckiego). Wskazani przez niego studenci - 20 matematyków - uczestniczyli w zajęciach prowadzonych przez mjr. Franciszka Pokornego, por. Maksymiliana Ciężkiego i inżyniera Antoniego Pallutha.

Z tej grupy tylko trzech matematyków zostało zaangażowanych przez Biuro Szyfrów Oddziału II Sztabu Głównego Wojska Polskiego. Najbardziej utalentowanym naukowcem był Marian Rejewski - niewysoki, skromny i rozważny młodzieniec, określany przez przyjaciół jako „nieśmiały okularnik”. Dwaj pozostali to jego uniwersyteccy koledzy - Henryk Zygalski i Jerzy Różycki. W tym samym czasie z Wilna do Warszawy przybył Gwido Langer, pasjonat nowoczesnej techniki. Najpierw objął on posadę kierownika komórki zajmującej się radiowywiadem, a następnie szefa Biura Szyfrów, które przekształcił w świetnie działającą strukturę. Za jego sprawą ważną rolę w działalności sekcji niemieckiej Biura odegrał A. Palluth, który zakupił cywilny egzemplarz Enigmy umożliwiający badania nad urządzeniem.

Zdjęcia przedstawiają egzemplarz Enigmy używanej podczas II wojny światowej. Urządzenie obecnie znajduje się obecnie w posiadaniu Agencji Wywiadu.

Pierwsze sukcesy polskich kryptologów

Zasadnicze znaczenie w pracach nad Enigmą miała bliska współpraca pomiędzy polskim i francuskim wywiadem. Francuzi przekazywali Warszawie kopie materiałów dotyczących militarnej wersji Enigmy otrzymywanych od pracującego dla nich niemieckiego szyfranta Hansa Thilo Schmidta. W zamian Polacy mieli dzielić się z Paryżem ewentualnymi efektami wykorzystania dostarczonych informacji. Dane te pozwoliły im skonstruować wierną kopię urządzenia. Nadal było to jednak za mało, by odczytywać niemieckie wiadomości. W końcu, dzięki materiałom przywiezionym do Warszawy 8 grudnia 1932 r. przez kpt. Gustava Bertranda, odpowiednika Gwidona Langerę w wywiadzie Francji, polskim kryptologom 31 grudnia 1932 r. w Pałacu Saskim w Warszawie, gdzie mieściła się wówczas siedziba Biura Szyfrów, po raz pierwszy udało się rozkodować szyfrogramy zaszyfrowane za pomocą Enigmy. Sukces przyszedł w samą porę, gdyż w Niemczech na początku 1933 r. zaszły zmiany polityczne, w wyniku których władzę uzyskał Adolf Hitler. W tym kontekście usprawnienie i zwiększenie efektywności prac kryptologów z sekcji niemieckiej, dysponujących tylko jednym egzemplarzem zrekonstruowanej Enigmy,

nabrało szczególnego znaczenia. Z tego powodu Oddział II Sztabu Głównego zlecił Wytwórni Radiotechnicznej AVA z Warszawy, kierowanej przez Leonarda i Ludomira Danielewiczów oraz Edwarda Fokczyńskiego i Antoniego Pallutha (pasjonaci krótkofalarstwa), opracowanie kolejnych modeli tego urządzenia. Powstało kilkanaście kopii Enigmy, z których Biuro Szyfrów korzystało już w 1934 r.

Rozwój techniki dekryptażu

Niemcy systematycznie modyfikowali konstrukcję i zasady działania Enigmy, na co polscy kryptolodzy za każdym razem odpowiadali kolejnymi nowatorskimi i skutecznymi sposobami łamania jej kodu i odczytywania zaszyfrowanych za jej pomocą depeesz. Jednym z efektów ich pracy było skonstruowanie w 1936 r. przyrządu nazwanego cyklometrem, który pozwalał na ustalenie aktualnego kodu Enigmy w ciągu kilkunastu minut. Z kolei, gdy we wrześniu 1938 r. niemieccy specjaliści wprowadzili następane innowacje w budowie i działaniu maszyny szyfrującej, M.Rejewski wspólnie z kolegami stworzył urządzenie - nazwane bombą Rejewskiego, pozwalające na automatyczne łamanie jej kodów. Jego unikatowość polegała również na wykorzystywaniu wyjątkowych koncepcji matematycznych takich jak np. teoria cykli. W ustaleniu kolejności wirników kodujących Enigmy pomagały opracowane przez H.Zygalskiego perforowane papierowe arkusze zwane płachtami Zygalskiego.

W przeddzień wybuchu II Wojny Światowej

W dniach 25-27 lipca 1939 r. w Warszawie odbyło się drugie spotkanie z przedstawicielami francuskiego i brytyjskiego wywiadu.

Pierwsza narada miała miejsce w styczniu 1939 roku w Paryżu i dotyczyła możliwości złamania szyfru Enigmy. Ustalono wtedy, że kolejna odbędzie się, jeżeli któraś ze stron spotkania będzie posiadała nowe informacje

na temat maszyny szyfrującej. Nikt spośród rozmówców reprezentujących wówczas stronę polską nie poinformował, że Polacy czytają niemieckie depesze szyfrowane Enigmą już od 6 lat. Jednak w okresie od stycznia do lipca 1939 roku sytuacja w Europie na tyle się zmieniła, że Polska strona zdecydowała, o konieczności podzielenia się tajemnicą z aliantami oraz o przekazaniu po jednej kopii Enigmy oraz kompletu płacht Zygałskiego oraz bomb Rejewskiego.

Podczas drugiego spotkania w lipcu w 1939 roku, stronę francuską reprezentował mjr Gustave Bertrand i kpt. Henri Braquenié, natomiast angielski wywiad - m.in. szef Rządowej Szkoły Kodów i Szyfrów w Bletchley Park kmdr Alistair Denniston, czołowy brytyjski kryptolog Alfred Dillwyn „Dilly” Knox oraz specjalista nasłuchu radiowego prof. Humphrey Sandwich.

Przedstawiciele francuskiego i brytyjskiego wywiadu 25 lipca 1939 r. zostali zaproszeni do ośrodka dekryptażu w Pyrach. Na gości czekały wykonane przez warszawską wytwórnię AVA urządzenia do dekryptażu szyfru Enigmy. Podczas wizyty sojusznicy zostali zapoznani ze sposobami uzyskiwania kluczy do maszyn szyfrujących. Podpułkownik G.Langer pokazał gościom, jak wykonać deszyfraz tajnej niemieckiej depeszy wysłanej z dowództwa SS. Tego dnia Polacy ujawnili aliantom strzeżoną przez wiele lat tajemnicę i przekazali im po jednej kopii Enigmy oraz materiały potrzebne do obsługi maszyny. Po zapoznaniu się z rezultatami działań polskich kryptologów, Brytyjczycy i Francuzi byli zdumieni nieosiągalnym wówczas dla nich – poziomem zaawansowania prac. Maszyny zostały wysłane do adresatów drogą morską, która w tym czasie uznawana była za najbezpieczniejszą opcję. Na bazie uzyskanych od Polaków informacji Brytyjczycy niezwłocznie przystąpili do tworzenia struktury kryptologicznej w Bletchley Park. Już w sierpniu 1939 r. zaczęli tam przybywać naukowcy, by rozpocząć prace nad niemieckim systemem szyfrowania. Wśród nich był również Alan Turing, genialny matematyk, który zajmował się tworzeniem własnych sposobów deszyfracji. Kryptolodzy z Bletchley Park z czasem zdobyli prawie całkowitą kontrolę nad niemieckimi szyframi, odszyfrowując depesze wszystkich rodzajów niemieckich wojsk i czytając je często szybciej niż ich adresat.

J. Garliński, *Enigma. Tajemnica drugiej wojny światowej*, Londyn 1980.

B. Johnson, *Sekrety drugiej wojny światowej. Wojna mózgów. Tajne badania naukowe i ich zastosowanie w czasie drugiej wojny światowej*, przeł. M. Wasilewski, Poznań 1997.

W. Kozaczuk, *W kręgu Enigmy*, Warszawa 1979.

M. Rejewski 1905-1980. *Życie Enigmą pisane*, red. S. Ciechanowski et. al., Bydgoszcz 2005.

Literatura uzupełniająca

M. Baldwin, *Wprowadzenie do ENIGMY. Wykład wygłoszony z okazji 65. rocznicy spotkania kryptologów polskich i alianckich w Lesie Kabackim (Pyry, koło Warszawy), 1939*; wykład przeł. i wstępem zaopatrzył Zdzisław J. Kapera, Kraków-Mogilany 2004.

M. Grajek, *Odnaleziony raport - czego nowego dowiedzieliśmy się o historii złamania Enigmy?*, [w:] *Enigma bez tajemnic. 85. rocznica sukcesu polskich kryptologów*, red. tenże, Toruń 2020, s. 41-57.

Z.J. Kapera, *Stan badań nad polską Enigmą 1932-1942*, [w:] *Wkład polskiego wywiadu w zwycięstwo aliantów w II wojnie światowej. Akta konferencji naukowej zorganizowanej w Krakowie w dn. 20-22.10.2002 r. przez Polską Akademię Umiejętności, Muzeum Armii Krajowej, Towarzystwo Obrony Zachodnich Kresów Polski i Instytut Historii Uniwersytetu Jagiellońskiego*, red. tenże, Kraków 2004, s. 13-26.

M. Rejewski, *Jak matematycy polscy rozszyfrowali Enigmę*, „Wiadomości Matematyczne” R.XXIII 1980, s. 1-28

M. Rejewski, *Wspomnienia z mej pracy w Biurze Szyfrów Oddziału II Sztabu Głównego 1930-1945*, Poznań 2013.

Sztafeta Enigmy. Odnaleziony raport polskich kryptologów, redakcja, opracowanie i tłumaczenie tekstów M. Grajek, Warszawa 2019.