80 lat temu polscy matematycy złamali niemiecką „Enigmę”

informacja.pl 31 grudnia 2012 r.

Międzysojusznicza operacja Enigma, znana również pod nazwą Ultra, była największą tajemnicą II wojny światowej po bombie atomowej. Uzyskana przez aliantów możliwość stałego, regularnego czytania setek tysięcy tajnych dyrektyw, rozkazów, raportów i innych szyfrowanych depesz sił zbrojnych III Rzeszy oraz jej sprzymierzeńców - zarówno z sieci radiowych szczebla strategicznego z kwaterą główną Hitlera włącznie, jak i dowództw operacyjnych i taktycznych Wehrmachtu, a także SS, SD, dyplomacji, kolejnictwa i innych resortów - była wielkim atutem w rękach państw sprzymierzonych.
Na podstawie badań i studiów prowadzonych od kilkunastu lat w wielu krajach, historycy są coraz bardziej skłonni przypisywać Enigmie - Ultrze rolę języczka u wagi w przechyleniu szali zwycięstwa na stronę przeciwników bloku państw faszystowskich w latach światowego konfliktu. Bez przesady można powiedzieć, że przez ogromny wkład do pokonania hitlerowskiego imperium tyranii Enigma, jako najwydajniejsze sojusznicze źródło informacji o przeciwniku wiatach 1939 - 1945, znacząco współkształtowała przyszłe oblicze świata. Jednak w przeciwieństwie do tajemnicy energii jądrowej, która ujawniła się w całopalnych stosach Hiroszimy i Nagasaki w sierpniu 1945 roku, u schyłku wojny na Dalekim Wschodzie, tajemnice Enigmy - podług greckiej etymologii właśnie tajemnicy, zagadki - miały jeszcze blisko trzydzieści lat przeleżeć w najtajniejszych wojennych sejfach.

W styczniu 1929 roku Biuro Szyfrów Sztabu Głównego Wojska Polskiego, kierowane w tym czasie przez majora Franciszka Pokornegodo do intelektualnej walki z niemiecką służbą kryptologiczną (Chi-Dienst) postanowiono wprząc matematykę. Na zapotrzebowanie Sztabu Głównego, dyrektor Instytutu Matematyki Uniwersytetu Poznańskiego prof. Zdzisław Krygówski sporządził listę studentów trzeciego i czwartego roku władających biegle niemieckim i mających dobre oceny. Wybranych dwudziestu kilku studentów wzięło udział w kursie kryptologii, prowadzonym przez oficerów i cywilnych kryptologów Sztabu Głównego (mjr Pokorny, kpt Maksymilian Ciężki, inż. Antoni Palluth).
Kurs szyfrowy w Poznaniu miał na celu znalezienie nowych talentów kryptologicznych i wzmocnienie polskiego wywiadu radiowego, walczącego z trudnym niemieckim przeciwnikiem. Zajęcia odbywały się wieczorami, kilka razy w tygodniu. Niektórzy z uczestników zrezygnowali, dochodząc do wniosku, że nie mają odpowiednich uzdolnień, zwłaszcza że nie stosowano wobec nich taryfy ulgowej i wymagano zdawania egzaminów razem z innymi studentami.
Trzej wyróżniający się słuchacze kursu: Marian Rejewski, Jerzy Różycki i Henryk Zygalski, jak też kilku innych adeptów kryptologii, potrafili pogodzić poznawanie szyfrów z normalnymi zajęciami uniwersyteckimi.

Pierwszym liczącym się sukcesem młodych matematyków - kryptologów, który upewnił kierowników Biura Szyfrów o trafności wyboru i celowości poprzedzających go paroletnich wysiłków, było samodzielne rozwiązanie przez nich czteroliterowego kodu niemieckiego marynarki wojennej.

Praca Rejewskiego nad materiałami z nasłuchu wojskowej Enigmy, której prostszy, "cywilny" model, zakupiony w Niemczech, został mu dostarczony, pozwoliły rozpoznać niektóre charakterystyczne cechy systemu. Rejewski zwrócił w szczególności uwagę na układ "kluczy" pierwszych kilku grup depesz szyfrowych. Zarysował się pewien ogólniejszy plan, strategia, która mogła prowadzić do wykrycia wewnętrznych połączeń urządzenia, co z kolei umożliwiłoby jego rekonstrukcję. Hipotezom swym Rejewski nadał postać układu równań permutacyjnych, w których wszakże liczba niewiadomych była zbyt wielka, aby można było uzyskać rozwiązanie.

Po niespełna dwóch miesiącach od chwili rozpoczęcia pracy nad Enigmą, na początku grudnia 1932 roku, Rejewski otrzymał od kierownika Biura Szyfrów, majora Gwidona Langera, cztery dokumenty dotyczące niemieckich szyfrów, a wśród nich ogólny zewnętrzny opis i rysunek wojskowej odmiany Enigmy oraz dwie już nieaktualne, pochodzące sprzed roku tabele kluczy. Dokumenty te, według zgodnych późniejszych ocen, nie umożliwiały odkrycia najważniejszych tajemnic Enigmy, a zwłaszcza ustalenia jej połączeń wewnętrznych. Jednak dla Rejewskiego okazały się bezcennym nabytkiem. W posiadanym już układzie równań eliminowały część niewiadomych, inne zaś czyniły bardziej podatnymi na ich usunięcie za pomocą operacji logicznych, wykorzystujących omyłki popełniane przez niemieckich szyfrantów Enigm.

Rozwiązanie przez Rejewsklego Enigmy, odtworzenie jej wszystkich połączeń wewnętrznych, zostało ostatecznie dokonane w ostatnich dniach grudnia 1932 roku, a praktycznie zastosowane, z udziałem włączonych już do tych prac Henryka Zygalskiego i Jerzego Różyckiego, w pierwszej dekadzie stycznia 1933 roku, kiedy od początku do końca odczytano najnowsze depesze niemieckie, dostarczone przez nasłuch radiowy. Odtąd, aż do 1939 roku, polski Sztab Główny, jak też inne instytucje wojskowe i rządowe, w szczególności Ministerstwo Spraw Zagranicznych, otrzymywały liczne, często wielkiej wagi informacje o niemieckich silach zbrojnych i innych resortach JII Rzeszy, dostarczane - bez ujawniania Enigmy jako ich źródła - przez referat niemiecki Biura Szyfrów.

Podług świadectw niektórych uczestników naj dłuższego , bo ponad sześcioletniego, wyłącznie polskiego okresu odczytywania Enigmy (styczeń 1933 - wrzesień 1939), rozwiązanych depesz niemieckich było wiele tysięcy, ale ich dokładniejszą liczbę trudno już bliżej oszacować. Podobnie trudno też ustalić zasady ich dystrybucji i sposoby wykorzystania.

W połowie lipca 1939 roku, wobec nieuchronnej już groźby wojny, szef polskiego Sztabu Głównego, gen. Wacław Stachiewicz, upoważnił Biuro Szyfrów do przekazania całej teoretycznej i praktycznej wiedzy o Enigmie, wraz z polskimi duplikatami Enigm i innymi urządzeniami do dekryptażu, przyszłym sojusznikom wojennym.