***Enigma do usłyszenia***– podcast Centrum Szyfrów Enigma w Poznaniu poświęcony jednemu   
z największych sukcesów kryptologicznych w historii ludzkości.

**Polskie urządzenia, które pomogły złamać szyfr Enigmy**

Złamanie szyfru Enigmy przez Mariana Rejewskiego w grudniu 1932 roku pokazało, że człowiek przy wykorzystaniu matematyki jest w stanie pokonać skomplikowany szyfr wygenerowany przez maszynę. Było to prawdziwą rewolucją w świecie kryptologii.

O tyle wprowadził swoim sukcesem kryptologię na zupełnie nowe tory, dlatego że nagle okazało się, że abstrakcyjna matematyka jest skutecznym narzędziem ataku na szyfry. Nikt tego nie przeczuwał, nikt tego nie zdawał sobie sprawy. Natomiast sukces Rejewskiego doprowadził do dzisiejszego stanu rzeczy, w którym kryptologia nie jest niczym innym jak jedną z dziedzin matematyki stosowanej.

Tłumaczył doktor Marek Grajek.

Z punktu widzenia dowództwa polskiej armii złamanie szyfru Enigmy miało znaczenie czysto praktyczne – wywiad wojskowy zyskał możliwość odczytywania depesz utajnianych przez zachodniego sąsiada. Pozyskane informacje umożliwiały reagowanie na działania Niemiec. By w pełni to wykorzystać, należało odczytywać wiadomości w dużych liczbach oraz w możliwie krótkim czasie, póki zawarte w nich informacje były aktualne. Aby temu sprostać, polscy matematycy musieli zmierzyć się z dwoma wyzwaniami – odtworzeniem maszyny przeciwnika, by dysponować narzędziem umożliwiającym szybkie deszyfrowanie wiadomości, oraz usprawnieniem metody rekonstrukcji kluczy. Stworzenie polskiej kopii Enigmy na podstawie matematycznych analiz Rejewskiego zlecono Antoniemu Palluthowi – współwłaścicielowi warszawskiej firmy AVA, współpracującej z Biurem Szyfrów.

Opowiada historyk regionalista Mieczysław Kędziora:

Palluth włożył w replikę Enigmy bo on można powiedzieć był całym mechanikiem i inżynierem, który kierował. Oczywiście nie robił tego sam bo miał zespół doskonałych fachowców jak Fokczyński, Bendlecki i inżynierowie bracia Danielowiczowie. Jeden wtenczas był jeszcze studentem, ale oni przecież byli współwłaścicielami firmy AVA. To była firma która robiła na potrzeby wojska.

Inżynierowie firmy AVA zaprojektowali urządzenia działające identycznie jak oryginalne. Nie znali jednak projektów niemieckiej maszyny, stąd polskie kopie miały odmienną konstrukcję. Charakterystycznym elementem, po którym można rozpoznać wyprodukowane w Warszawie urządzenia, jest łącznica kablowa. W oryginalnej Enigmie była umieszczona z przodu maszyny, natomiast w polskiej kopii z tyłu. Różnice te dowodzą, że polskie Enigmy zostały odtworzone na drodze teoretycznej, a inżynierowie AVY zbudowali urządzenie, którego nigdy nie widzieli.

Odnalezienie klucza wiadomości było najbardziej żmudnym zajęciem w procesie łamania szyfru Enigmy. Wymagało to odgadnięcia, w jaki sposób nadawca wiadomości ustawił wirniki maszyny. Dla trzech rotorów trzeba było sprawdzić ponad 100 tysięcy możliwych ustawień. Proces ten można było usprawnić poprzez wykorzystanie charakterystycznych cykli szyfru Enigmy i stworzenie bazy wszystkich kluczy wiadomości. Taki katalog pozwalałby na błyskawiczne ustalenie klucza wiadomości, jednak jego ręczne stworzenie wymagałoby kilku lat pracy. Z tego powodu polscy matematycy zdecydowali się zaprojektować wyspecjalizowane urządzenie pozwalające na badanie cykli szyfru Enigmy. Maszynę nazwano – zgodnie z jej działaniem – cyklometrem. Urządzenie przyspieszyło przygotowanie katalogu kluczy wiadomości, który skrócił czas odnajdywania właściwego ustawienia wirników do kilku minut. Opracowany katalog jednak bardzo szybko stał się przestarzały. Zmiany wprowadzone przez Niemców w konstrukcji maszyny uniemożliwiały jego dalsze wykorzystywanie.

Odpowiedzią polskich kryptologów na nową sytuację było opracowanie dwóch niezależnych metod określania kluczy wiadomości. Pierwszą z nich były płachty zaprojektowane przez Henryka Zygalskiego, będące udoskonaloną formą katalogu cykli. Zygalski zdecydował się na wycięcie otworów w arkuszach papieru w miejscach występowania charakterystycznych cykli szyfru Enigmy. Nałożenie na siebie odpowiedniej liczby płacht na podświetlonej powierzchni pozwalało sprawdzić, czy dana kombinacja wirników jest prawidłowa. Jeśli po zakończonej pracy z któregoś otworu wydostawało się światło, oznaczało to, że odnaleziono klucz wiadomości. W przeciwnym razie należało sprawdzić inny zestaw arkuszy.

Rewolucyjna okazała się koncepcja Mariana Rejewskiego, który zaprojektował urządzenie automatycznie sprawdzające wszystkie możliwe ustawienia wirników. Nazwano je bombą. Istnieją różne wersje pochodzenia tej nazwy. Jedna z nich odnosi się do charakterystycznego tykania urządzenia, przypominającego bombę zegarową. Inna z kolei odsyła do nazwy deseru, bomby lodowej, przy którym matematycy mieli wpaść na pomysł jej skonstruowania. Gdy maszyna trafiła na klucz właściwy dla danej wiadomości, zatrzymywała się i wskazywała odpowiednią kombinację ustawień wirników. Zbadanie wszystkich kombinacji kluczy przez sześć równolegle działających urządzeń zajmowało zaledwie dwie godziny.

Wszystkie wypracowane przez polskie Biuro Szyfrów materiały zostały przekazane sojusznikom – Francji i Wielkiej Brytanii na konferencji w Pyrach w lipcu 1939 roku. Koncepcja automatycznego sprawdzania kluczy przez bomby wyznaczyła kierunek prac aliantów, którym przewodził brytyjski kryptolog Alan Turing. Od konstrukcji specjalistycznych maszyn wspomagających dekryptaż konkretnego szyfru był już tylko krok do zaprojektowania urządzenia uniwersalnego – odpowiednika dzisiejszego komputera. Nieprzypadkowo po zakończeniu II wojny światowej nad rozwijaniem narzędzi tego typu pracowali byli kryptolodzy z Wielkiej Brytanii i USA. Owocem ich pracy były pierwsze programowalne urządzenia cyfrowe. Warto pamiętać, że historia tych wydarzeń została zapoczątkowana w Poznaniu w 1929 roku.

Podcast Centrum Szyfrów Enigma zrealizowano w ramach projektu *Enigma bez barier.* Autorami scenariusza są Grzegorz Wanat i Sławomir Wierzbicki. Czytał Sławomir Wierzbicki.   
W podcaście wykorzystano dźwięki Enigmy nagrane przez Patryka Piłasiewicza, a także fragmenty rozmów Piotra Bojarskiego z rodzinami kryptologów oraz ekspertami, zrealizowanych na zlecenie Urzędu Miasta Poznania. Produkcja – Poznańskie Centrum Dziedzictwa. Dofinansowano ze środków Muzeum Historii Polski w Warszawie w ramach programu „Patriotyzm Jutra”.