Osoby które zmieniły świat

Polacy którzy złamali enigmę



Czym jest Enigma?

Pochodzenie i zasada działania

Człowiek a maszyna

- Pod koniec I wojny światowej kryptolodzy znali i potrafili skutecznie złamać wszystkie znane do tej pory metody szyfrowania i kodowania informacji. Aby rozkodować informację wystarczyło poczekać na najprostszy błąd szyfranta, wykradzenie części rozkodowanej depeszy, lub użytego klucza.

- Kodowanie tą drogą było bardzo niepewne i żmudne, dlatego w końcowej fazie I wojny światowej, jednocześnie w różnych miejscach świata zaczęły pojawiać się pierwsze maszyny stworzone do tego typu zadań. Znacznie skracały czas szyfrowania i odszyfrowywania wiadomości, były także znacznie bezpieczniejsze.

Pierwsze maszyny szyfrujące

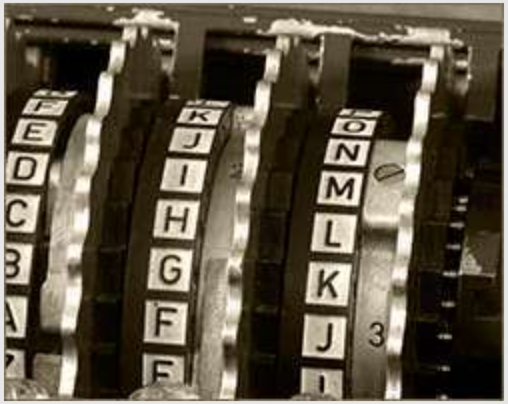
- Pierwsza maszyna szyfrująca była dziełem dwóch oficerów marynarki holenderskiej, zostali oni jednak okradzeni ze swego wynalazku przez zwierzchników państwowych. W tym samym czasie maszynę szyfrującą opatentował także Amerykanin, Edward Hebern, lecz nie przyniosła mu ona sukcesu.

- Wreszcie, w lutym 1918 roku, wniosek patentowy dotyczący maszyny szyfrującej złożył niemiecki inżynier, Arthur Scherbius. Jego wynalazek, maszyna szyfrująca Enigma, miała z czasem zyskać status najsłynniejszej maszyny szyfrującej w historii.

Enigma

- Enigmy trafiły na niemiecki rynek. Wtedy oto zainteresowało się nią niemieckie wojsko i zakupiło kilka specjalnie zmodyfikowanych egzemplarzy, a następnie by nie wzbudzać podejrzeń, powoli zaczęto wycofywać maszynę z rynku.

- Mechanizm szyfrujący składał się z trzech bębnów kręcących się w jedną stronę oraz jednego dodatkowego, kręcącego się w przeciwną. Po ustawieniu bębnów według klucza i wpisaniu litery, pokazywała się litera zakodowana. Aby zaś rozkodować informację, wystarczyło odwrócić proces.



Ciekawostka - ilość kombinacji enigmy wynosiła około 10^116, jest to

100 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000

Enigma w polskich rękach

Historia trzech matematyków

Sekret Enigmy

- Kryptolodzy większości krajów świata uznali Enigmę za maszynę niemożliwą do złamania. Brytyjczycy, którzy reprezentowali w tym czasie najwyższy poziom w łamaniu cudzych szyfrów i kodów, zrezygnowali nawet z prowadzenia nasłuchu niemieckiej łączności radiowej szyfrowanej Enigmą. Uznali, że nie ma sensu tracić czasu na prowadzenie nasłuchu depesz, których i tak nie uda się złamać. Natomiast Francuzi, po zakończeniu I w.ś zaniedbali rozwój służb kryptologicznych.

- Nie mogąc liczyć na kryptologów, pokładali nadzieje w szpiegach licząc, że zdołają oni ukraść lub kupić sekret Enigmy. Ich nadzieje spełniły się, gdy z francuskim wywiadem skontaktował się urzędnik pracujący w niemieckim biurze szyfrów, gotów sprzedać niektóre z jego sekretów. W ciągu następnych 10 lat sprzedał Francuzom instrukcje obsługi Enigmy oraz klucze do szyfru obejmujące okres wielu miesięcy.

Informacje o Enigmie

- Francuzi nie dysponowali kryptologami, którzy potrafiliby wykorzystać materiały dostarczone przez szpiega. W efekcie najpierw zwrócili się z propozycją współpracy do Brytyjczyków. Już po trzech dniach z Londynu nadeszła negatywna odpowiedź: Brytyjczycy uznali materiały za bezwartościowe. Z braku lepszych pomysłów w następnej kolejności Francuzi zwrócili się do Warszawy, udostępniając od tej pory kopie wszystkich materiałów w zamian za obietnicę podzielenia się przez Polaków ewentualnymi efektami wykorzystania dostarczonych informacji

- Pewnego dnia 1929 roku urząd celny w Warszawie wysłał alarmową wiadomość do Biura Szyfrów Wojska Polskiego. Dostarczona bowiem do nich została niewiadomego pochodzenia paczka, o zwrot której pieczołowicie ubiegał się nieznajomy człowiek. Żądał odesłania paczki do Niemiec, twierdząc, że jest to omyłkowo przysłana aparatura radiowa. Został on odesłany z powrotem, z racji, że polscy celnicy kończyli pracę. W międzyczasie paczka została otworzona, a w niej ukazał się wojskowy model enigmy. W międzyczasie Polacy w pośpiechu zrobili zdjęcia, przerysowali okablowanie, a następnie ponownie zapakowali paczkę.

Trzech matematyków

- Szef niemieckiej sekcji polskiego Biura Szyfrów, Maksymilian Ciężki, szybko uświadomił sobie konieczność użycia zupełnie nowych metod ataku na szyfr. Zorganizował kurs kryptologii dla grupy studentów matematyki za Uniwersytetu Poznańskiego, po czym najlepszym jego absolwentom pozwolił terminować przez trzy lata w profesji kryptologa w filii Biura Szyfrów, specjalnie w tym celu utworzonej w Poznaniu.

- We wrześniu 1932 roku trójka matematyków, która przetrwała okres próby, została przeniesiona do Warszawy. Byli to Henryk Zygalski, Jerzy Różycki i Marian Rejewski.

Polscy matematycy z Uniwersytetu Poznańskiego, od lewej: Henryk Zygalski, Jerzy Różycki i Marian Rejewski, którzy w 1932 roku złamali szyfr Enigmy.

Na zdjęciu Maksymilian Ciężki

Ciekawostka – Ciężki w pierwszej kolejnosci okazał próbki szyfru inżynierowi Ossowieckiemu, znanemu specjaliście od zjawisk paranormalnych. Jednak szyfr Enigmy nie okazał się dla niego przejżysty.

Złamanie kodu

- Jesienią 1932 roku pod przewodnictwem najstarszego z nich - Mariana Rejewskiego, matematycy zabrali się do pracy. Szybko przekształcili dostępne informacje o maszynie w układ równań, po czym zabrali się do jego rozwiązywania.

- Po drodze napotkali kilka przeszkód. Pierwszą z nich był fakt, że rolę zmiennych w jego równaniach odgrywały *permutacje. Rejewski jako pierwszy sformułował niezbędną teorię, a jedno z jego twierdzenie w wiele lat potem zostało określone mianem "twierdzenia, które wygrało II wojnę światową".

- Drugim i ostatnim problemem była nieznajomość codziennego klucza. Jednak tygodniach prób zaczęli wpisywać najprostsze kody typu AAA, ABC. Wydedukowali, że na pewno kiedyś Niemcy wykażą się kreatywnością i zaczną wpisywać tego typu kody. Mieli rację. W grudniu 1932 roku Enigma została złamana. Szyfr uważany za niemożliwy do złamania poddał się po niespełna 3 miesiącach ataku.

*Permutacja – przekształcenie zbiorów liczbowych poprzez nakładanie ich na samych siebie.

Wikipedia: https://pl.wikipedia.org/wiki/Permutacja

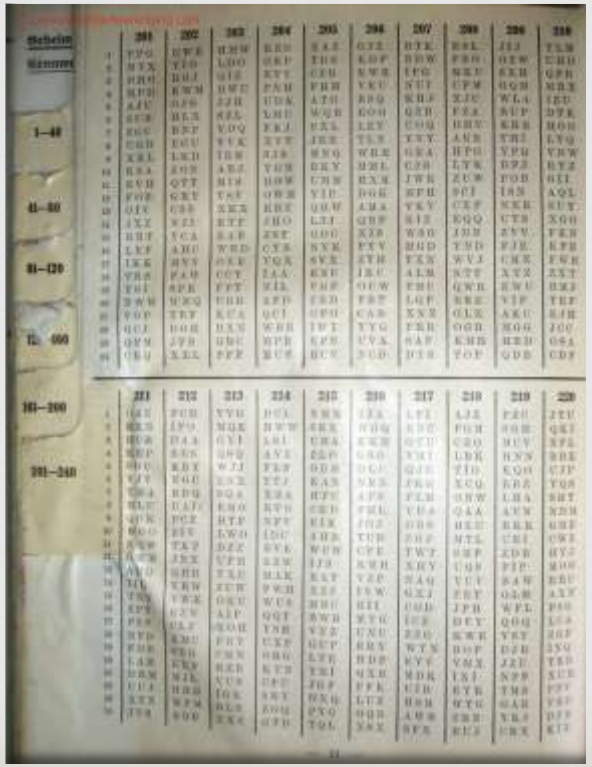


Tabela kluczy Enigmy

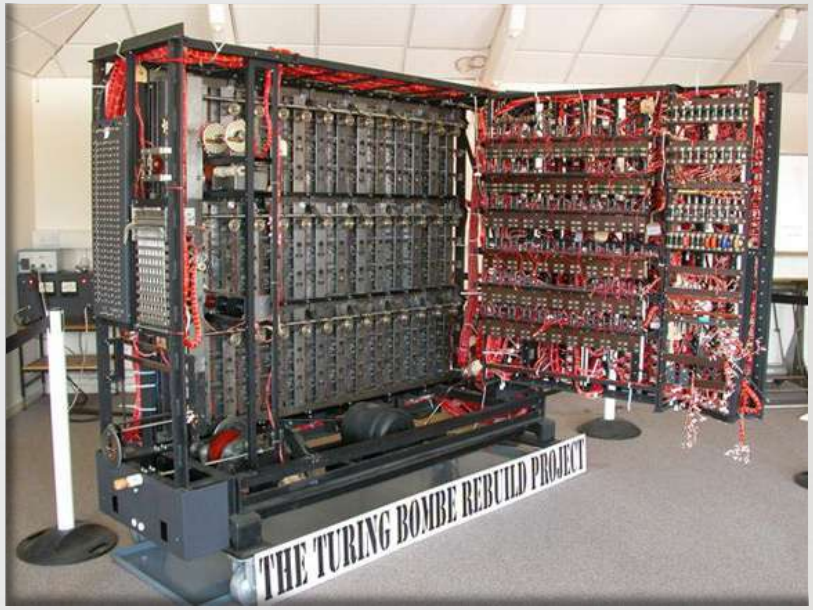
Cyklometr Rejewskiego

- Raz rozkodowana depesza nic jednak nie znaczyła. Niemcy codziennie zmieniali ustawienie bębnów, co nie pozwalało na ponowne rozkodowanie wiadomości. Aby sobie z tym poradzić Rejewski wynalazł tak zwany Cyklometr.

- Składał się z dwóch zestawów wirników Enigmy i był wykorzystywany do ustalenia długości i liczby cykli permutacji generowanych przez Enigmę. Po zapisaniu katalogu wszystkich charakterystyk można było odczytywać odpowiednie permutacje odpowiadające ustawieniu wirników danego dnia. Pochłonęło to ponad rok pracy, ale po zakończeniu projektu w już roku 1935, określenie klucza dziennego było już możliwe w czasie kilku godzin.

Bomba kryptologiczna

- 24 lipca 1949 roku pod Warszawą odbyła się konferencja kryptologów z Polski, Francji i Anglii, gdzie zostały im przekazane prace nad złamaniem kodu enigmy, kilka zrekonstruowanych modelów, oraz instrukcje budowy bomby kryptologicznej – urządzenia stworzonego przez trzech polskich kryptologów, które łącząc kilka enigm potrafiło sprawdzić kilkanaście tysięcy opcji ustawienia wirników w mniej niż dwie godziny.



Angielska wersja bomby kryptologicznej – bomba Turinga

Po kapitulacji

Ucieczka z kraju

- W wyniku kampanii wrześniowej, Polskie Biuro Szyfrów działało tylko przez kilka dni, a później trzeba było ewakuować ludzi. Rejecki, Różycki i Zygalski przez Rumunię trafili do Francji, gdzie także pracowali nad złamaniem enigmy, lecz w znacznie gorszych warunkach. Francuzi posiadali bowiem tylko dwa egzemplarze.
- Podczas pobytu Polaków we Francji 9 stycznia 1942 w wyniku katastrofy statku pasażerskiego Lamoricière na Morzu Śródziemnym, Jerzy Różycki zginął wraz z 221 innymi pasażerami.
- Pozostali dwaj byli chwilowo aresztowani w Hiszpanii. Po uwolnieniu natychmiast wyemigrowali do Anglii.

Tablica upamiętniająca Jerzego Różyckiego w wyszkowskim gimnazjum. Na tablicy (1926r) rok ukończenia szkoły.

Odsunięci od projektu

- Henryk Zygalski i Marian Rejewski – Polscy kryptologowie, odkrywcy sposobu rozszyfrowania Enigmy, twórcy Bomby Kryptologicznej zostali najzwyczajniej odsunięci od projektu. Anglicy w międzyczasie stworzyli własny system deszyfrujący opierający się na podstawie badań polskiej trójki i na bieżąco potrafili rozszyfrowywać niemieckie depesze. Polacy natomiast zostali przeniesieni do Polskiego Batalionu Łączności.

Zasługi polskiej trójki

Uratowane istnienia

Kontynuacja projektu

- Po konferencji z 24 lipca 1949r. Brytyjczycy na bazie uzyskanych informacji niezwłocznie przystąpili do budowy wielkiej organizacji kryptologicznej, która u kresu wojny tylko w jednym ośrodku w Bletchley Park zatrudniała blisko 12 tysięcy ludzi.
- Kryptolodzy z Bletchley Park z czasem zdobyli prawie całkowite panowanie nad niemieckimi szyframi, łamiąc depesze wszystkich rodzajów niemieckich wojsk i czytając je często szybciej niż właściwy adresat. Jest oczywiste, że dekryptaż Enigmy odegrał kapitalną rolę w trakcie II wojny światowej.
- Coraz powszechniej też uznaje się, że przekazanie aliantom sekretu łamania jej szyfru stanowiło najważniejszy polski wkład w zwycięstwo aliantów w całym konflikcie. Jakie jednak było znaczenie tego sukcesu dla losów wojny?

Największy polski sukces

- Historycy różnią się w ocenie. Nawet najostrożniejsi wśród nich zgadzają się, że złamanie Enigmy przyczyniło się do skrócenia wojny o co najmniej 2-3 lata. Zważywszy, że średnio w ciągu jednego roku wojny traciło życie około 10 milionów ludzi oznacza to, że Marian Rejewski i jego koledzy ocalili około 20-30 milionów istnień ludzkich.
- Gdyby wojna w Europie trwała jeszcze jesienią 1945 roku, pierwsze egzemplarze bomby jądrowej zostałyby zrzucone nie na miasta japońskie, lecz na Berlin i inne miasta naszego kontynentu. W tym sensie polscy kryptolodzy ocalili Europę od użycia broni jądrowej.
- Gdyby wojna trwała dłużej, armie rosyjskie zakończyłyby swój marsz na zachód nie w Berlinie i na Łabie, lecz pomaszerowałyby do Paryża i dalej - Żelazna Kurtyna zimnej wojny zapadałaby zapewne nad znaczną częścią Europy.
- Ale to tylko ostrożne szacunki znaczenia sukcesu polskich kryptologów. Historycy zwracają uwagę, że w czasie II wojny światowej były okresy, w których alianci znajdowali się niebezpiecznie blisko częściowej lub całkowitej porażki. Klęski ponoszone w Bitwie o Atlantyk w połowie 1942 roku sprawiły, że w Wielkiej Brytanii do niebezpiecznie niskiego poziomu spadł poziom strategicznych zapasów: paliw, żywności, surowców do produkcji broni i amunicji. Gdyby nie dekryptaż depesz Enigmy, gdyby U-Bootom udało się zatopić kilkadziesiąt statków więcej, być może w połowie 1942 roku Wielka Brytania musiałaby poprosić o pokój, nie mogąc uzbroić swych żołnierzy i wyżywić obywateli.
- Bez wysp brytyjskich - późniejszy kontratak z udziałem wojsk USA okazałby się wielokroć bardziej skomplikowany, jeśli w ogóle możliwy; co mogłoby diametralnie zmienić wynik wojny.

I to zasługa trzech polskich kryptologów.

Koniec

Honorowe złożenie kwiatów pod pomnikiem kryptologów przez prof. Andrzeja Lesickiego - rektora UAM w Poznaniu

Źródła:

https://www.polskieradio.pl/39/156/Artykul/752845,Zlamali-szyfr-Enigmy-ocalili-30-milionow-ludzi
https://pl.wikipedia.org/wiki/Enigma
https://pl.wikipedia.org/wiki/%C5%81amanie_szyfru_Enigmy#Polska
Enigma. Historia bez Cenzury - https://www.youtube.com/watch?v=uhSSVsXBPk4
http://lamaczeszyfrow.pl/index.php?id=165
https://pl.wikipedia.org/wiki/Permutacja
https://pl.wikipedia.org/wiki/Cyklometr
https://pl.wikipedia.org/wiki/Bomba_kryptologiczna
https://pl.wikipedia.org/wiki/Jerzy_R%C3%B3%C5%BCycki_(matematyk)
https://amu.edu.pl/aktualnosci/archiwum-na-gown/347226-medal-dla-poznanskich-kryptologow

Prezentację wykonał:
Jakub Haberek