Polskie metody i urządzenia do łamania szyfru Enigmy

mgr inż. Roman Iwanicki

XVI SEMINARIUM WEP

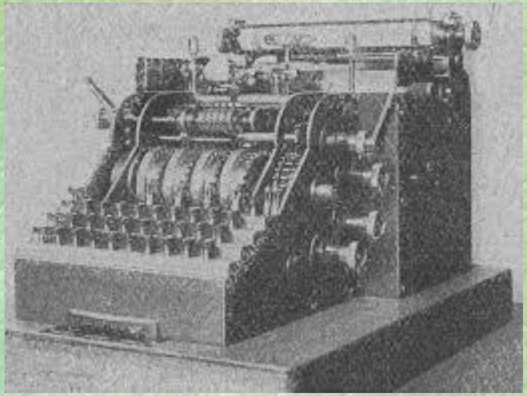
11 kwietnia 2018 r.

Agenda prezentacji

1. Powstanie Enigmy
2. Rodzina urządzeń
3. Wojskowe modele Enigmy M3 i M4
4. Schematy Enigm M3 i M4
5. Klucze kryptograficzne, moc kryptograficzna Enigmy M3
6. Zarządzanie kluczami, tworzenie kluczy depeszowych
7. Zespół polskich kryptologów
8. Przebieg prac kryptoanalitycznych do 1939 r.
9. Aktywność Sztabu Głównego WP w dziedzinie radiowywiadu
10. Polskie metody i urządzenia do łamania szyfru Enigmy
11. Znaczenie sukcesu polskich kryptologów

Powstanie Enigmy

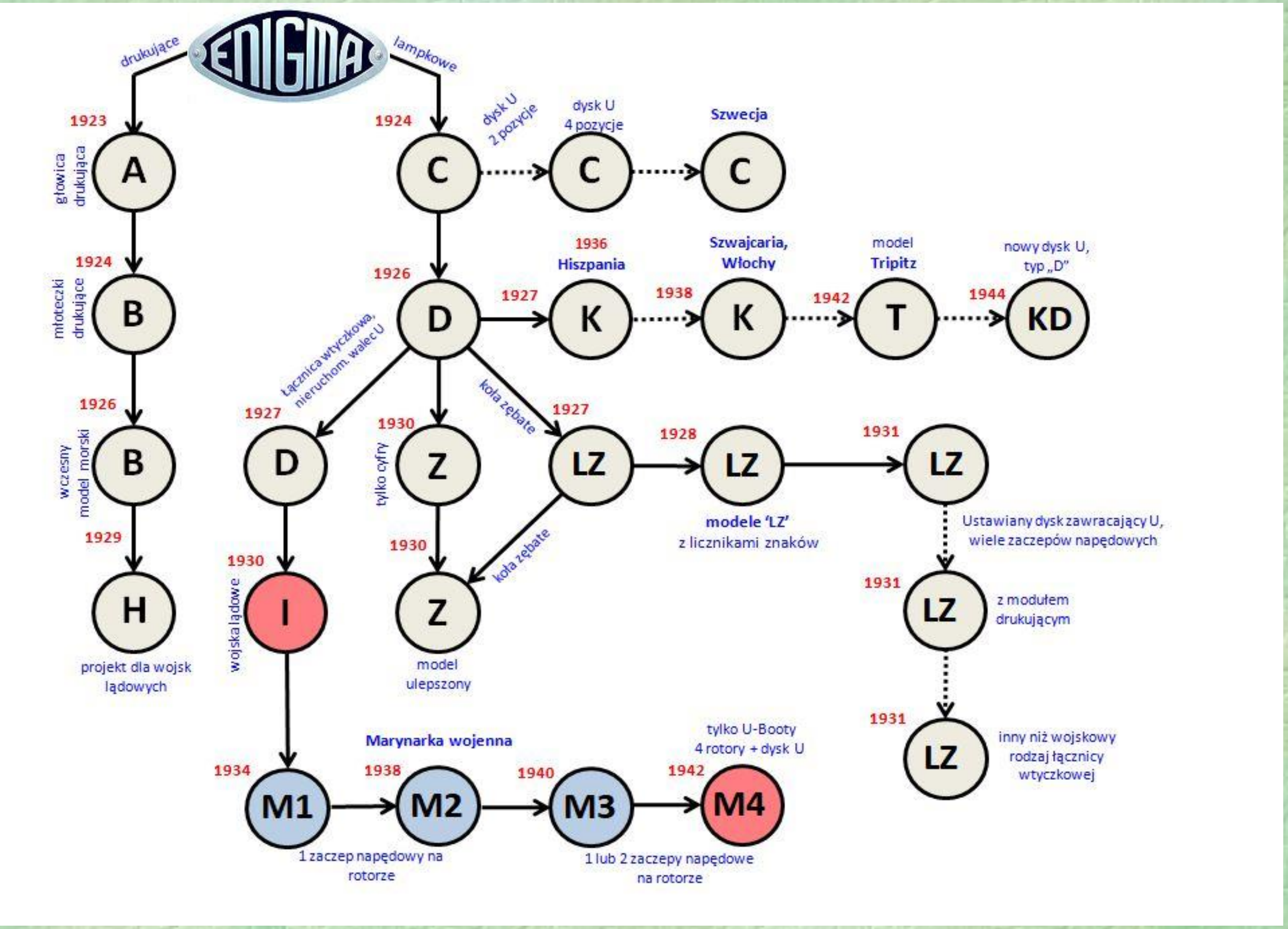
- Patent Artura Scherbiusa (23 lutego 1918 roku)
- Patent Hugo Kocha (7 października 1919 roku)
- Enigmę Model A zaprezentowano w 1923 r. na kongresie Światowego Związku Pocztowego w Bernie



Enigma Model A

W 1929 r. firma *Scherbius & Ritter*, odkupiła patent Hugo Kocha. Później firma ta przekształciła się w firmę *Chiffriermaschinnen AG* , która do końca wojny produkowała różne modele Enigm.

Rodzina urządzeń



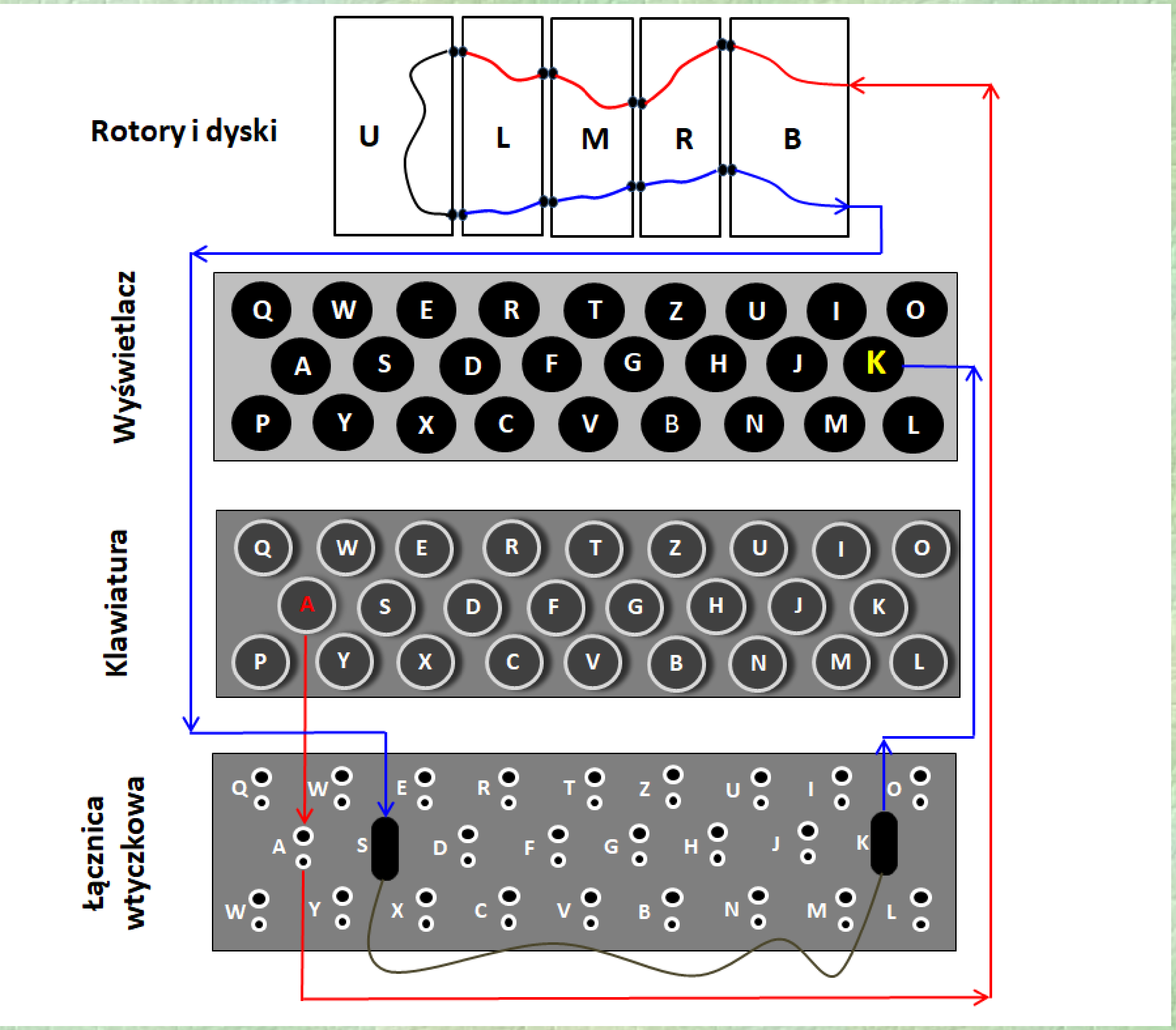
Model D trafił też w celach „poznawczych" do innych krajów, w tym do Polski, W. Brytanii, Japonii, USA

Enigmy wojskowe M3 i M4

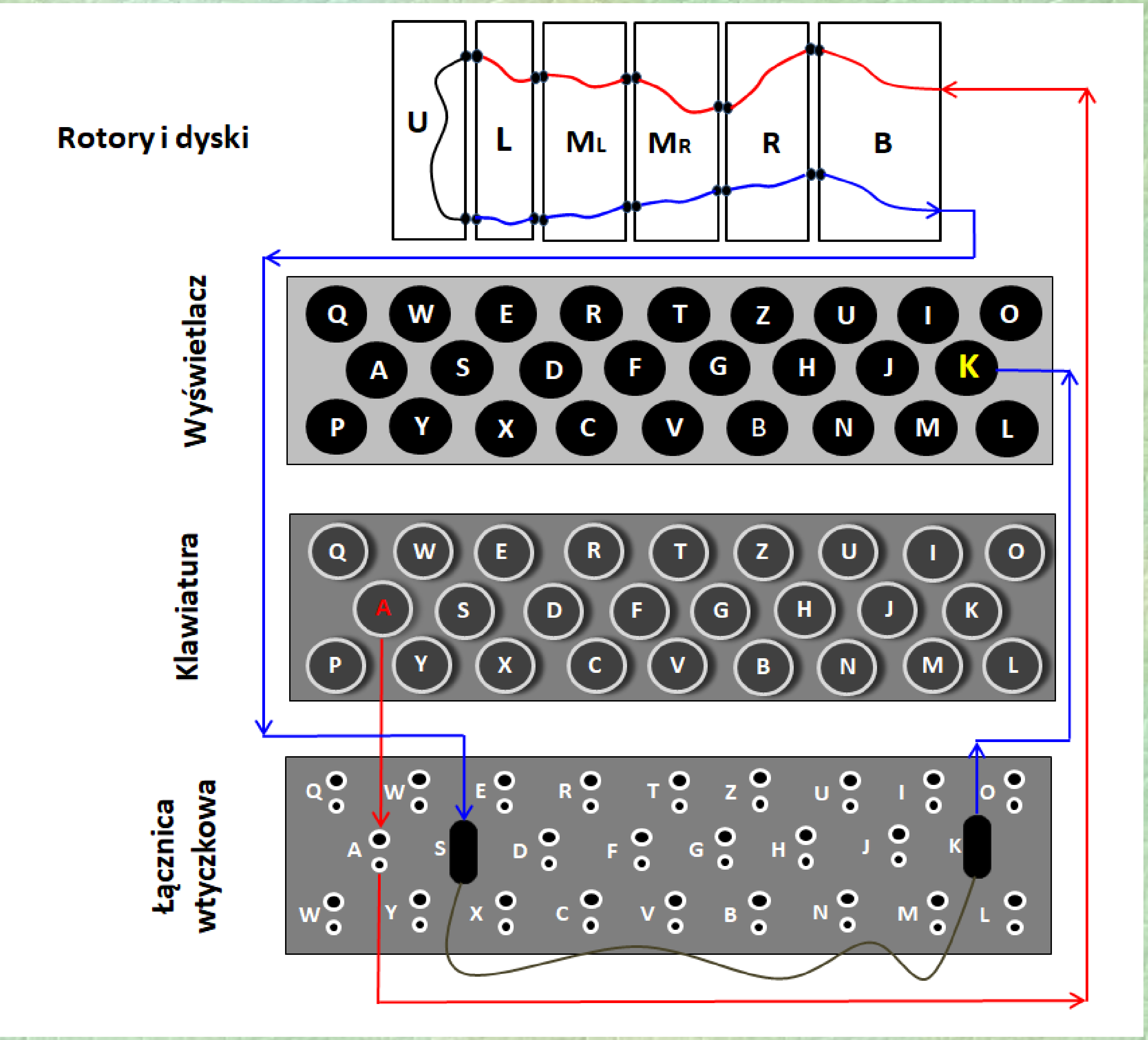
Enigma M3 podstawowy model wojsk lądowych i lotnictwa

Enigma M4 model marynarki wojennej (od 1.02.1942 r.)

Schemat Enigmy Model M3



Schemat Enigmy Model (M4)



Klucze kryptograficzne Enigmy

Klucz konstrukcyjny (strukturalny)

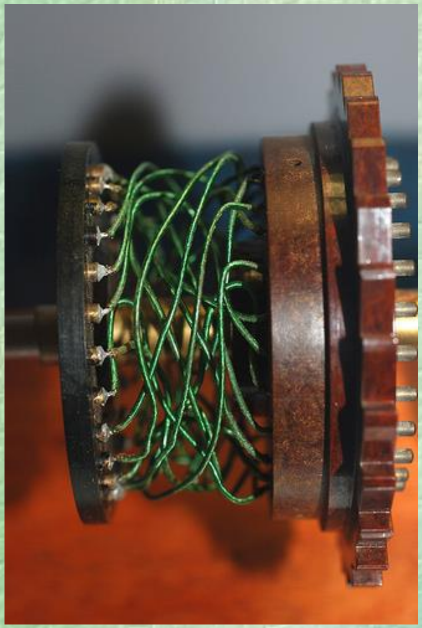
- połączenia wewnątrz rotorów L, M, R i dysku U
- połączenia dysku B z klawiturą. Łącznie ok. **$2{,}08 * 10^{119}$**

Ustawienia operacyjne (klucze kryptograficzne)

- *kolejność ustawień* rotorów na osi (z tabel)
- *ustawienie zaczepów napędowych* na rotorach R i M (z tabel); na L nie był ważny bo nie działał
- *połączenia łącznicy* ; 6-10 kabli (z tabel)
- *położenie depeszowe* każdego z rotorów do szyfrowania depeszy (wybór indywidualny.)

Łącznie ok. **$7{,}1 * 10^{18}$** ustawień operacyjnych

Całkowita liczba ustawień **ok. $1{,}5 * 10^{138}$** !



rotor Enigmy

Klucze depeszowe Enigmy

- Znaczenie klucza depeszowego
- Klucze depeszowe w okresie 1932 - 1938
  - **szyfrant:** dokonuje ustawień Enigmy zgodnie z tabelami kluczy
  - wybiera indywidualne *ustawienie depeszowe* rotorów
  - szyfruje dwukrotnie swój wybór przy pomocy klucza z tabeli (*ustawienia zasadniczego*) i przesyła wynik w nagłówku depeszy (pierwsze 6 liter)
  - przestawia położenia rotorów na *ustawienia depeszowe* i szyfruje depeszę
- Klucze depeszowe w okresie od 15.IX.1938 do V.1940
  - **szyfrant:** wybiera dwa 3 literowe ustawienia (*zasadnicze i depeszowe)*
  - ustawia rotory wg. *ustawienia zasadniczego* i dwukrotnie szyfruje *ustawienie depeszowe;* wynik – 9 liter (*ustawienie zasadnicze* i zaszyfrowane *ustawienie depeszowe)* przesyła w nagłówku depeszy
  - przestawia położenie rotorów na *ustawienie depeszowe* i szyfruje depeszę.
- Różnice między obiema metodami

Wskaźniki ustawień depeszowych

Przykłady z nagłówek depesz z jednego dnia

do 15.IX.1939		*po 15.IX.1939*
AUQ AMN	TXV TTI	SHP, CHV PZT
BNH CHL	IKG JKF	RTJ, WAH WIK
BCT CGJ	IKG JKF	OMN, HLT ICK
CIK BZY	IJD JHU	HPL, RAW KTW
DDB VDV	JEC MIC	DER, OET INJ
EJP IPS	MAW UPX	TIM, KHL VNJ
FBR KLE	NXD QTU	DQX, LWJ KWR
GPB ZSV	NXD QTU	CVT, AIS ALM
HNO THD	RJL WPX	PCH, HIL VNT
HNO THD	RJL WPX	NOT, KTD HND

Zespół polskich kryptologów

zdjęcie z 1932 r.

Marian Rejewski (16.08.1905-13.02.1980)

- 1923 – zdał egzamin maturalny w Bydgoszczy, podejmuje studia na Uniwersytecie Poznańskim
- I.1929 – bierze udział w kursie kryptologicznym zorganizowanym przez SG WP w Poznaniu
- 1.III.1929 – uzyskuje tytuł magistra filozofii (matematyki) na Uniwersytecie Poznańskim
- 1930 – odbywa roczny staż w Getyndze, później asystent na Wydziale Matematyki UP
- 1.IX.1932 – przyjęty do Biura Szyfrów,
- IX – X.1932 – rozwiązanie niemieckiego kodu morskiego, wyniki wykorzystane przez Brytyjczyków do złamania morskiej Enigmy
- X - XI.1932 – analiza szyfru Enigmy, samotna praca po godzinach
- XII.1932 – **złamanie Enigmy** tj. rozwiązanie układu równań permutacyjnych tj. wyznaczenie połączeń wewnętrznych Enigmy (klucza strukturalnego); budowa replik Enigmy w zakładach AVA.

Zespół polskich kryptologów


UNIWERSYTET POŻNAŃSKI

WYDZIAŁ MATEMATYCZNO-PRZYRODNICZY

DYPLOM MAGISTRA FILOZOFJI

Pan Marjan Rejewski

urodzony dnia 16 sierpnia 1905 w Bydgoszczy, odbył przepisane studja na Uniwersytecie Poznańskim na Wydziale Matematyczno-Przyrodniczym w zakresie matematyki i zdał następujące przepisane egzaminy:

z rachunku różniczkowego i całkowego ze wstępem do analizy	z wynikiem dobrym
z geometrji analitycznej	z wynikiem bardzo dobrym
z zasad algebry wyższej wraz z elementami teorji liczb	z wynikiem bardzo dobrym
z mechaniki teoretycznej	z wynikiem bardzo dobrym
z fizyki doświadczalnej	z wynikiem dobrym
z ogólnych zasad nauk filozoficznych ze szczególn. uwzgl. zasad logiki	z wynikiem bardzo dobrym
z teorji grup	z wynikiem bardzo dobrym
z funkcyj eliptycznych	z wynikiem bardzo dobrym
z fizyki teoretycznej (optyki i fizyki cząsteczkowej)	z wynikiem bardzo dobrym

oraz przedstawił z wynikiem bardzo dobrym pracę magisterską na temat:
Opracować teorję funkcyj podwójnie perjodycznych drugiego i trzeciego rodzaju oraz wskazać jej zastosowanie.

Wobec tego Rada Wydziału Matematyczno-Przyrodniczego Uniwersytetu Poznańskiego na wniosek Komisji Egzaminacyjnej nadaje Panu Marjanowi Rejewskiemu

stopień magistra filozofji

jako dowód zakończenia przez niego studjów wyższych w zakresie matematyki

W Poznaniu, dnia 1 marca 1929 roku

Antoni Jakubski
Dziekan

dyplom Mariana Rejewskiego

Marian Rejewski (c.d.)

- 1933 – 1939 bieżące wyznaczenie kluczy do Enigmy przy pomocy różnych metod i urządzeń
- 24.07.1939 – spotkanie z sojusznikami w Pyrach, przekazanie replik Enigmy oraz metod łamania
- 1939 – 1940 ewakuacja przez Rumunię do Francji
- 1940 – 1942 praca we Francji (ośrodki ‘Bruno’ i ‘Cadix’ oraz ‘Post Z’ na przedmieściu Algieru)
- I.1943 ewakuacja z Francji przez Pireneje, aresztowanie i internowanie w Hiszpanii
- VII.1943 ewakuacja przez Gibraltar do W. Brytanii; m.in. łamanie kody SS; w W. Brytanii nie dopuszczony do prac przy Enigmie
- 20.IX.1946 – powrót do Polski, do Bydgoszczy, wiele posad, m.in. księgowy w Wojewódzkim Związku Spółdzielni Pracy
- 1973 gen. Bertrand ujawnia tajemnicę złamania Enigmy
- 1974 Rejewski opisuje udział Polaków w złamaniu Enigmy

Zespół polskich kryptologów

zdjęcie z lat trzydziestych

Henryk Zygalski (15.07.1908 - 30.08.1978)

- 1926 – egzamin maturalny w Poznaniu
- I.1929 – jako student III roku matematyki, bierze udział w kursie kryptologicznym
- 1930-1932 asystent na wydziale matematyki UP
- 1.IX.1932 – przyjęty do Biura Szyfrów w Warszawie wraz z M. Rejewskim i J. Różyckim
- I.1933 – włączony do prac nad szyfrem Enigmy
- pomysłodawca ‘płacht Zygalskiego’, znanych w Bletchley Park, jako ‘Jeffrey’s apparatus’
- 1933 – 1939 pracuje w zespole łamiącym Enigmę
- 1939 – 1943 wspólnie z innymi pracownikami B.Sz. ewakuuje się się do Francji, potem praca we Francji i ewakuacja do W. Brytanii;
- od 1943 praca w W. Brytanii; nie dopuszczony do łamania Enigmy
- pozostał na emigracji w W. Brytanii, gdzie zmarł.

Zespół polskich kryptologów

zdjęcie z lat dwudziestych

Jerzy Różycki (24.07.1909 – 9.01.1942)

- 1927 – rozpoczął studia matematyczne na Uniwersytecie Poznańskim im. A. Mickiewicza
- I.1929 – jako student II roku matematyki bierze udział w kursie kryptologicznym
- 1.IX.1932 – przyjęty do Biura Szyfrów w Warszawie (z M. Rejewskim i H. Zygalskim)
- I.1933 – włączony do prac nad szyfrem Enigmy
- 1933 – 1939 pracuje w zespole zajmującym się bieżącym wyznaczaniem kluczy Enigmy
- twórca ‘metody zegara’
- 1939 – 1942 wspólnie z innymi pracownikami B.Sz. ewakuował się do Francji, potem we Francji pracował w ośrodkach ‘Bruno’ ‘Cadix’ oraz filii ‘Cadix’ w Afryce Północnej
- 9.01.1942 zginął w katastrofie statku ‘Lamoriciere’ w drodze z Afryki Północnej do Francji

Przebieg prac kryptoanalitycznych do 1939

- X.1932 – XII.1932, M. Rejewski wylicza klucz strukturalny przez rozwiązanie układu równań permutacyjnych
- 1933 – 1936 ręczne wyznaczanie kluczy kryptograficznych, 1933 odkrycie cyklicznej zmienności liter kluczy depeszowych, opracowanie „płacht Zygalskiego”
- 1936 opracowanie kartoteki cykli (ponad 100 tys. ustawień) przy pomocy „cyklometru” wyprodukowanego w zakładach AVA; czas wyznaczenia kluczy do depeszy ok. 20 min.
- 1937 wyznaczenie połączeń wewnętrznych nowego rotora U
- 1938 zmiana systemu kluczy depeszowych, dochodzą dwa nowe rotory IV i V. M. Rejewski wraz kolegami projektuje „bombę kryptologiczną”, która powstaje w zakładach AVA w ciągu 3 miesięcy; zestaw 6 „bomb” wyznacza klucze w ciągu ok. 2 h.

Przebieg prac kryptoanalitycznych do 1939

24-26.VII.1939 spotkanie w Pyrach (‘Wicher’)

- goście: G. Bertrand, H. Braqueni (kryptolog) A. Denniston (szef GC&CS), A. Knox, gł. kryptolog , oraz oficer radiowywiadu bryt.
- gospodarze: G. Langer, M. Ciężki oraz kryptolodzy – M. Rejewski, H. Zygalski i J. Różycki.
- przebieg i atmosfera spotkania
- przekazane materiały: repliki Enigmy, idea ‘płacht Zygalskiego’ i bomby kryptologicz., metod wyznaczenia połączeń wew. Enigmy, - wszystkie przedwojenne dokonania BSz.
- IX. 1939 ewakuacja do Francji

Tablica pamiątkowa przy bramie ośrodka ‘Wicher’ w Pyrach

Inicjatywy Sztabu Głównego WP

- budowa sieci stacjonarnych stacji nasłuchowych zapewniających bieżący dopływ depesz szyfrowych przechwyconych z eteru
- współpraca wywiadowcza z sojusznikami, najlepsza z wywiadem francuskim
- ‘rewolucyjny’ pomysł SG WP wzmocnienia zespołu wojskowych kryptologów cywilnymi matematykami (kurs w Poznaniu)
- zapewnienie ochrony materiałów z deszyfrażu: pełna konspiracja źródła, przekazywanie tylko przetworzonych materiałów, drobne dezinformacje np. źródła informacji
- budowa placówki ‘Wicher’ w Pyrach i jej codzienna obsługa

Wskaźniki ustawień depeszowych

Przykłady z nagłówków depesz z jednego dnia (cykle)

do 15.IX.1939		*po 15.IX.1939*
AUQ AMN	TXV TTI	SHP, CHV PZT
BNH CHL	IKG JKF	RTJ, WAH WIK
BCT CGJ	IKG JKF	OMN, HLT ICK
CIK BZY	IJD JHU	HPL, RAW KTW
DDB VDV	JEC MIC	DER, OET INJ
EJP IPS	MAW UPX	TIM, KHL VNJ
FBR KLE	NXD QTU	DQX, LWJ KWR
GPB ZSV	NXD QTU	CVT, AIS ALM
HNO THD	RJL WPX	PCH, HIL VNT
HNO THD	RJL WPX	NOT, KTD HND

Metody i urządzenia – ‘cyklometr’

- ‘Cyklometr’ przeznaczony był do zbudowania *kartoteki cykli (kc)*, która powstała na podstawie dwukrotnego szyfrowania *ustawienia depeszowego* (6 liter na początku depeszy)
- *kartoteka cykli* składała się z 105 456 pozycji; ustawienia rotorów od pozycji *AAA* do pozycji *ZZZ*
- każdej pozycji w *kc* odpowiadały 3 liczby będące *numerami cykli* dla każdej pozycji *klucza depeszowego*; *cykli* było 101
- *kc* wykorzystywano do wyznaczenia *ustawienia zasadniczego* na dany dzień; była to tzw. „*charakterystyka dzienna*”
- na podst. depesz z danego dnia wyznaczano *numery cykli*, które identyfikowały *ustawienie/ustawienia zasadnicze* rotorów
- *ustawienie zasadnicze* rotorów pozwalało na wyznaczenie *ustawienia depeszowego* rotorów i rozszyfrowanie depeszy.

Metody i urządzenia – ‘cyklometr’

*‘**Cyklometr**’* rekonstrukcja graficzna
(*http://www.cryptomuseum.com*)
Oryginał wyprodukowany w zakładach AVA w Warszawie

- dwa zestawy rotorów Enigmy; rotory w zestawie I ustawione na AAA, a w zestawie II na AAD (+3 poz.)
- przełączniki służą do włączenia prądu w obwodzie, który zależnie od długości cyklu zapala pewną ilość lampek.
- połowa zapalonych lampek zawsze parzysta wskazuje *długość cyklu*
- przełącznik po prawej stronie reguluje jasność lampek zależną od ich ilości
- dla jednego ustawienia rotorów trzeba było sprawdzić wszystkie litery (A – Z)
- rotory R przesuwane były o 1 pozycję i dokonywano odczytów długości cykli
- następnie rotory M przesuwane były o 1 pozycję, rotory R na początek itd.

Wskaźniki ustawień depeszowych

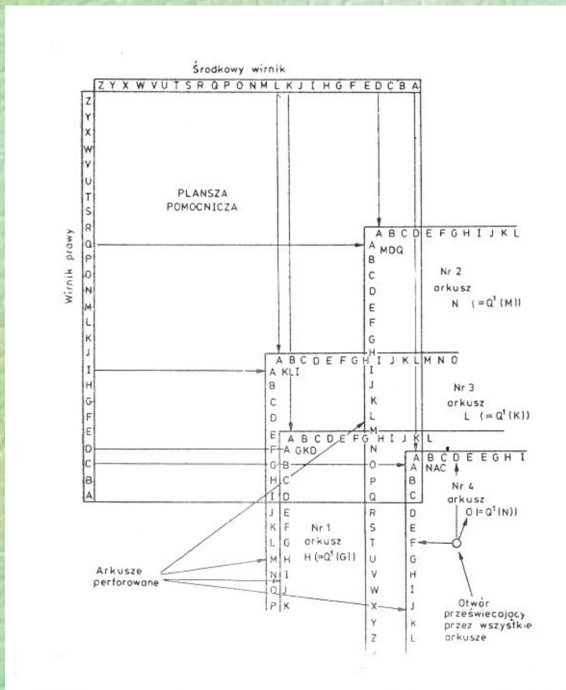
Przykłady z nagłówek depesz z jednego dnia

do 15.IX.1939		*po 15.IX.1939*	
AUQ AMN	TXV TTI	SHP,	CHV PZT
BNH CHL	IKG JKF	RTJ,	WAH WIK
BCT CGJ	IKG JKF	OMN,	HLT ICK
CIK BZY	IJD JHU	HPL,	RAW KTW
DDB VDV	JEC MIC	DER,	OET INJ
EJP IPS	MAW UPX	TIM,	KHL VNJ
FBR KLE	NXD QTU	DQX,	LWJ KWR
GPB ZSV	NXD QTU	CVT,	AIS ALM
HNO THD	RJL WPX	PCH,	HIL VNT
HNO THD	RJL WPX	NOT,	KTD HND

Metody i urządzenia – ‘płachty Zygalskiego’

- 15.IX.1938 zmienił się sposób wyboru *ustawień depeszowych*
- kryptolodzy zaobserwowali teraz rzadziej pojawiające się powtórzenia liter na pozycjach 1 - 4, 2 - 5, i 3 – 6, tj. zaszyfrowanych *ustawień depeszowych*
- *kartoteka cykli* stała się nieprzydatna; trzeba było stworzyć katalog tzw. *punktów stałych* (permutacji jednoelementowych – ‘*samiczek’*) dla wszystkich możliwych ustawień rotorów
- katalog *punktów stałych* służył do wyznaczania położenia rotorów na osi oraz ich położeń początkowych
- położenie *punktów stałych* oznaczano otworem na arkuszu 51x51 pozycji; dla każdej kolejności rotorów na osi (6) trzeba było wykonać 6 po 26 arkuszy (po 15.XII.1938 60 x 26 kpl.)
- przed wojną wycięto żyletkami 6 kpl. arkuszy.

Metody i urządzenia – ‘płachty Zygalskiego’



- szkic pokazujący sposób posługiwania się arkuszami pochodzi z książki *K.* Gaja *Szyfr Enigmy metody złamania*
- arkusze nakładano na pudełko z szybą podświetlaną od spodu
- pierwszy arkusz stanowił współrzędne koordynacyjne wg. których nakładano z odpowiednim przesunięciem arkusze odpowiadające kolejnym depeszom
- każdy kolejno nakładany arkusz zmniejszał liczbę prześwietlanych otworków
- jeśli nie nastąpiła pomyłka, świecący punkt wskazywał kolejność rotorów oraz ich położenie zasadnicze
- poniżej angielska wersja arkuszy Zygalskiego z Bletchley Park (*Jeffrey’s apparatus’*)

Metody i urządzenia – ‘bomba’

- Metoda arkuszy (‘*płacht*’) Zygalskiego była bardzo skuteczna, ale była też bardzo pracochłonna; w zasadzie mogli z niej korzystać tylko kryptolodzy, potrzebna była automatyzacja
- M. Rejewski w dyskusji z kolegami zaproponował konstrukcję automatu składającego się 3 par rotorów, po jednej parze dla każdej pozycji klucza depeszowego;
- do wybuchu wojny w zakładach AVA wykonano 6 *bomb kryptologicznych*, które sprawdzały jednocześnie wszystkie ustawienia 3 rotorów na osi
- nazwa przejęta przez Brytyjczyków (‘*bombe’**) pochodziła od charakterystycznego ‘tykania’ urządzenia lub od chwili powstania koncepcji – kryptolodzy w kawiarni jedli lody nazywane ‘bombami’.

* ideę działania oraz dokumentację polskich *‘bomb’* przekazano Brytyjczykom w języku niemieckim w czasie spotkania w Pyrach w lipcu 1939 r.

Metody i urządzenia – ‘bomba’

‘Bomba’ rekonstrukcja graficzna (*http://www.cryptomuseum.com)* Oryginały wyprodukowano w zakładach AVA w Warszawie

- przed uruchomieniem urządzania każdy z zestawów rotorów był wstępnie ustawiany na podstawie ustawienia *zasadniczego* z depeszy
- przy pomocy przełączników, konfigurujących połączenia wewnętrzne, wybierano którego *punktu stałego* (‘*samiczki*’) szukamy dla każdej pary rotorów
- silnik ukryty w szafce synchronicznie poruszał wszystkie pary rotorów.
- przekaźniki wewnątrz *bomby* połączone z przełącznikami na płycie czołowej zatrzymywały urządzenie, gdy spełnione zostały warunki logiczne określone przez kryptologów – czyli znaleziony został poszukiwany *punkt stały.*
- od 15.XII.1938 potrzeba było 60 bomb; 5 rotor.

Znaczenie złamania szyfru Enigmy

- monitorowanie komunikacji wojskowej i innych formacji (rozkazy i meldunki) na wielu frontach lądowych, powietrznych i morskich; w rezultacie znajomość zamierzeń nieprzyjaciela skróciła przebieg wojny 2-3 lata.
- monitorowanie przebiegu operacji wojskowych i wywiadowczych, w tym dezinformacyjnych
- dowiedziono, że łamaniem szyfrów powinni zajmować się matematycy, inżynierowie oraz specjaliści od łączności
- dowiedziono, że przy łamaniu szyfrów mogą ze sobą współpracować zespoły wojskowe i cywilne (pomysł zastosowany w 1939 r. w Bletchley Park)
- po raz pierwszy w historii kryptoanalizy do łamania szyfrów zastosowano urządzenia (tu elektromechaniczne)

Znaczenie złamania szyfru Enigmy

- urządzenia wykorzystywane do wyznaczania ustawień początkowych Enigmy (zwłaszcza *bomba* i jej angielska następczyni) stanowiły punkt zwrotny w praktycznym rozwinięcia koncepcji Turinga nt. budowy automatu wykonującego obliczenia wg. określonego algorytmu; co było podstawą rozwoju współczesnej informatyki
- złamanie Enigmy powinno być wyjątkową lekcją pokory dla projektantów i konstruktorów współczesnych urządzeń i systemów zabezpieczających;
- złamanie Enigmy pokazało też, że badania i certyfikacje urządzeń zabezpieczających są warunkiem koniecznym, ale nie zawsze wystarczającym do zbudowania skutecznych urządzeń i systemów zabezpieczających.

Dziękuję za uwagę
i proszę o pytania

XVI SEMINARIUM WEP

11 kwietnia 2018 r.