

DESZYFROWANIE DEPEszy

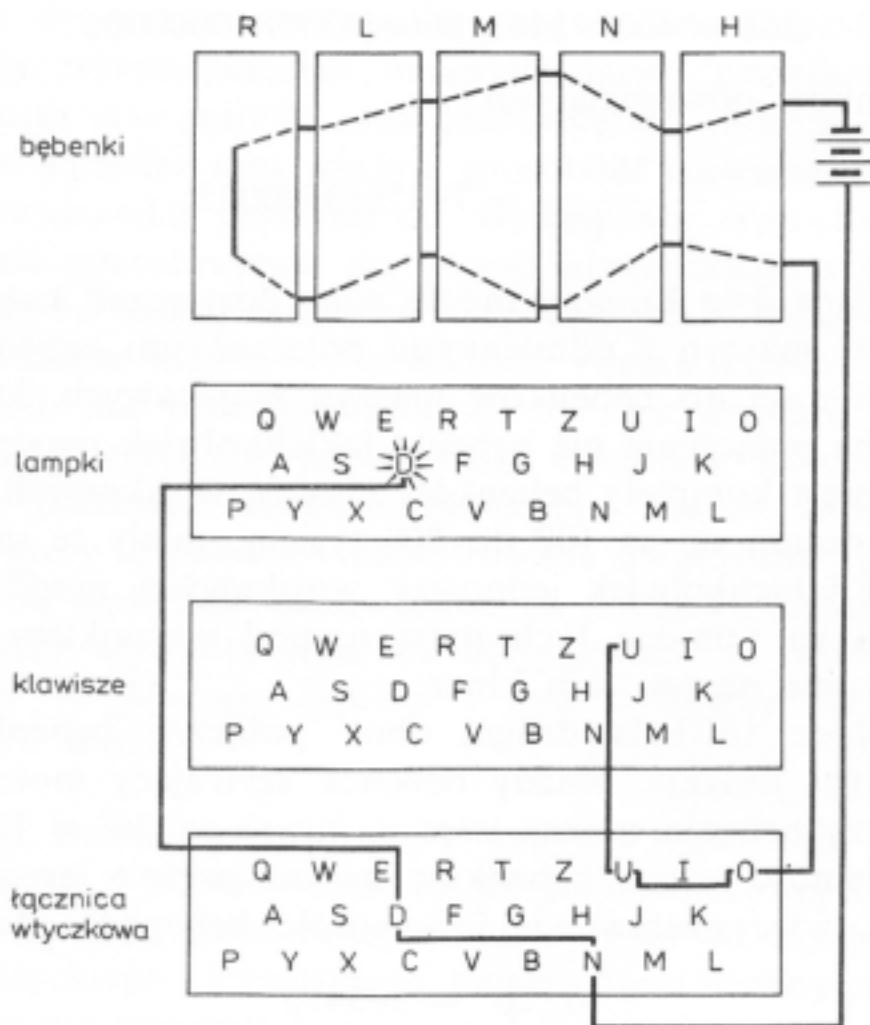
- Znając ustawienia szyfranta:

- pozycję wirników (II-III-I)
- ustawienia pierścieni(BCD)
- ustawienia wirników (SDK)

- Odszyfrowanie:



SCHEMAT PRZEBIEGU PRĄDU W ENIGMIE WOJSKOWEJ



ENIGMA A MATEMATYKA

DO ZŁAMANIA SZYFRU ENIGMY ZASTOSOWANO METODY MATEMATYCZNE

- Metody kombinatoryczne,
 - metody probabilistyczne,
 - a przede wszystkim **teorię permutacji**.
-
- Permutacja, to ciąg składający się ze skończonej liczby elementów.
 - Na przykład **trzy różne** elementy **a b c** możemy ustawić na
 $3! = 1 \times 2 \times 3 = 6$ sposobów (6 ciągów)
abc acb bac bca cab cba

ENIGMA. SŁÓW KILKA O LICZBACH

Budowa maszyny

- Ilość potencjalnych wirników szyfr.: $(26!)^3$
- Ilość potencjalnych walców wejściowych: $26!$
- Sposoby ustawienia trzech wirników szyfr.: $3!=6$
- Konfiguracja reflektora (wirnika odwracającego):
 $1*3*5*7*...*25$

Ustawienia bieżące

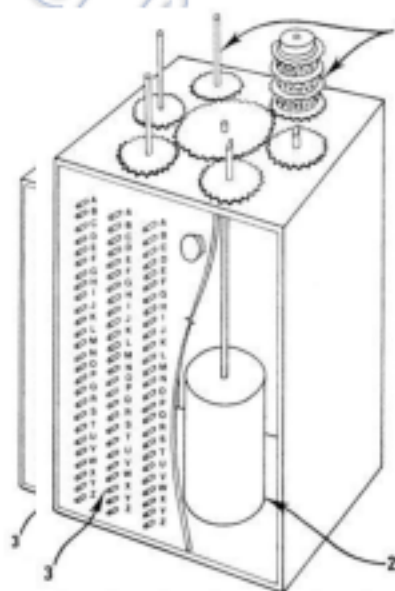
- Konfiguracje pierścieni: $26*26$
- Wybór ustawień wirników: $26*26*26$
- Wybór ustawień łącznicy: $26!/(14! * 2^{6*6}) = 100391791500$
- Łączna liczba możliwości : $3,06 * 10^{141}$

Uwaga! Znak ^ oznacza potęgowanie, znak * oznacza mnożenie.

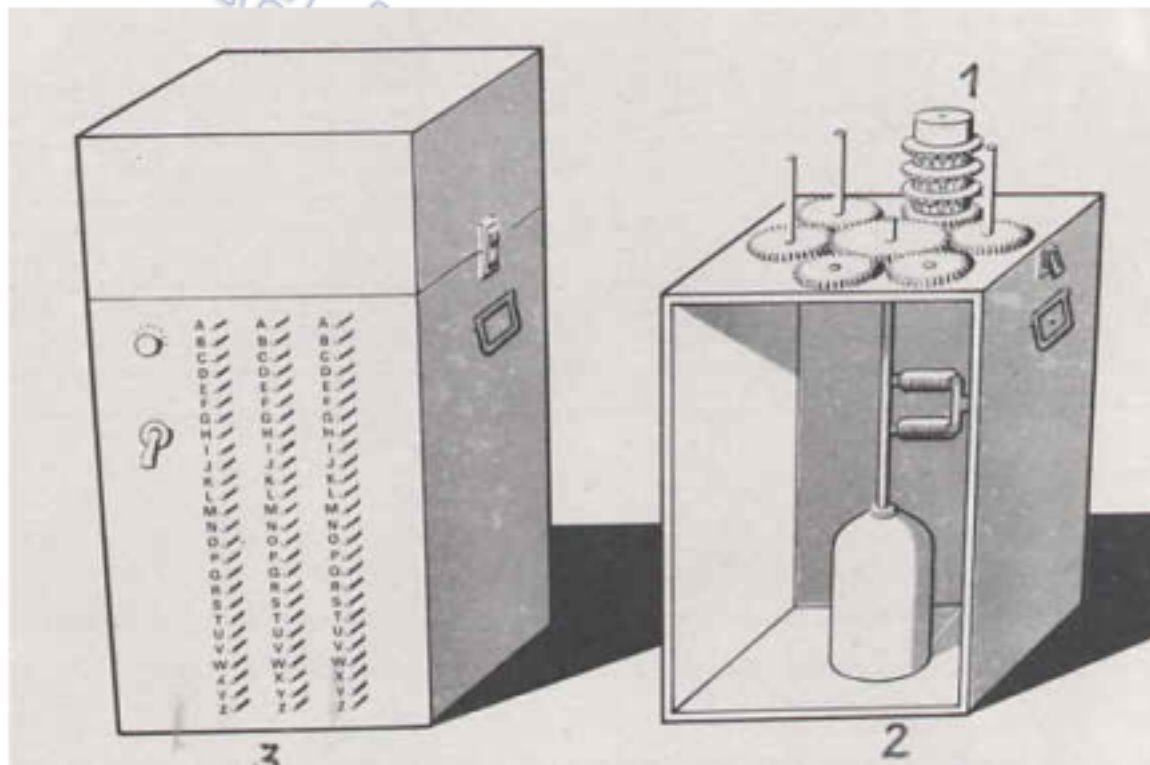
METODY POMOCNICZE W PRACY KRYPTOLOGÓW

- Metoda zegara (wybór i ustalanie wirnika szybkiego mechanizacja dekryptażu), **Różycki**)
- Metoda perforowanych płacht (wyznaczania ustawień pierścieni i kolejności wirników, **Zygalski**)
- Metoda rusztu, a następnie cyklometru (ustalanie połączeń łącznicy, **Rejewski**)

Bomby (przyspieszenie pracy,
Rejewski)



BOMBA KRYPTOLOGICZNA REJEWSKIEGO – przyspieszenie pracy

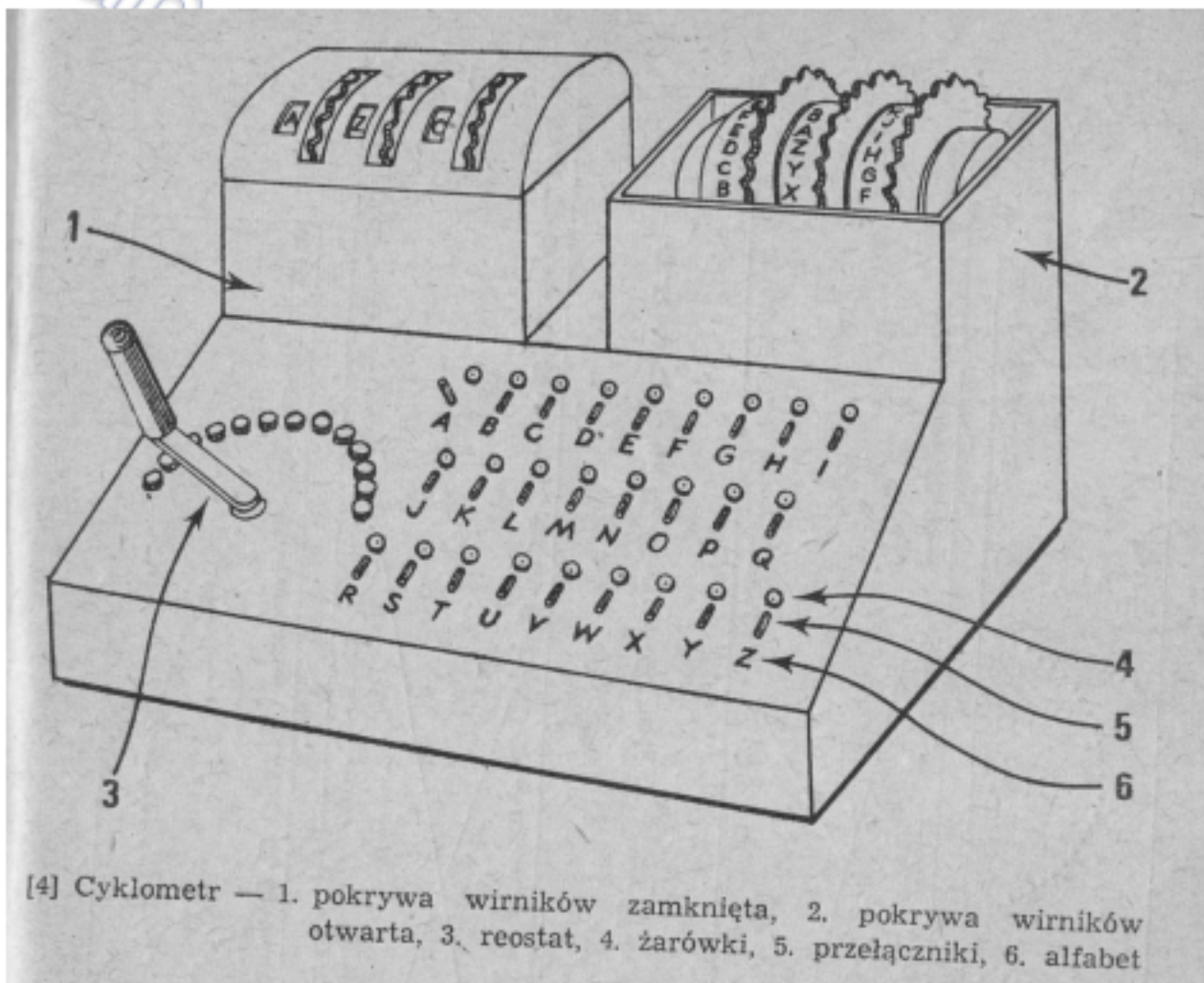


PŁACHTY ZYGALNE
PIERŚCIENI I K...

37

CYKLOMETR MARIANA REJEWSKIEGO.

ZNAJDOWANIE POŁĄCZEŃ WTYCZKOWYCH



PRZEKAZANIE ALIANTOM TAJEMNICY

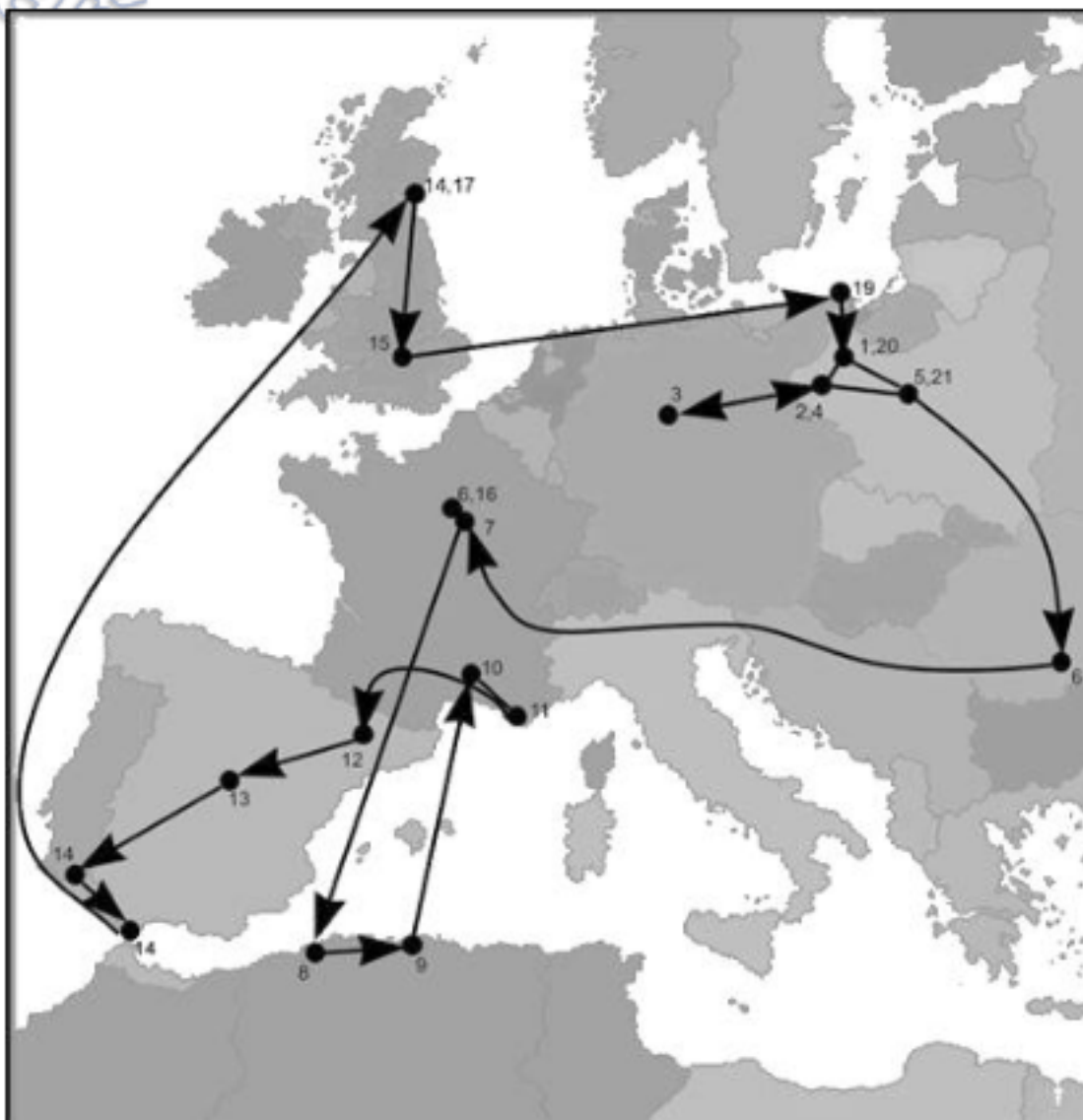
- **25-27 lipca 1939 roku** przekazano Francji i Anglii dorobek polskich kryptologów:
 - tajemnice związane z Enigmą,
 - posiadaną przez nich wiedzę i sprzęt.
- **Przekazano skonstruowane w Polsce**
 - kopie Enigmy oraz
 - materiały dotyczące metod pracy, czyli szyfrowania i rozszyfrowywania depeesz , m.in.
 - metodę bomb,
 - zegara,
 - płacht i inne.

BLECHLEY PARK, OŚRODEK DEKRYPTAŻU, Wielka Brytania



TRZEJ KRYPTOLODZY W CZASIE II WOJNY ŚWIATOWEJ, SZLAKIEM M. REJEWSKIEGO,

Różyckiego do 1942 (pkt. 2-9) i Zygalskiego do 1945 (pkt. 2-15)



TRZEJ KRYPTOLODZY, OD PRAWEJ:

MR, JR, HZ; POŁUDNIOWA FRANCJA, 1941



LOSY MARIANA REJEWSKIEGO

PO II WOJNIE ŚWIATOWEJ

- 1945-1946 Szkocja, kurs techniki wywiadu,
- 1946 – 1967, Bydgoszcz,
- praca:
 - kierownik sekcji sprzedaży, kierownik referatu ogólnego, referenta finansowego, starszy księgowy, instruktor księgowości**
- firmy:
 - Kabel Polski, Państwowe Przedsiębiorstwo Miernicze; Związek Spółdzielni Rzemieślniczych; Wojewódzki Związek Spółdzielni Pracy;
- **cały czas – miał nadzór policji politycznej.**

LOSY MARIANA REJEWSKIEGO

PO II WOJNIE ŚWIATOWEJ, CD

- **1967** Kończy opracowanie „*Wspomnienia...*”, przesyła je do Wojskowego Instytutu Historycznego w Warszawie,
- 1969 – 1980, Warszawa,
- **1973** – książka francuskiego generała **Gustave’a Bertranda**, **MR po raz pierwszy publicznie ujawnił charakter swej przedwojennej i wojennej pracy,**
- **1974** pisze Uzupełnienie „*Wspomnień...*”, prace wspomnieniowo-dokumentacyjne, związane z polskim wkładem w pokonanie Enigmy,
- **1980** **umiera** na zawał serca, pochowany na warszawskich Powązkach w asyście kompanii honorowej Wojska Polskiego na Cmentarzu Wojskowym.

LOSY MARIANA REJEWSKIEGO

PO II WOJNIE ŚWIATOWEJ, CD

- **1978** Krzyż Oficerski Orderu Odrodzenia Polski,
- **1979** Srebrny Medal za Zasługi dla Obronności Kraju,
- **1979** Członek Honorowy Polskiego Towarzystwa Matematycznego,
- **1948** Medal Wojenny 1939-1945 (The War Medal 1939-1945),
- **2000** Krzyż Wielki Orderu Odrodzenia Polski (wręczył rodzinom kryptologów premier Jerzy Buzek).

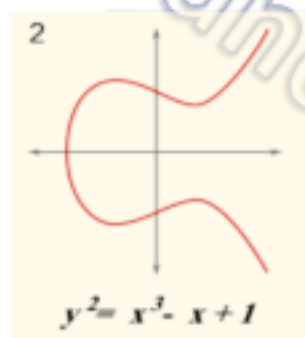
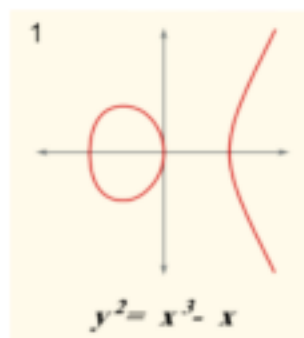
LOSY HENRYKA ZYGALSKIEGO PO II WOJNIE ŚWIATOWEJ

- Został w Londynie, do 1948 służył w armii,
- **1948-1950** powtórzył studia matematyczne w Imperial College of Technology,
- **do 1978** wykładał matematykę w Polish University College, University of Surrey,
- **1977** Polski Uniwersytet na Obczyźnie w Londynie przyznał mu tytuł doktora honoris causa w zakresie nauk matematycznych i historii naturalnej,
- **1978** zmarł w Liss koło Portsmouth, grób cmentarz Greenwood Father Commons w Liss.

KRYPTOLOGIA NA WMI UAM

Nowoczesne badania z kryptologii aktualnie oparte są na dziedzinach:

*algebra, teoria liczb, geometria algebraiczna,
teoria algorytmów, matematyka dyskretna,
krzywe eliptyczne, podpisy cyfrowe.*



Z tych dziedzin prowadzimy:

- o zajęcia dla studentów,
- o badania naukowe,
- o prace magisterskie i doktorskie,
- o organizujemy międzynarodowe konferencje z kryptologii.

PAMIĘĆ O TRZECH KRYPTOLOGACH

TABLICA W COL. MINUS UAM





**Collegium Minus UAM,
odsłonięcie tablicy
pamiątkowej,
20.11.1983**

**Od prawej: Rektor UAM
prof. Zbigniew
Radwański,**

**Monika Kruś
siostra H. Zygałskiego,**

**Barbara Różycka,
żona J. Różyckiego**

PO TABLICA W LESIE KABACKIM

NA TERENIE TEGO OBIEKTU W LATACH 1936-1939
PRACOWALI WYBITNI POLSCY MATEMATYCY-KRYPTOLODZY



MARIAN REJEWSKI
JERZY RÓŻYCKI
HENRYK ZYGALSKI

KTÓRZY DOKONALI ZŁAMANIA KODU NIEMIECKIEJ MASZYNY SZYFRUJĄCEJ
„ENIGMA”

OSIĄGNIĘCIE TO STAŁO SIĘ ISTOTNYM WKŁADEM POLSKI
W ZWYCIĘSTWO SPRZYMIERZONYCH
W II WOJNIE ŚWIATOWEJ

WARSZAWA OL 10. 1999 R.

TABLICE UFUNDOWANO Z INICJATYWY
ŻOŁNIERZY I PRACOWNIKÓW
CENTRALNEGO STANOWISKA DOWODZENIA



PAMIĘĆ O KRYPTOLOGACH, HENRYK ZYGALSKI, POZNAŃ



75 LAT ZŁAMANIA SZYFRU ENIGMY, 2007: mennica monety 2 zł, 10, zł, 100 zł

Monety emisji 2007

Monety emisji 2007

Narodowy Bank Polski



nominał	100 zł
metal	900/1000Au
stempel	lustrzany
średnica	21,00 mm
masa	8,00 g
wielkość emisji (nakład)	8.000 szt.

Awers: Centralnie, wizerunek orla ustalony dla godła Rzeczypospolitej Polskiej. W tle tabele literowo oraz kartasowo zaznaczony ideowy schemat działania maszyny szyfrującej Enigma. W otoku napis: RZECZPOSPOLITA POLSKA, oznaczenie roku emisji: 2007 oraz napis: 100 ZŁ. Pod lewą łapą orla znak mennicy: .

Rewers: Z lewej i z prawej strony stylizowane żarówki z maszyny szyfrującej Enigma. Wokół nich dwa zbiory okręgów odzwierciedlających promienie światła. U góry w trzech rzędach litery alfabetu połączone liniami z dwoma rzędami liter znajdującymi się poniżej. Pod żarówkami napis: 75. ROCZNICA ZŁAMANIA SZYFRU ENIGMY.



nominał	10 zł
metal	925/1000 Ag
stempel	lustrzany
średnica	32,00 mm
masa	14,14 g
wielkość emisji (nakład)	52.000 szt.

Awers: Wizerunek orla ustalony dla godła Rzeczypospolitej Polskiej, nad orłem napis: RZECZPOSPOLITA POLSKA. W tle stylizowany schemat działania maszyny szyfrującej Enigma oraz wytłaczający się z kompozycji linii stylizowany napis: ENIGMA. Pod schematem z lewej strony oznaczenie roku emisji: 2007. U dołu napis: 10 ZŁ. Pod lewą łapą orla znak mennicy: .

Rewers: Umowny labirynt połączeń nawiązujący do działania maszyny szyfrującej Enigma. W środku napis: ENIGMA. Pod nim napis: 1932 odwrócony o 180 stopni. W otoku napis: 75. ROCZNICA ZŁAMANIA SZYFRU ENIGMY.

Na boku: napis MARIAN REJEWSKI, HENRYK ZYGALSKI, JERZY RÓŻYCKI, rozdzielony gwiazdkami.



nominał	2 zł
metal	stop CuAl5Zn55n1
stempel	zwykły
średnica	27,00 mm
masa	8,15 g
wielkość emisji (nakład)	900.000 szt.

Awers: Wizerunek orla ustalony dla godła Rzeczypospolitej Polskiej, po bokach orla oznaczenie roku emisji: 20-07, pod orłem napis: 2 ZŁ, w otoku napis: RZECZPOSPOLITA POLSKA, poprzedzony oraz zakończony sześcioma perełkami. Pod lewą łapą orla znak mennicy: .

Rewers: Stylizowane koło wienka szyfrującego Enigma. Na obwodzie w kółkach napis: REJEWSKI RÓŻYCKI ZYGALSKI. Wokół środka napis: 75. ROCZNICA ZŁAMANIA SZYFRU ENIGMY.

Na boku: Ośmiokrotnie powtórzony napis: NBP, co drugi odwrócony o 180 stopni, rozdzielony gwiazdkami.

Projektant monet: Ewa Tyc-Karpińska

Informacje o sposobie nabycia monet na stronie:
www.nbp.pl

Monety zostały wyprodukowane w Mennicy Polskiej SA
w Warszawie.

Skład i druk: Drukarnia NBP

Monety

75. rocznica złamania szyfru Enigmy

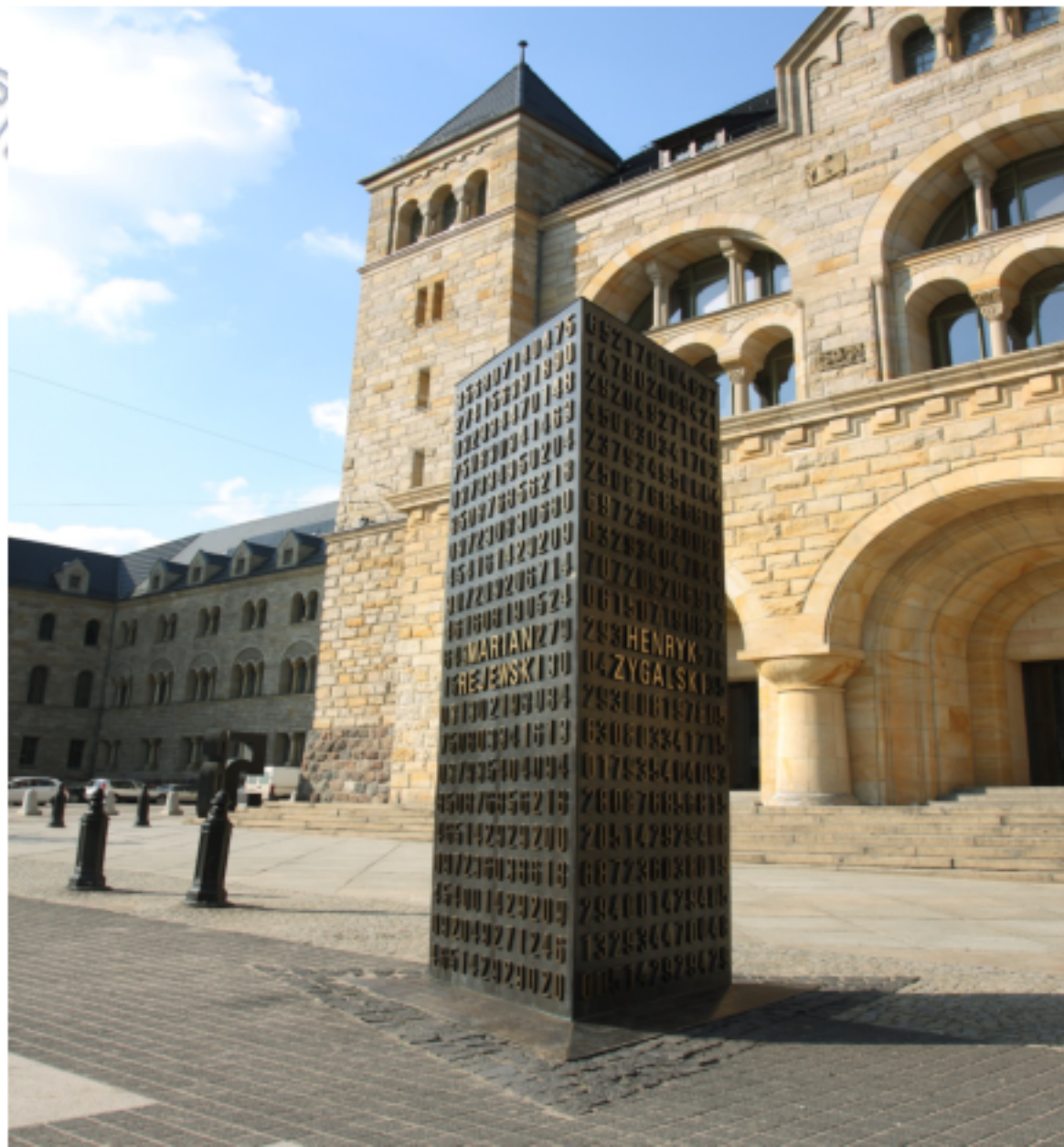


POMNIK MARIANA REJEWSKIEGO W BYDGOSZCZY, UL. GDAŃSKA



PAMIĘĆ O TRZECH KRYPTOLOGACH

POMNIK PRZED ZAMKIEM W POZNANIU



WYSTAWA: ENIGMA. ODSZYFROWAĆ ZWYCIĘSTWO, 17.10.2012, SENAT RP



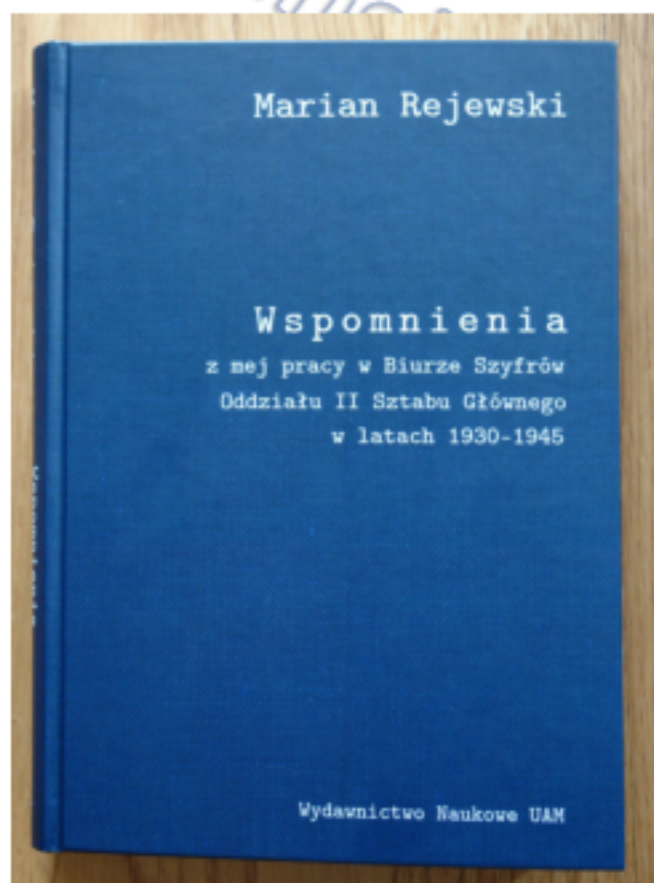
KSIĄŻKA DWUJĘZYCZNA:

MARIAN REJEWSKI *WSPOMNIENIA...*

Marian Rejewski

*Wspomnienia
z mej pracy w Biurze Szyfrów
Oddziału II Sztabu Głównego
w latach 1930 – 1945*

Wydawnictwo Naukowe
Uniwersytetu
im. Adama Mickiewicza
Poznań 2011



STRONA REDAKCYJNA POLSKIEJ CZĘŚCI KSIĄŻKI

Opracowanie i redakcja:

*Magdalena Jaroszevska z zespołem:
Marek Grajek, Jerzy Jaworski, Tomasz Kubiak*

Przypisy: *Marek Grajek, Jerzy Kaczorowski*

Skład i łamanie: *Paweł Mleczo*

Projekt okładki:

Katarzyna Rybarczyk-Krzywdzińska

Redaktor techniczny

Elżbieta Rygielska

Translated by

*Antoni Józef Bohdanowicz,
Bogusława Whyatt, Chris Whyatt*

Książka obejmuje:

**Wspomnienia, Uzupełnienie, Przypisy, Fotografie,
Dokumenty,...**

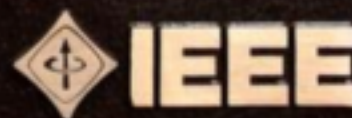
**ODZNACZENIE MILESTONE
TABLICA PAMIĄTKOWA, 2014
NA UL. ŚNIADECKICH 8 W WARSZAWIE
PRZED INSTYTUTEM MATEMATYCZNYM PAN**

Odznaczenie IEEE - "Kamień milowy" w rozwoju
inżynierii elektrycznej i obliczeniowej

Złamanie po raz pierwszy kodów Enigmy przez zespół
matematyków z polskiego Biura Szyfrów w latach 1932-1939

Polscy matematycy Marian Rejewski, Jerzy Różycki i Henryk Zygalski z krajowego Biura Szyfrów złamali kody maszyny szyfrującej Enigma. Pracując razem z inżynierami fabryki AVA w Warszawie zbudowali „bombę” – pierwszą maszynę deszyfrującą kody Enigmy. Ich osiągnięcia były podstawą do dalszych prac Brytyjczyków nad deszyfracją, które w okresie późniejszym z pomocą Amerykanów, przyczyniły się do zakończenia II-giej Wojny Światowej.

Sierpień 2014r



ODZNACZENIE MILESTONE DLA POLSKICH MATEMATYKÓW



**MEDAL UAM ALUMNO BENE MERENTI
DLA TRZECZ KRYPTOLOGÓW, 2018**



MEDAL UAM ALUMNO BENE MERENTI DLA KRYPTOLOGÓW, 2018, ODEBRAŁY RODZINY



ZNACZENIE ZŁAMANIA ENIGMY



ZNACZENIE ZŁAMANIA ENIGMY, CD

Znaczący wkład Polaków
do szybszego zwycięstwa aliantów
w II wojnie światowej,
skrócenie wojny o 2-3 lata,
ocalenie wielu istnień ludzkich!

Prezentacja:

KRYPTOLODZY Z UNIWERSYTETU POZNAŃSKIEGO I NIEMIECKA MASZYNA SZYFRUJĄCA ENIGMA

- o Autorzy opracowania:

Magdalena Jaroszevska, Bartosz Naskręcki,

opracowanie Notatek: Magdalena Jaroszevska

- o Źródła:

- o informacji wykorzystanych do prezentacji,

- o kolejnych slajdów

- o Notatek do poszczególnych slajdów

Znajdują się w oddzielnym pliku.

*„Jeszcze wiele mam wam do powiedzenia,
ale teraz nie możecie tego znieść.”*

św. Jan 16:12–15