



KRYPTOLOGIA

dr inż. Jacek Czerniak

jczerniak@ukw.edu.pl

MECHNICZNA MASZYNA SZYFRUJĄCA ENIGMA

dr inż. Jacek Czerniak

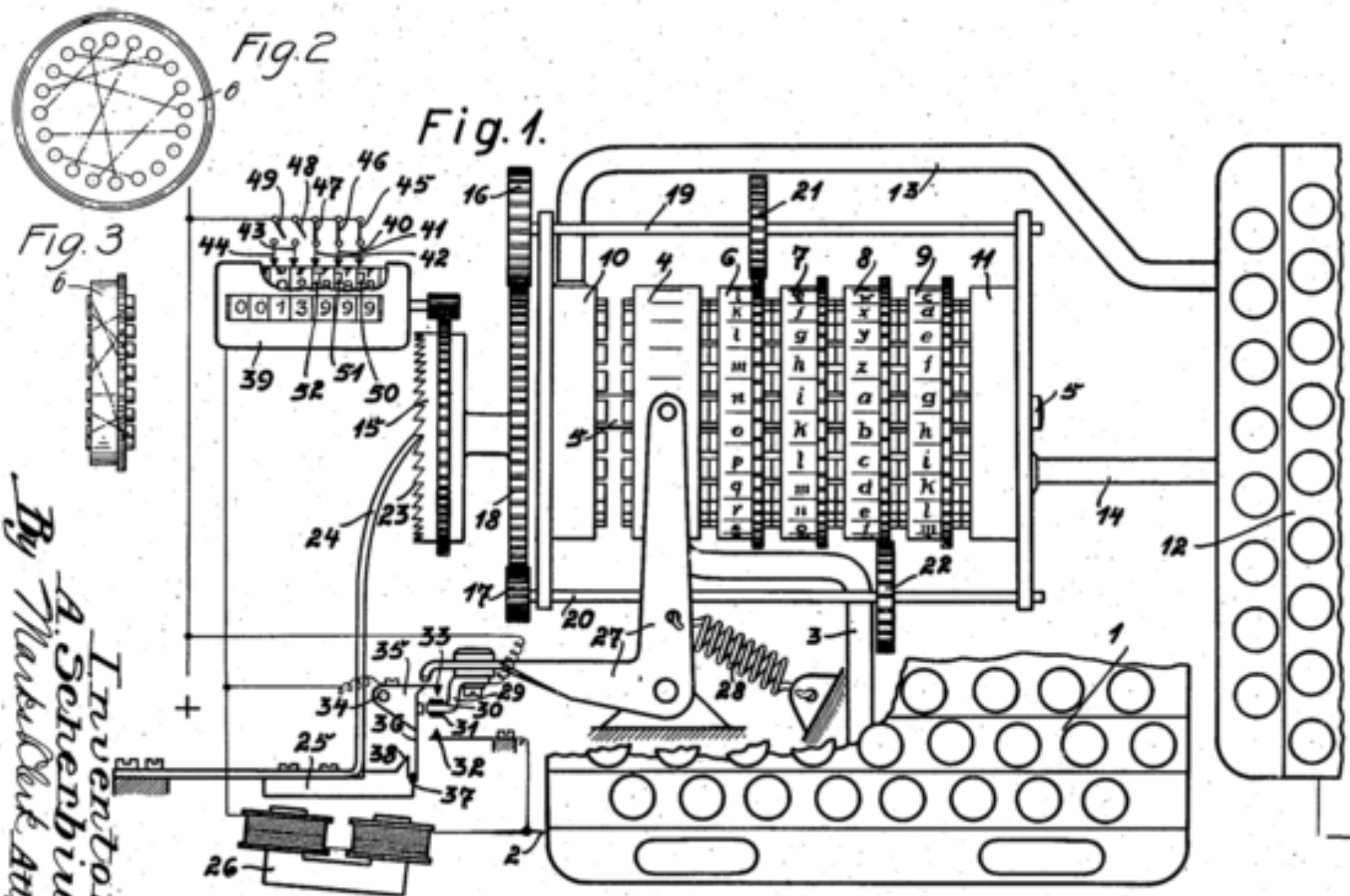


Jan. 24, 1928.

A. SCHERBIUS

1,657,411

CIPHERING MACHINE
Filed Feb. 6, 1923



Inventor
A. Scherbius,
By Mark DeL. Atty.

WERSJE ENIGMY

- Enigma (handlowa)



- Enigma G - 1926r.



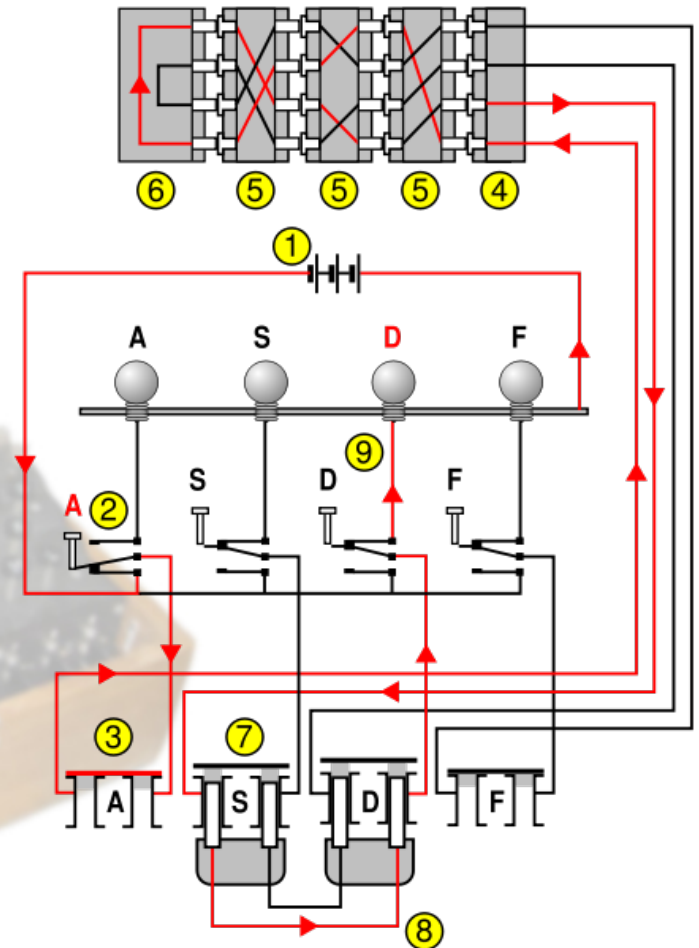
WERSJE ENIGMY

- Enigma Eins (E Eins) -1930r.
- Enigma M4 - 1939r.



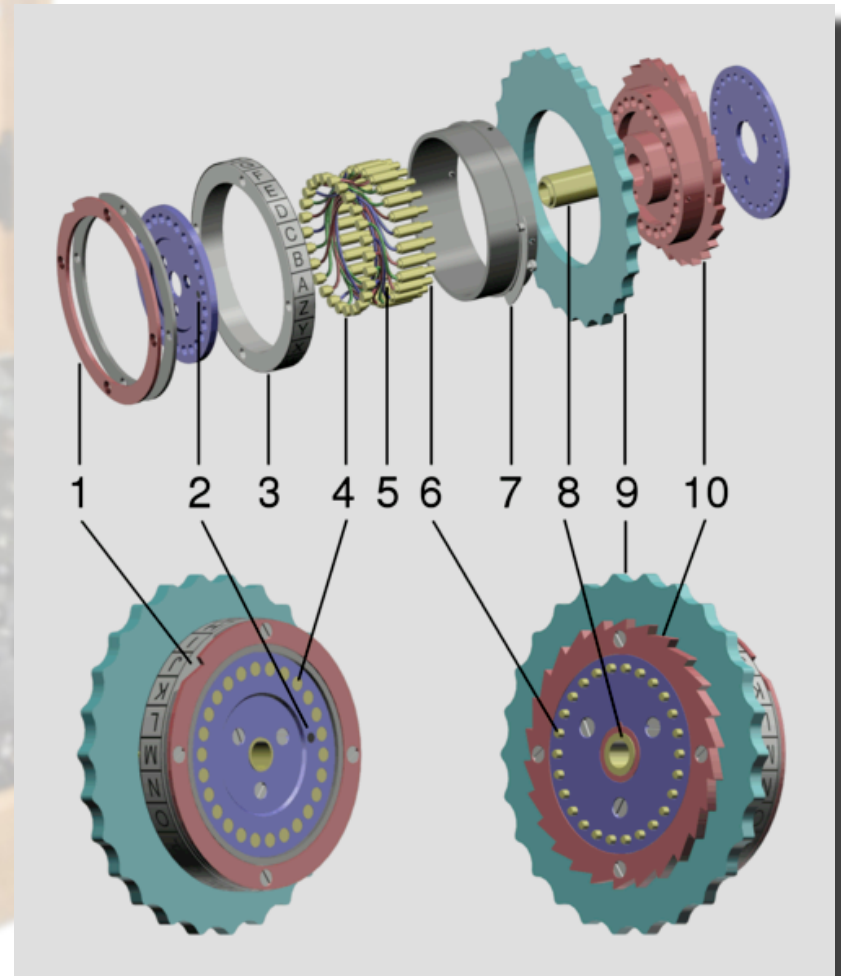
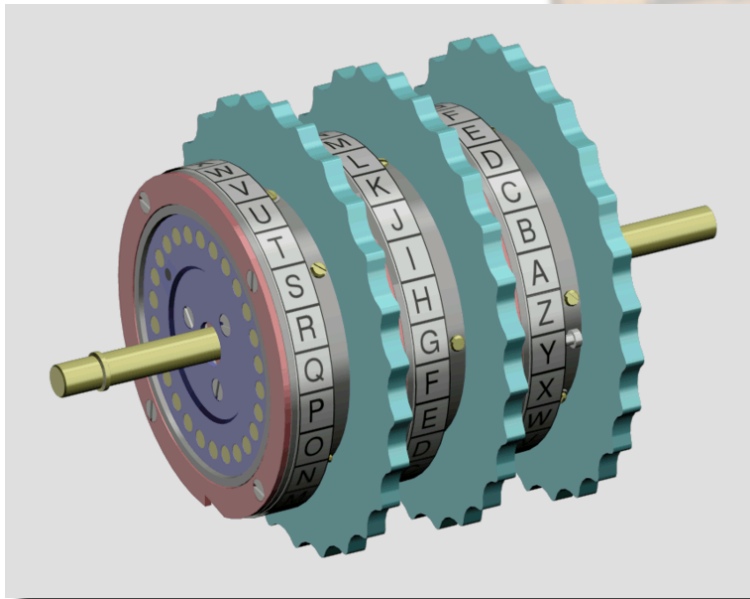
BUDOWA ENIGMY

- ENIGMA klawiatura
- ENIGMA lampki oświetleniowe
- ENIGMA zestaw bębneków
- ENIGMA łącznica
- ENIGMA bateria zasilająca
- ENIGMA mechanizm obrotowy



BUDOWA ENIGMY

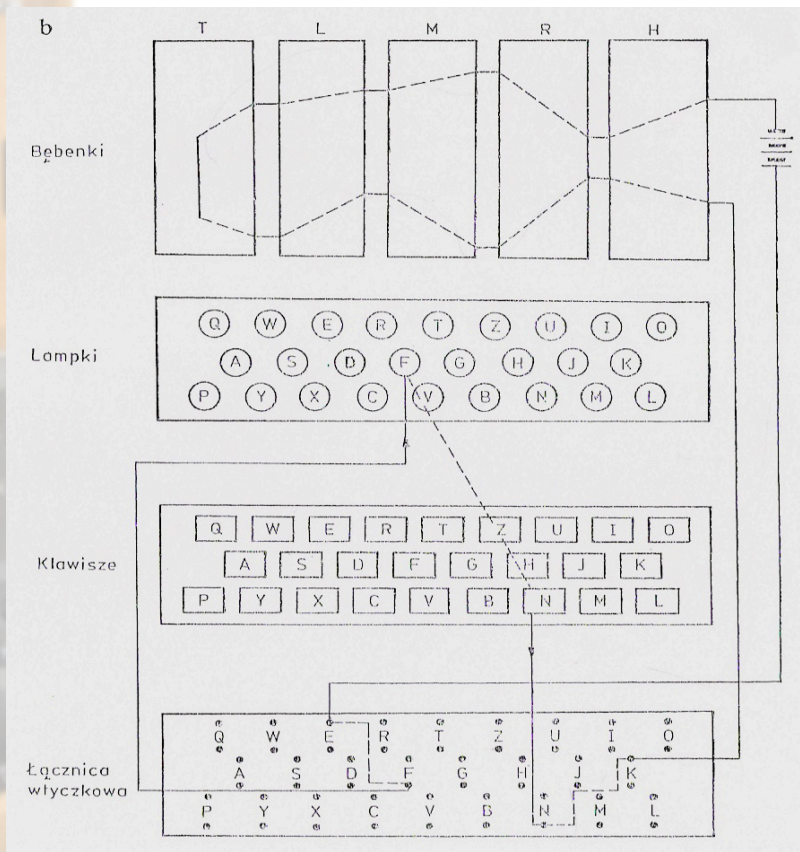
Budowa wirników szyfrujących



ZASADA SZYFROWANIA

KONFIGURACJA KLUCZA DZIENNEGO

- Numery aktualnie zainstalowanych bębneków
- Pozycje obręczy
- Położenia bębneków
- Liczba połączeń łącznicy i ich konfiguracja



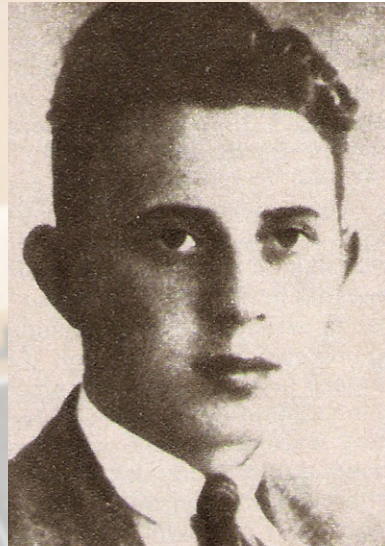
OBWÓD PRĄDU:

KLAWIATURA - ŁĄCZNICA - BĘBENEK WST. - BĘBENKI RML
- BĘBENEK ODW. - BEBENKI LMR - ŁĄCZNICA - TABLICA

10.12.2013

Kryptologia wprowadzenie UKW

SYLWETKI KRYPTOLOGÓW



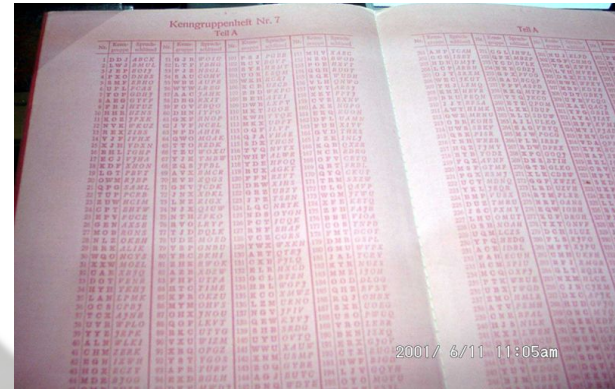
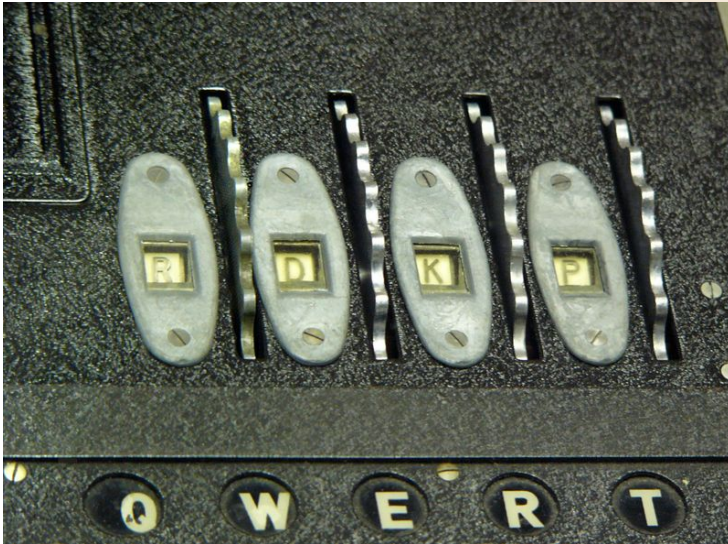
Styczeń 1929r. - kurs kryptologii

Jesień 1930r. - filia BS w Poznaniu

Wrzesień 1932r. - praca w BS4 w Warszawie
i początek prac nad szyfrem Enigmy

Grudzień 1932r. - złamanie kodu Enigmy

KLUCZ- definicja



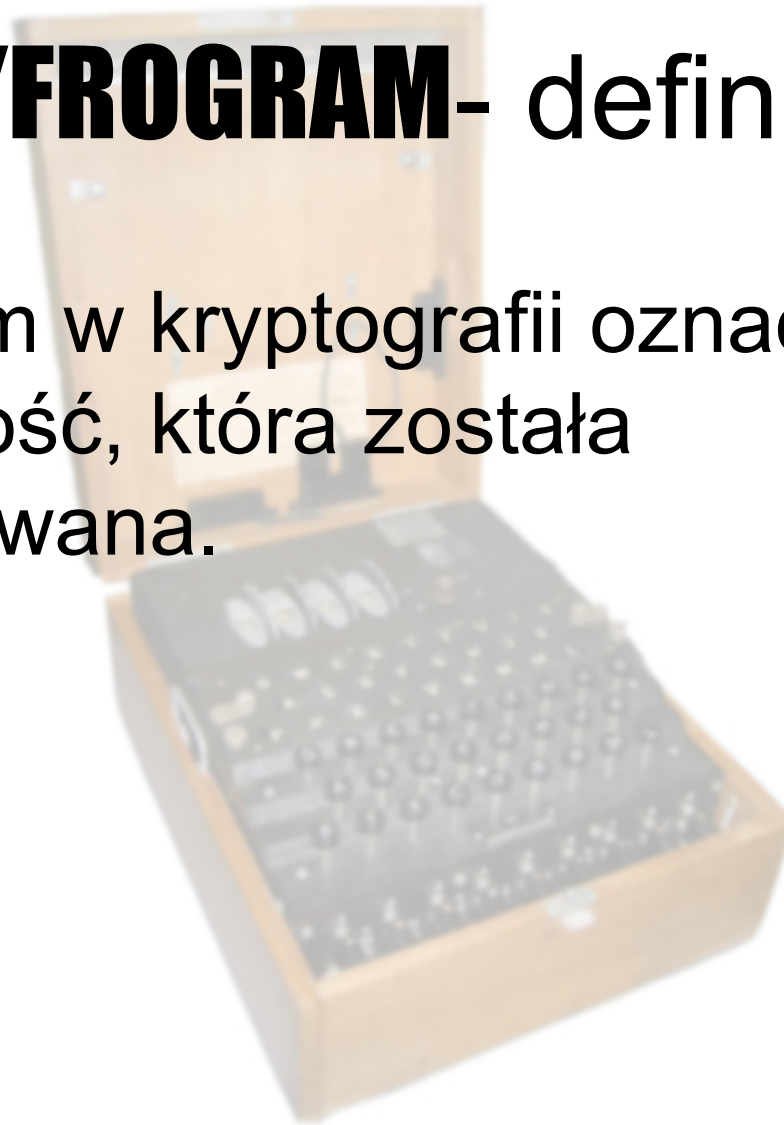
Klucz (ang. key) – w kryptografii informacja umożliwiająca wykonywanie pewnej czynności kryptograficznej – szyfrowania, deszyfrowania, podpisywania, weryfikacji podpisu itp.

SZYFR- definicja

- Szyfr to procedura takiego przekształcania wiadomości, żeby była ona niemożliwa (lub bardzo trudna) do odczytania przez każdego, kto nie posiada odpowiedniego klucza.
- Wiadomość przed zaszyfrowaniem nazywa się tekstem jawnym (*plaintext*), a wiadomość zaszyfrowaną – szyfrogramem (*ciphertext*). Jako ciekawostkę można podać, że Marian Rejewski używa w swoich pracach określeń **kler** na tekst jawny i **krypt** na tekst tajny.
- Szyfrowanie jest zajęciem bardzo starym, aczkolwiek nowoczesna kryptografia narodziła się dopiero w epoce komputerów i starsze szyfry są z dzisiejszego punktu widzenia zupełnie bezużyteczne.

SZYFROGRAM- definicja

Szyfrogram w kryptografii oznacza wiadomość, która została zaszyfrowana.



KRYPTOLOGIA- definicja



- Kryptologia (z gr. *kryptós* "ukryty", *logos* "słowo") to nauka zajmująca się układaniem. Wyróżniane są dwa główne działy kryptologii:
 - * Kryptografia
 - * Kryptoanaliza

KRYPTOGRAFIA- definicja

- Kryptografia (z gr. *kryptós* "ukryty", *gráphein* "pisać") to nauka zajmująca się układaniem szyfrów. Wyróżniane są dwa główne nurty kryptografii:
 - * Kryptografia symetryczna
 - * Kryptografia asymetryczna

Kryptografia symetryczna

W kryptografii symetrycznej klucz służy do szyfrowania i deszyfrowania wiadomości. Do obu tych czynności używa się tego samego klucza, dlatego powinien być znany tylko uczestnikom. Taki klucz jest przypisany do danej komunikacji, nie do posiadacza, dlatego zwykle do każdego połączenia jest generowany nowy klucz. Może do tego służyć np. (oparty na kryptografii asymetrycznej) protokół Diffiego-Hellmana.

Kryptografia asymetryczna

W kryptosystemach asymetrycznych wyróżniamy klucz publiczny oraz prywatny. Ten pierwszy może być zupełnie jawny, drugi powinien znać tylko właściciel. Matematyczna konstrukcja kluczy powinna być taka, żeby wygenerowanie prywatnego na podstawie publicznego było jak najtrudniejsze obliczeniowo. Zależnie od kryptosystemu, wygenerowanie klucza publicznego na podstawie prywatnego również może być trudne (RSA), lub trywialne (ElGamal).

C.D.N.

Dziękuję za uwagę



jczerniak@ukw.edu.pl