# Matematyczna podróż w głąb Enigmy

Przemysław Biecek[1] Teresa Jurlewicz[2]

[1] IM PAN, BioTech UWr, [2] IMiI PWr

22 lutego 2008

# Szyfr Skytale

Skytale to jedna z najstarszych metod szyfrowania. Używana w starożytnej Grecji, głównie przez Spartan.
Na laskę nawijano pasek pergaminu, na którym pisano tekst na stykających się brzegach, tak jak to pokazano na rysunku.
Aby odczytać tekst należało posiadać laskę o identycznej grubości.

# Szyfr Cezara

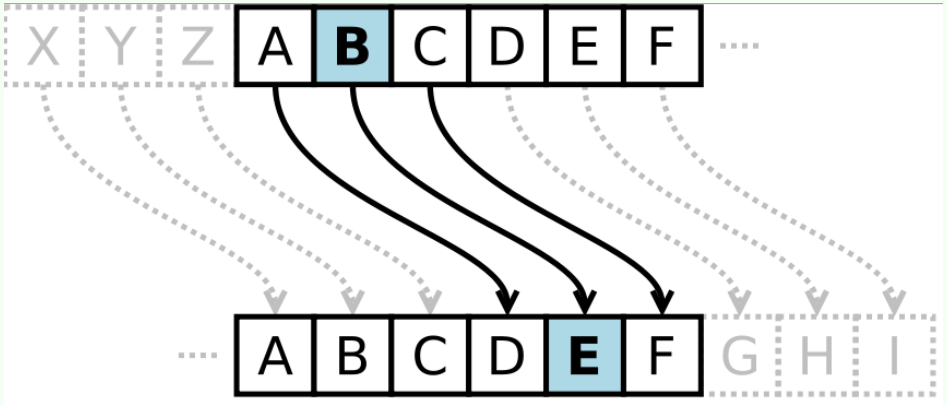
Jeden z najpopularniejsych szyfrów podstawieniowych.
Nazwa pochodzi od Juliusza Cezara, który szyfrował nim swoją korespondencję z Cyceronem.

| | |
|---|---|
| Tekst jawny: | ABCDEFGHIJKLMNOPQRSTUVWXYZ |
| Szyfrogram: | DEFGHIJKLMNOPQRSTUVWXYZABC |

| | |
|---|---|
| Tekst jawny: | Olimpijczycy |
| Szyfrogram: | Rolpslmfcbfb |

# Szyfr Cezara

Szyfrowanie




$$E_n(x) = (x + n) \mod 26$$

Deszyfrowanie

$$D_n(x) = (x - n) \mod 26$$

Gdzie $n$ oznacza parametr przesunięcia (oryginalnie =3), a $x$ to indeks szyfrowanej litery w alfabecie łacińskim.

# Szyfr Cezara

Przed Cezarem, jego adoptowany syn, Oktawian August, używał szyfru z przesunięciem 1.
Pierwsze udokumentowane techniki złamania szyfru Cezara pochodzą z IX wieku (w tym czasie Arabowie odkryli analizę częstościową).
Wraz z odkryciem tej techniki szyfr Cezara utracił swoją praktyczną wartość.

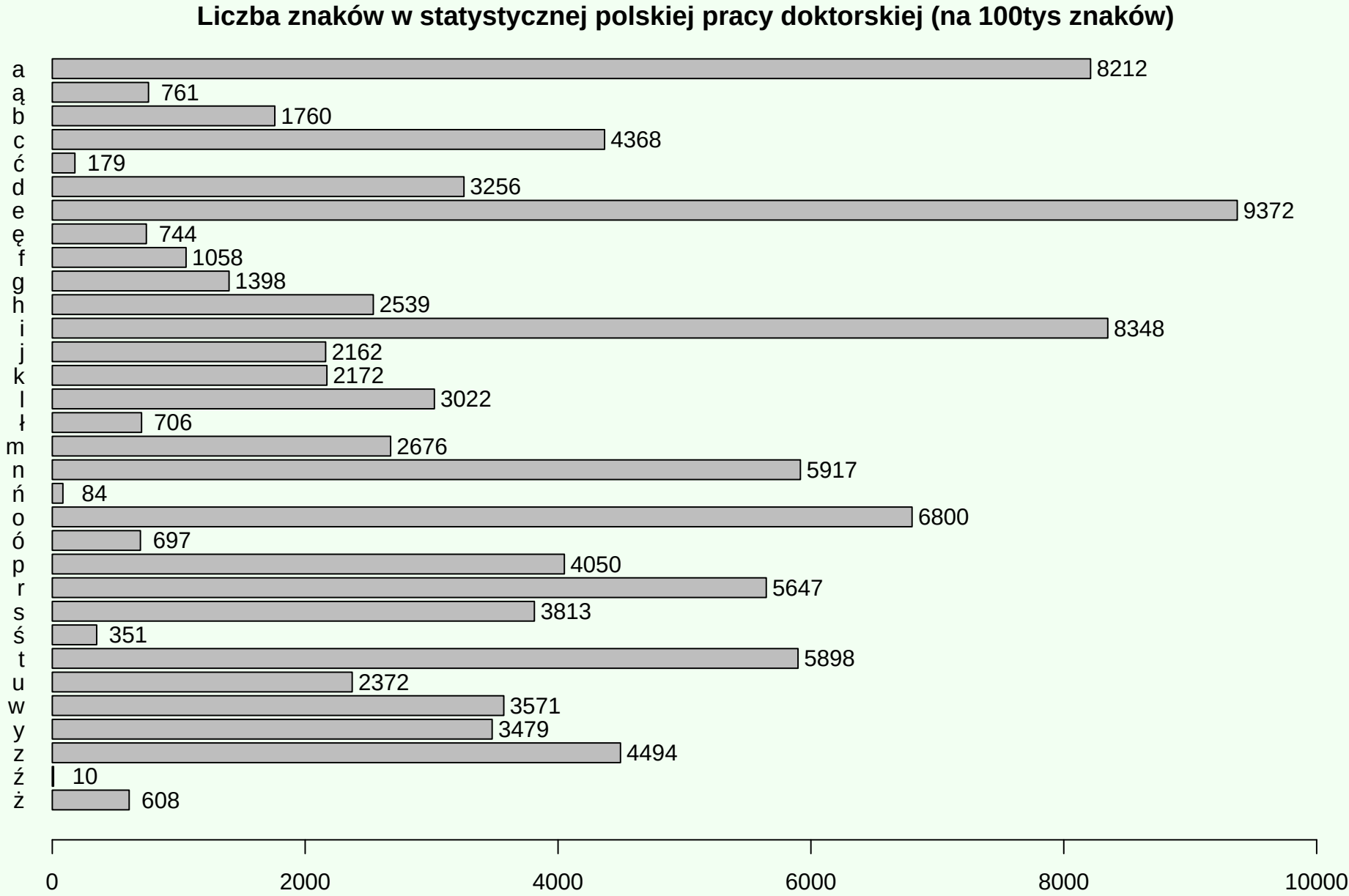
## Wersja ROT13

Najpopularniejsza w Internecie wersja szyfru Cezara wykorzystuje przesunięcie o 13 znaków (szyfr symetryczny). Znaki niełacińskie nie są kodowane.

# Gaderypoluki

Gaderypoluki to rodzaju symetrycznego szyfru podstawieniowego stosowanego w harcerstwie do kodowania krótkich wiadomości. Szyfrowanie jest oparte na krótkim, łatwym do zapamiętania kluczu. Klucz ten zapisuje się w formie ciągu par liter które w kodowanym tekście są ze sobą zamieniane. Najczęściej stosowany klucz to „GA-DE-RY-PO-LU-KI", skąd pochodzi nazwa szyfru. Litery, których nie ma liście zamienników, pozostawia się w szyfrowanym tekście bez zmian.

| | |
|---|---|
| tekst jawny: | Olimpijczycy |
| klucz: | GA-DE-RY-PO-LU-KI |
| tekst zaszyfrowany: | Pukmokjczrcr |


Liczba znaków w statystycznej polskiej pracy doktorskiej (na 100tys znaków)
a 8212
ą 761
b 1760
c 4368
ć 179
d 3256
e 9372
ę 744
f 1058
g 1398
h 2539
i 8348
j 2162
k 2172
l 3022
ł 706
m 2676
n 5917
ń 84
o 6800
ó 697
p 4050
r 5647
s 3813
ś 351
t 5898
u 2372
w 3571
y 3479
z 4494
ź 10
ż 608
0
2000
4000
6000
8000
10000

# Szyfr Vigenere'a (złamany w wieku XVIII)

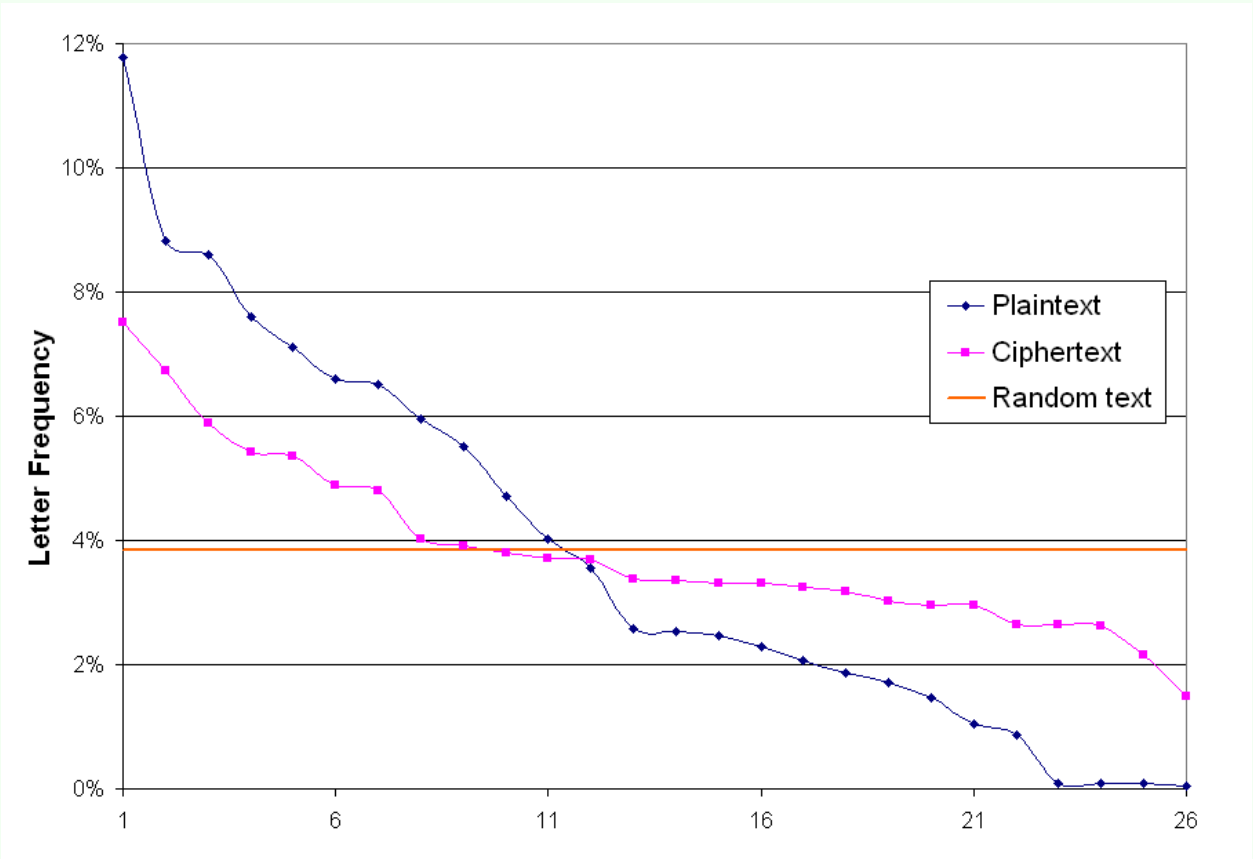
Szyfr Vigenere'a to szyfr podstawieniowy o zmiennej tablicy podstawień.
Wykorzystywany jest autoklucz, pierwsza litera (np. N) jest tajna, pozostałe są kolejnymi literami tekstu jawnego.

| | |
|---|---|
| tekst jawny: | TO JEST BARDZO TAJNY TEKST |
| klucz: | NT OJES TBARDZ OTAJN YTEKS |
| tekst zaszyfrowany: | GH XNWL UBRUCN HTJWL RXOCL |

| | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A |
| C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B |
| D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C |
| E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D |
| F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E |
| G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F |
| N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M |

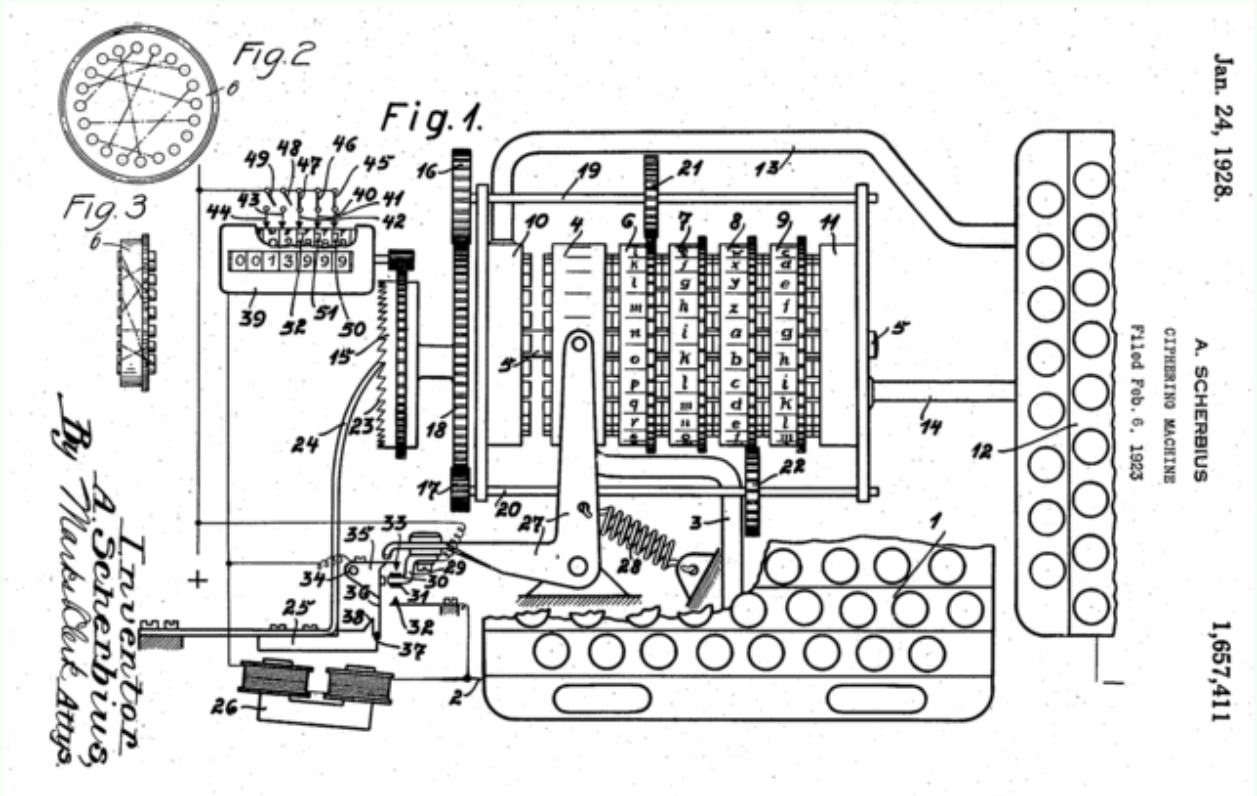
# Szyfr Vigenere'a (złamany w wieku XVIII)

Ten szyfr również można złamać analizą częstościową.
Należy analizować częstość występowania par znaków.



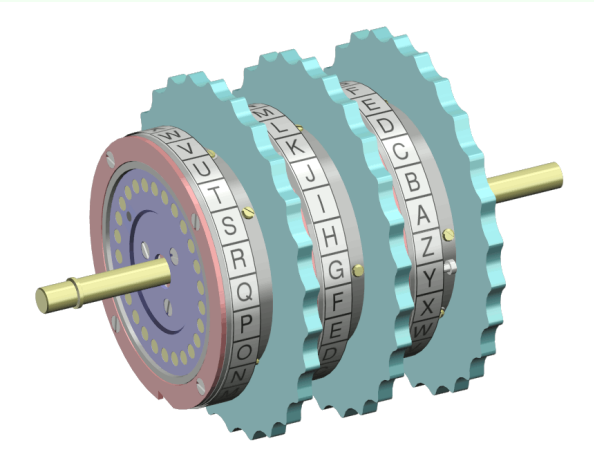
# Budowa Enigmy

Hugo Koch zaprojektował maszynę szyfrującą, ze zmiennym szyfrem podstawieniowym innym dla każdego znaku. Komercyjna wersja była sprzedawana przez Scherbius & Ritter od 1918 roku.



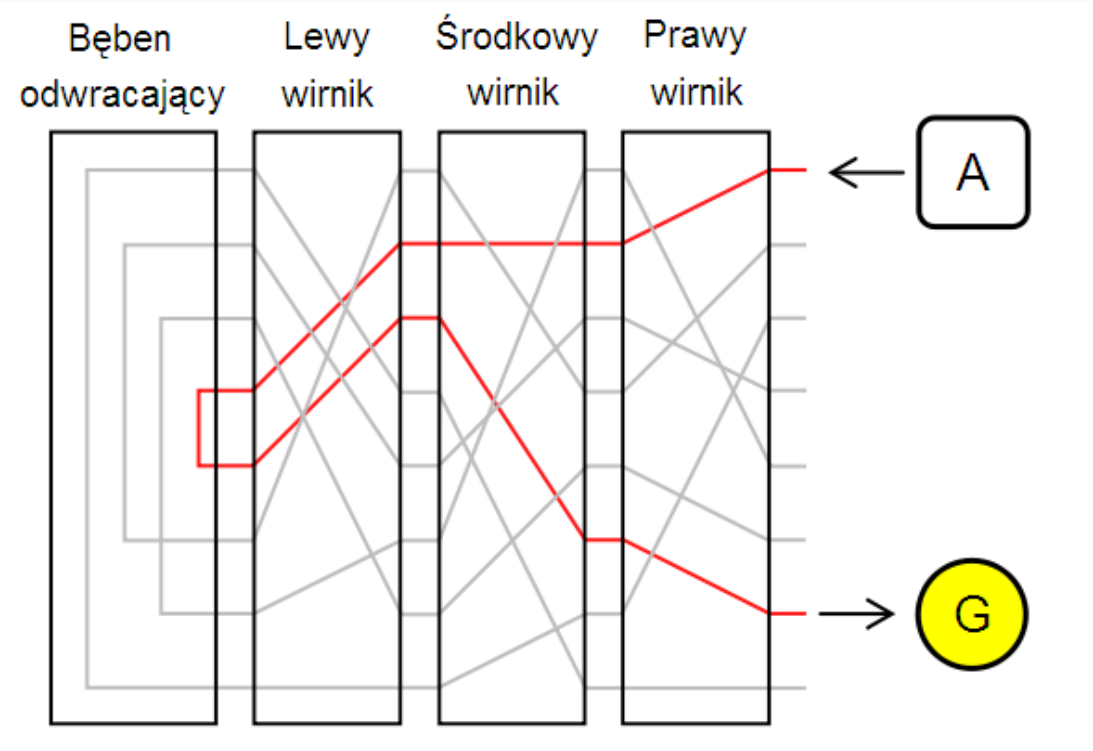
# Budowa Enigmy

Dzięki zastosowaniu obrotowych wirników oraz zmiennej łącznicy Enigma była odporna na wszystkie znane techniki dekryptażu.
Do Enigmy produkowano różnorodne wyposażenie dodatkowe, np. zdalną drukarkę.



# Budowa Enigmy

Szyfr Enigmy jest symetryczny dzięki zastosowaniu walca odwracającego. Ułatwiło to pracę szyfrantom, ale również kryptologom.



# Budowa Enigmy

Enigmę można opisać jako złożenie permutacji.
Niech P oznacza permutację dla łącznicy kablowej, U oznacza permutację dla walca odwracającego, a L,M,R oznaczają permutacje dla trzech kolejnych wirników. Szyfrowanie pierwszego znaku przez Enigmę (E) można opisać jako:

$$E = PRMLUL^{-1}M^{-1}R^{-1}P^{-1}$$

Po każdym naciśnięciu klawisza wirniki obracają się zmieniając przekształcenie. Niech $S$ będzie permutacją odpowiadającą przesunięciu o 1. Wtedy dla $i$ tego znaku szyfrowanie przez Enigmę (E) można opisać jako

$$E = PS^{-i}RS^{i}MLUL^{-1}M^{-1}S^{-i}R^{-1}S^{i}P^{-1}$$

# Klucz Enigmy

Dzienny klucz Enigmy (jej początkowe ustawienie) zawierało następujące informacje:

- Kolejność wirników (Walzenlage) — numery oraz kolejność w jakiej mają być zamontowane wirniki.
- Ustawienie wirników (Ringstellung) — pozycja w jakiej należało ustawić początkowy obrót wirników.
- Ustawienie łącznicy kablowej (Steckerverbindungen) — schemat połączenia wtyczek na łącznicy kablowej.

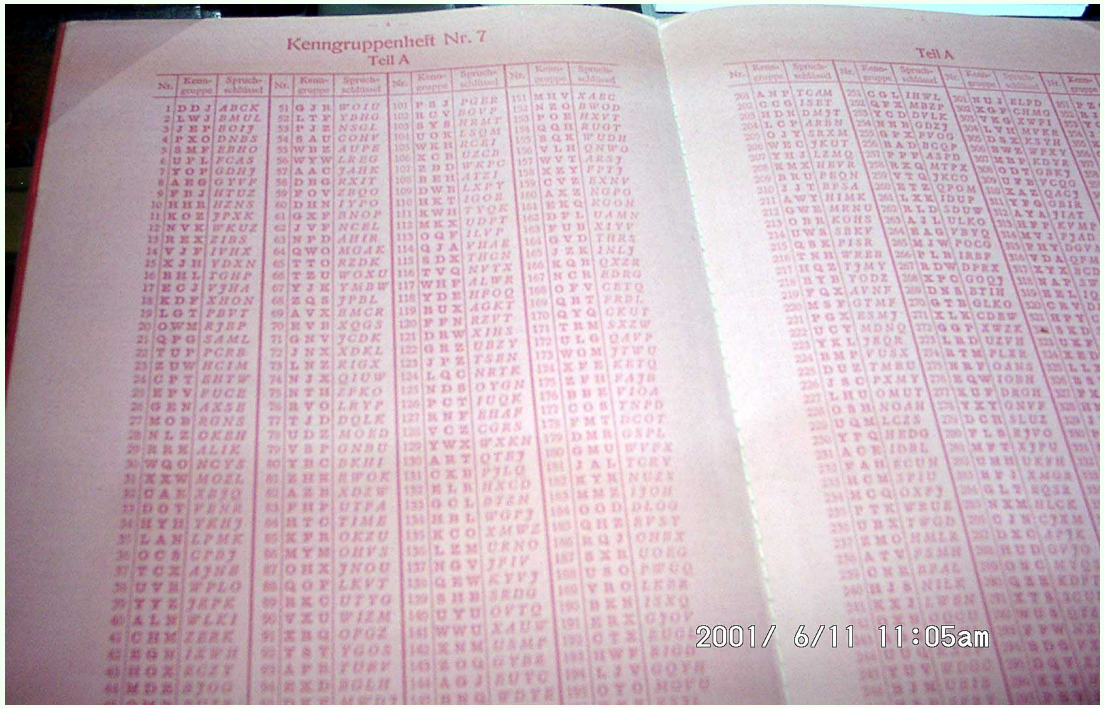
Ponadto operator miał wybrać unikalny (odmienny dla każdej wiadomości) trzyliterowy klucz wiadomości.

# Klucz Enigmy

Wywiady angielski i francuski znały zasadę działania Enigmy. Jednak z uwagi na liczbę możliwych kluczy dziennych

$$\approx 6!\ 26^3\ \frac{26!}{2^6\ 6!\ 14!} \approx 10^{16}$$

uznały ją za niemożliwą do złamania.



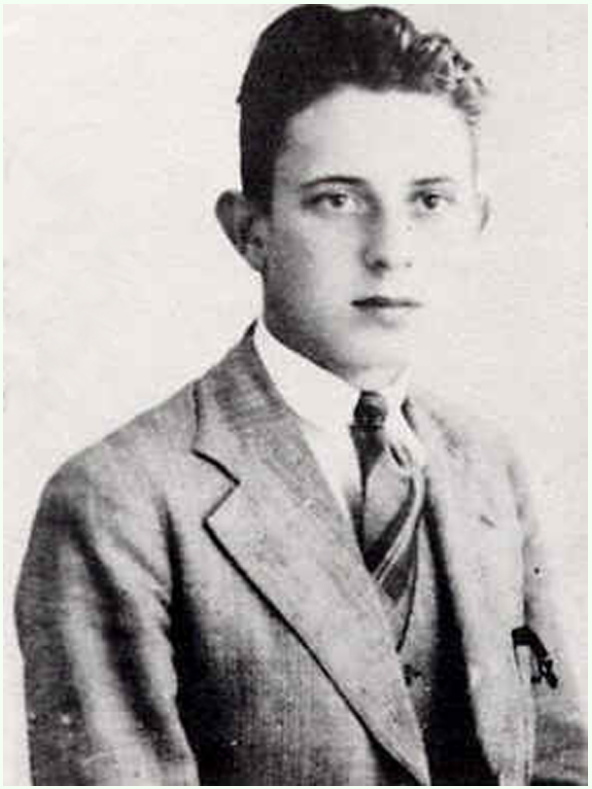
# Biuro Szyfrów

W styczniu 1929 w Uniwersytecie Poznańskim zorganizowano kurs kryptologii dla studentów matematyki znających język niemiecki.

Jesienią 1930 utworzono w Poznaniu filię Biura Szyfrów w której zatrudniono m.in. Mariana Rejewskiego, Jerzego Różyckiego oraz Henryka Zygalskiego.

Mocarstwa zachodnie tak mocno wątpiły w możliwość złamania algorytmu szyfrującego Enigmy. Francuski wywiad przekazał plany budowy maszyn Enigma zdobyte około roku 1931 przez francuskiego agenta traktując te informacje jako bezwartościowe.

# Polscy krzptolodzy


# Teoria koincydencji

Stała koincydencji to prawdopodobieństwo pojawienia się dwóch identycznych liter odległych o pewną ustaloną liczbę znaków.

Czynadchodzącecociepłenietoznakostatecznegokończazimyczy
tożmożliwyjestjeszczepowrótmrozówiśnieguGrzegorzGumiń
skiZimajużniewróciPoniedziałkowyskoktemperaturyniebędzi
echwilowycałyostatnitydzieńlutegobędziebardzociepłyTer

- Dla języka polskiego charakterystyczna stała koincydencji to 0.048.
- Tekst po zaszyfrowaniu szyfrem podstawieniowym ma taką samą stałą koincydencji.
- Dobrze zaszyfrowany tekst w którym częstości znaków są losowe ma stałą koincydencji równą 0.038 dla 26 znakowego alfabetu.

# Teoria koincydencji

Okazuje się, że depesze o tych samych prefixach stosują ten sam podstawieniowy szyfr (mają stałą koincydencji charakterystyczną dla języka niemieckiego).

`rfbwldpcaihwbqxemtpobfvgqihfgrojvddzluwsjurnkthcly`
`rfbwldnwelsoapxoazybbyzrqqcjdxcfkhingdfcmjvpiktelm`

Ale depesze o różnych prefixach mają stałą koincydencji charakterystyczną dla losowych znaków.

`rkxwfokiscixjwtwqapdredbwlfvgkcojhstnpboafnugvuemh`
`wdxroohrktgusdtudeqlswfpvfqnrcyavzjlyiknoxhonmgepw`

Wniosek: Początek depeszy koduje klucz dla reszty depeszy.

# Łamanie Enigmy

W ciągu dwóch lat Marian Rejewski złamał kod Enigmy rozbudowując matematyczną teorię cykli.

**Obserwacja 1**

Każdą permutację można rozłożyć na cykle.

**Definicja 1**

Transpozycje to cykle o długości 2.

**Definicja 2**

Inwolucja to permutacja, której złożenie ze samą sobą jest identycznością. Inwolucja składać się może wyłącznie z punktów stałych i transpozycji.

# Teoria cykli

Permutacje możemy składać

| Permutacja A | Permutacja B | Złożenie B∘A |
|---|---|---|
| a $->$ c | a $->$ b | a $->$ d |
| b $->$ d | b $->$ c | b $->$ e |
| c $->$ a | c $->$ d | c $->$ b |
| d $->$ e | d $->$ e | d $->$ a |
| e $->$ b | e $->$ a | e $->$ c |

Permutacja A: (ac)(bde)
Permutacja B: (ac)(bde)
Złożenie B∘A: (ad)(bec)

# Łamanie Enigmy

**Twierdzenie 1**

Złożenie inwolucji to permutacja w której elementy transpozycji trafiają do cykli tej samej długości.

**Twierdzenie 2**

Jeżeli w permutacji jest parzysta liczba cykli o tej samej długości to można taką permutację rozłożyć na dwie inwolucje.

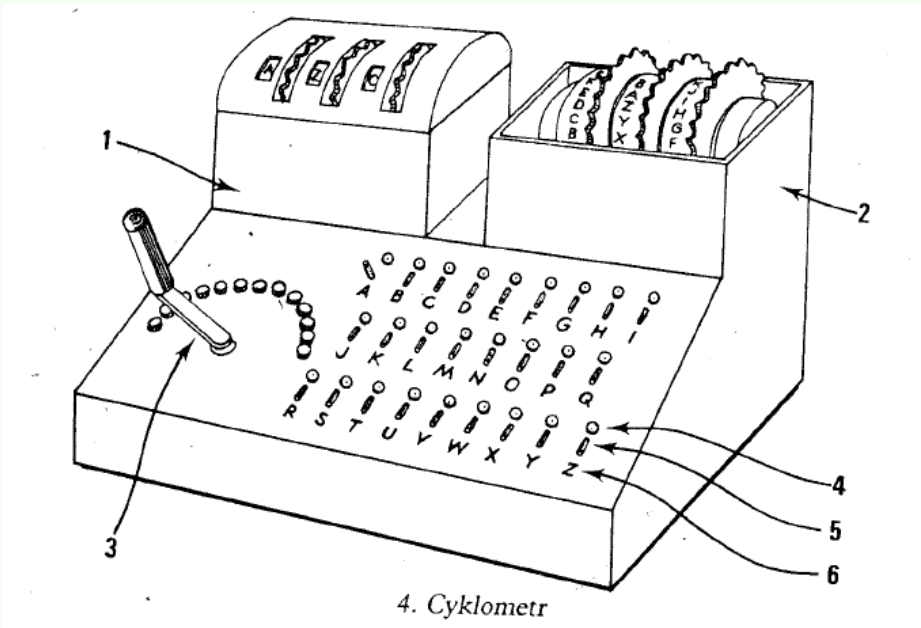
# Teoria cykli

Analizując początki depesz możemy odkryć cykle w złożeniach odpowiednich permutacji (pomiędzy pozycjami $i$ a $i+3$). Znaleźliśmy cykle (a)(bc)(dvpfkxgzyo)(eijmunqlht)(rw)(s).

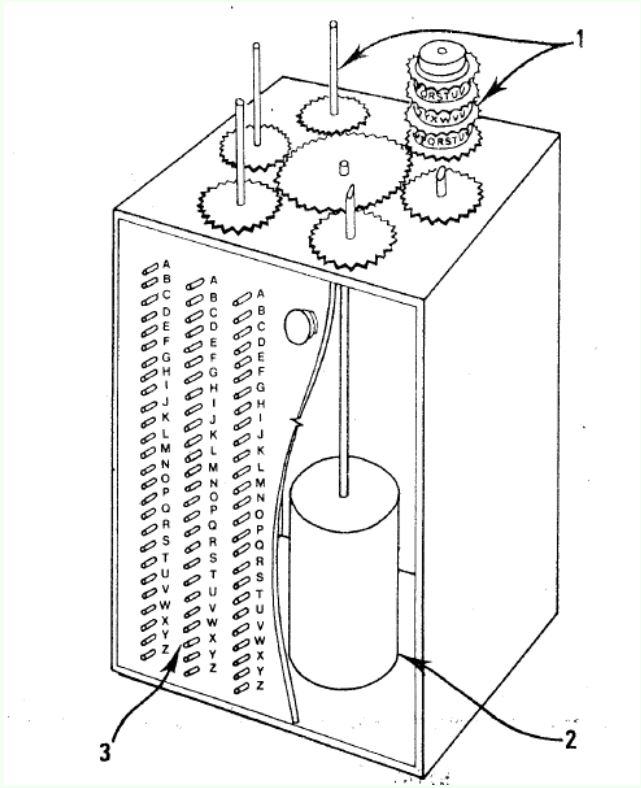
| | | |
|---|---|---|
| auq amn | maw uxp | sug smf |
| bnh chl | nxd qtu | tmn eby |
| cik bzt | nlu qfz | taa exb |
| ddb vdv | obu dlz | use nwh |
| ejp ips | pvj feg | vii pzk |
| fbr kle | qga lyb | vii pzk |
| gpb zsv | rjl wpx | vqz pvr |
| ikg jkf | syx scw | xrs gnm |
| khb xjv | syx scw | ypc osq |
| khb xjv | syx scw | ypc osq |
| maw uxp | sug smf | zsj ywg |

# Maszyny do dekodowania szyfrogramów

Aby zautomatyzować proces dekodowania skonstruowano Cyklometr i Bombę kryptograficzną do dekodowania depesz.



4. Cyklometr

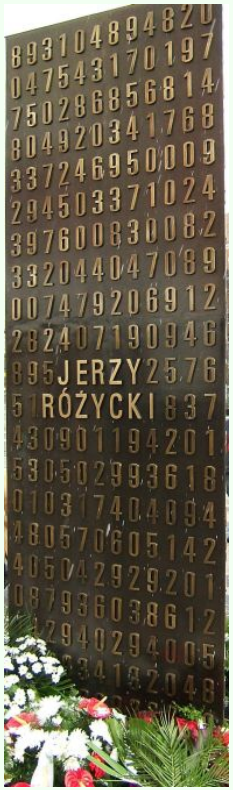


# Co działo się później

- Niemcy nieustannie modyfikują Enigmę. Do jej rozkodowania potrzebne są coraz większe nakłady finansowe. Miesiąc przed wybuchem wojny (26 lipca 1939) Biuro szyfrów przekazuje rozpracowaną maszynę wywiadowi francuskiemu i angielskiemu.
- Metody dekryptażu rozwijane są Bletchley Park. Do rozkodowania najbardziej skomplikowanej wersji Enigmy „Lorenz" powstał Colossus - pierwszy na świecie komputer.
- Władysław Kozaczuk i Jerzy Straszak, w swej publikacji twierdzą, że „panuje ogólne przekonanie, że Ultra zaoszczędziła światu co najmniej dwóch lat wojny i prawdopodobnie zapobiegła zwycięstwu Hitlera".

# Bohaterowie

10 listopada 2007 z okazji 75 lecia złamania Enigmy odsłoniono „Pomnik kryptologów”.





# Warto przeczytać

- Marian Rejewski. Jak matematycy polscy rozszyfrowali Enigmę. Roczniki PTM. Wiadomości Matematyczne 1980 (dostępny elektronicznie).
- Leszek Gralewski. Złamanie Enigmy. Wyd. Adam Marszałek, 2005.
- Marek Grajek. Enigma. Bliżej prawdy. Wyd. Rebis 2007.
- 21 numer MMM Magazynu Miłośników Matematyki (dostępny elektronicznie).
- Strona z zagadkami o Enigmie http://www.im.pwr.wroc.pl/ tjurlew/dfn2007E.htm.
- Adres symulatora http://www.biecek.pl/projects/Enigma2/Enigma.html.