Barbara Roszkowska Lech

Matematyczna podróż w głąb Enigmy

MATEMATYKA DLA CIEKAWYCH ŚWIATA

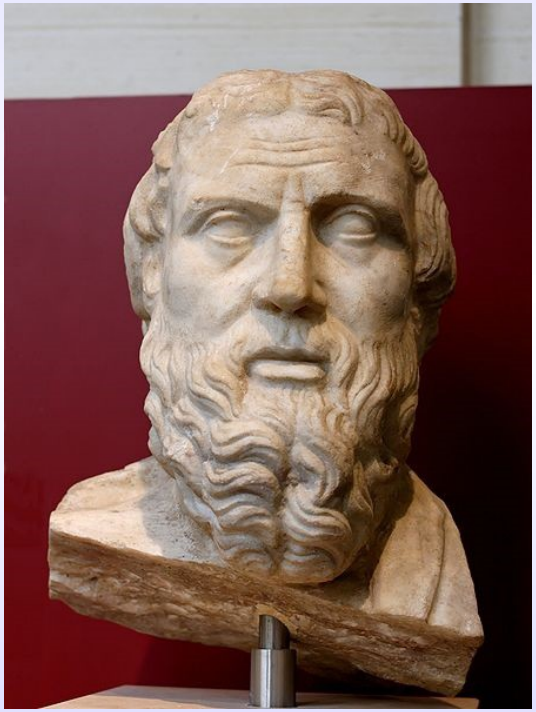
WYDZIAŁ
MATEMATYKI I NAUK
INFORMACYJNYCH


ENIGMA

Kryptologia

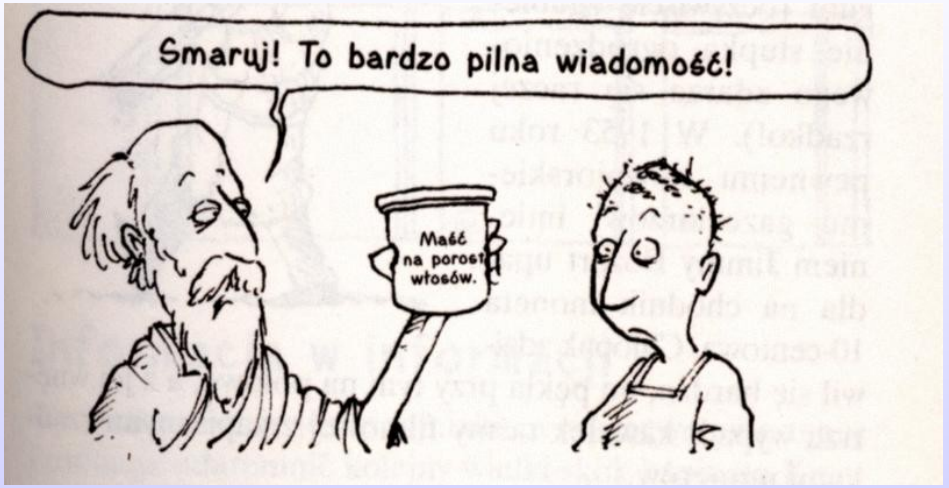
- Steganografia (steganos- zakryty)
  zajmuje się ukrywaniem istnienia wiadomości
- Kryptografia (kryptos)
  zajmuje się ukrywaniem znaczenia wiadomości
- Kryptoanaliza
  metody odczytywania wiadomości

Historia przesyłania informacji w tajemnicy



Herodot V pne

- Przypadek Demaratosa
- Histajeus i Arystogoras



Metody steganografii

- Zaznaczanie liter
- Pisanie niewidzialnym atramentem
- Nakłuwanie szpilką liter
- Metoda mikropunktu
- Ukrywanie wiadomości w plikach graficznych lub dźwiękowych
- ...

Ukryte na pierwszym planie

„ Złe warunki pogodowe.
Baza wysunięta opuszczona.
Oczekiwanie na poprawę.”

James Morris
wiadomość dla gazety ” The Times” 1953

Klucz

Zakodowana wiadomość	Znaczenie
Złe warunki pogodowe. Wiatr nadal dokuczliwy.	Everest zdobyty. Próba wejścia zaniechana.
Przełęcz Południowa nie do utrzymania.	Band
Ściana Lhotse niemożliwa do zdobycia.	Bourdillon
Obóz na grani nie do utrzymania.	Evans
Wycofanie do zachodniej kotliny.	Gregory
Baza wysunięta opuszczona.	Hillary
Obóz V opuszczony.	Hunt
Obóz VI opuszczony.	Lowe
Obóz VII opuszczony.	Noyce
Oczekiwanie na poprawę.	Tenzing
Niedługo następne informacje.	Ward

Szyfr zakonu Krzyżackiego

- L lesen- czytać
- S swigen - milczeć
- K keren - obracać

STU KOT LJEST KOZDRAB SOK LTRUDNE KEINADAZ

To jest bardzo trudne zadanie

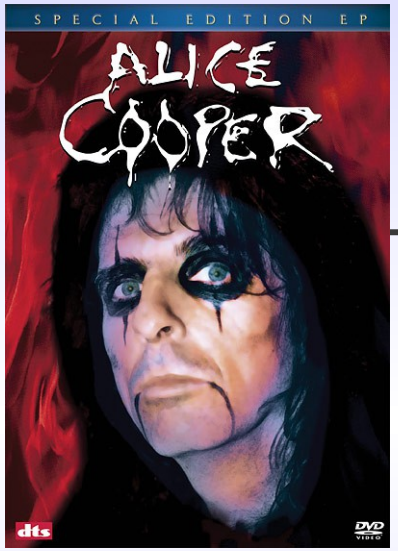
Kryptologia

- Steganografia (steganos- zakryty)
  zajmuje się ukrywaniem istnienia wiadomości
- Kryptografia (kryptos)
  zajmuje się ukrywaniem znaczenia wiadomości
- Kryptoanaliza
  metody odczytywania wiadomości

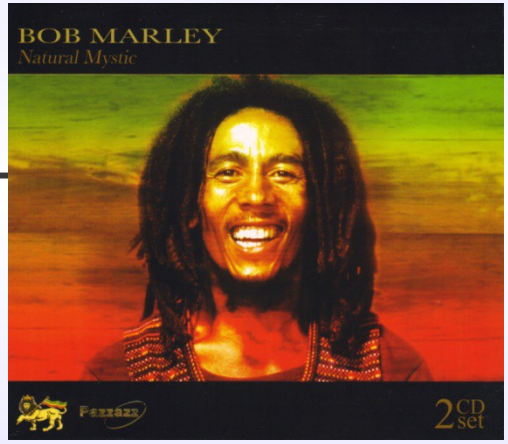
Kryptografia

- Krypto grafos - grec. ukryte pismo
- Kryptografia – „Sztuka przekształcania tekstu pisanego, zrozumiałego dla wszystkich, w tekst zaszyfrowany zrozumiały tylko dla wtajemniczonych znających dany szyfr;” Słownik j. pol. PWN.
- Szyfr – „Rodzaj kodu, zapisu tekstu za pomocą systemu umownych znaków w celu zatajenia treści tekstu przed osobami niepowołanymi” Słownik j. pol. PWN

Cel: bezpieczna komunikacja



Alicja

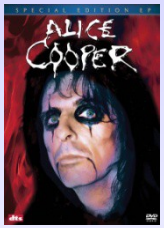


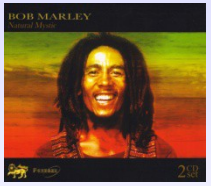
Bob

Ewa

- Szyfrowanie to funkcja $K \times P \rightarrow C$
- Deszyfrowanie to funkcja $K \times C \rightarrow P$

Co to jest szyfr ?





klucz *K*

klucz *K*

algorytm szyfrowania E

szyfrogram C = E(K,M)

algorytm odszyfrowywania D

wiadomość M

wiadomość M=D(K,C)

Scenariusz

1. Alicja i Bolek ustalają szyfr (E,D).
2. Alicja i Bolek ustalają **tajny** klucz K.
3. Alicja wybiera wiadomość M, oblicza C=E(K,M), wysyła C do Bolka.
4. Bolek oblicza D(K,C).
5. Ewa otrzymuje C.

Podstawowa zasada bezpieczeństwa

Zasada Kerckhoffsa Auguste Kerckhoffs 1883

Szyfr *(E,D)* musi być bezpieczny nawet jeśli Ewa zna algorytmy *E* i *D.*

Jedyna rzecz której Ewa nie zna to klucz *K*

Historia kryptografii

. . .

. . .

Juliusz Cezar

Enigma

komputery

czasy starożytne

współczesność

Szyfr Cezara - I w. p.n.e.

- A B C D E F G H I J K L M . . .
- D E F G H I J K L M N O P . . .

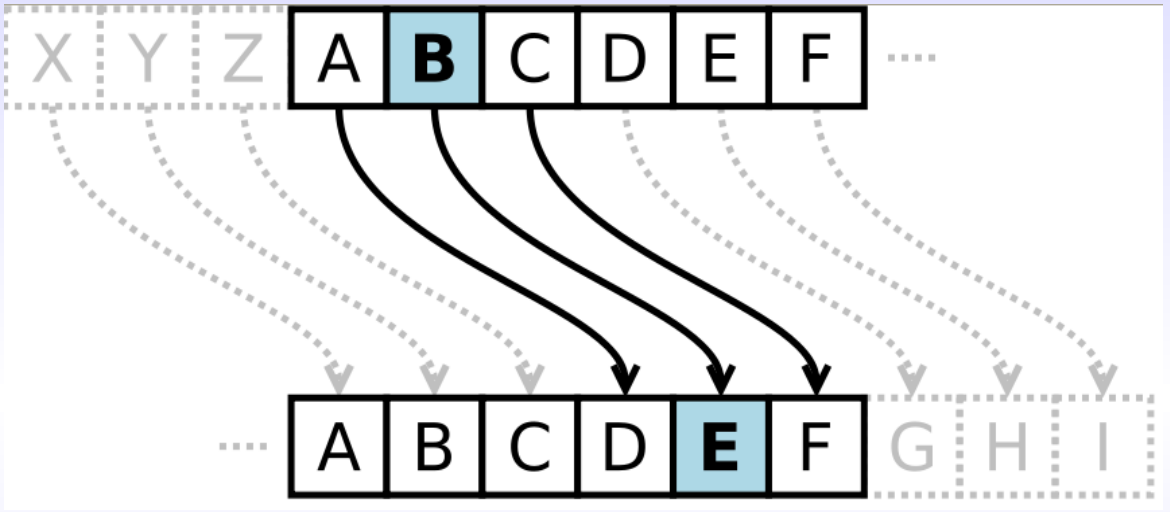
- GALLIA EST OMNIS DIVISA
- JDOOLD HVW RPQLV GLYLVD

Tylko 26 możliwych kluczy

Kolejnym literom alfabetu łacińskiego przyporządkujemy liczby od 0 do 25.

Systemy kryptograficzne można teraz z definiować z użyciem działań algebraicznych modulo 26.

Szyfr Cezara



$$EK(x) = x + K \pmod{26}$$

$$DK(y) = y - K \pmod{26},$$

Inne przykład szyfrowania

- $E(m) = am \pmod n$
  $D(c) = a^{-1} c \pmod n$

- $E(m) = am+b \pmod n$
  $D(c) = a^{-1} (c - b) \pmod n$

Szyfr z Kamasutry

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

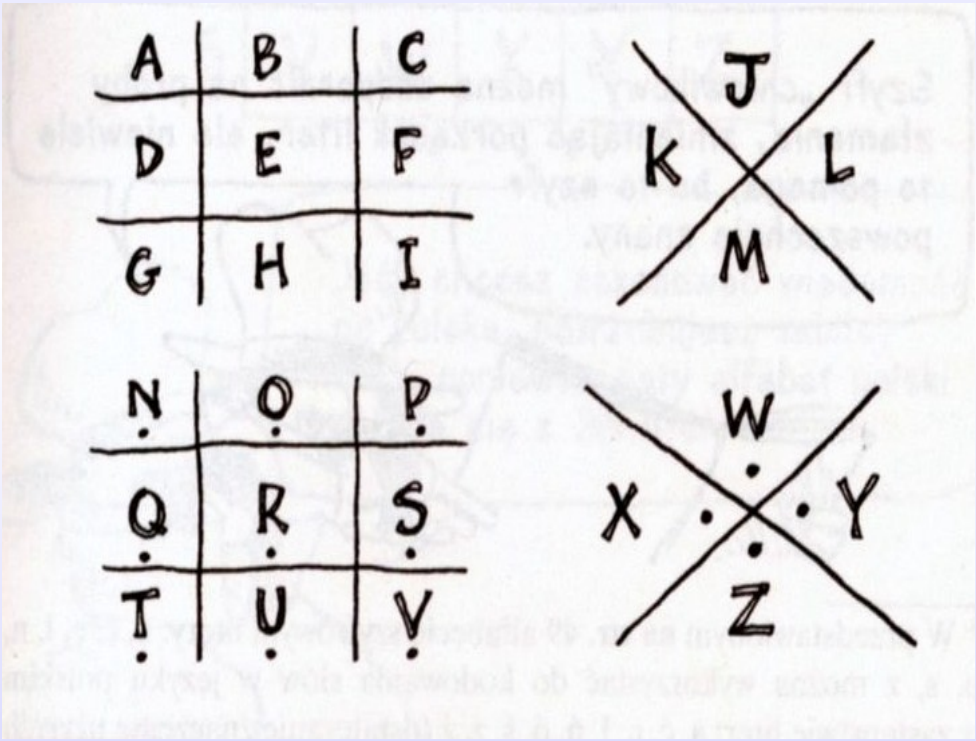
SPOTKANIE

NYQZJVSGU

Szyfr wolnomularzy

Używali go w XVIII wieku wolnomularze do protokołowania swoich zebrań

Szyfr ten polega na zastąpieniu liter symbolami według następującego wzoru:



Kryptologia

- Steganografia (steganos- zakryty)
  zajmuje się ukrywaniem istnienia wiadomości
- Kryptografia (kryptos)
  zajmuje się ukrywaniem znaczenia wiadomości
- Kryptoanaliza
  metody odczytywania wiadomości

Częstość występowania liter w alfabecie angielskim

A	8.167	J	0.153	S	6.327
B	1.492	K	0.772	T	9.056
C	2.782	L	4.025	U	2.758
D	4.253	M	2.406	V	0.978
E	12.702	N	6.749	W	2.360
F	2.228	O	7.507	X	0.150
G	2.015	P	1.929	Y	1.974
H	6.094	Q	0.095	Z	0.074
I	6.966	R	5.987		

Szyfry wieloalfabetowe

Johanes Trithemius

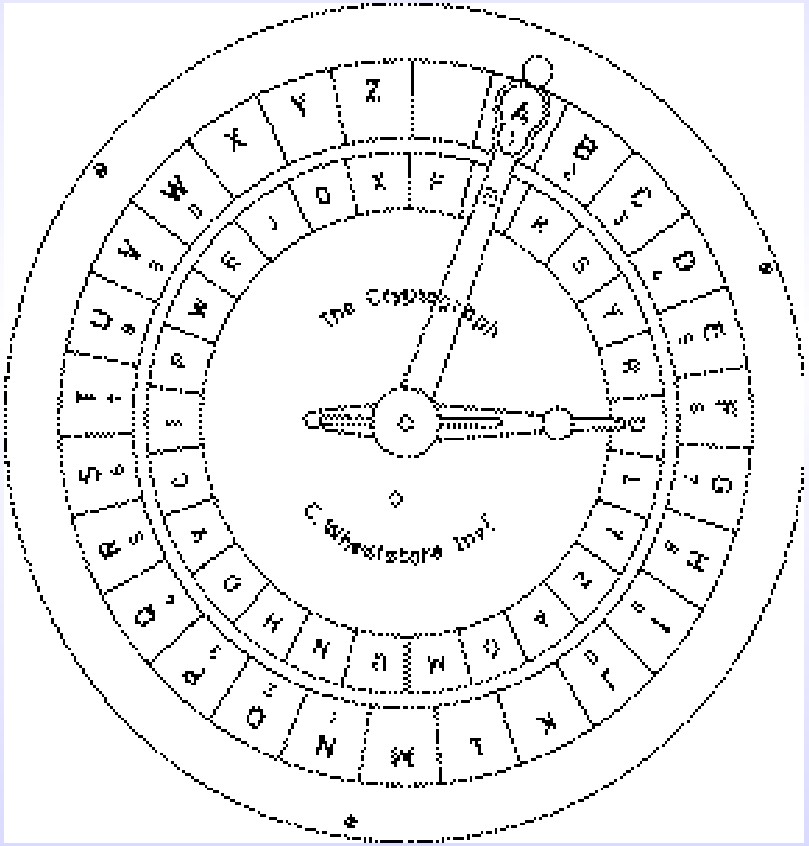
1462-1516

Autor pierwszego podręcznika kryptografii

Jeden z prekursorów szyfrów wieloalfabetowych

Szyfry wieloalfabetowe

Ojcem szyfrów wieloalfabetowych był Leon Battista Alberti . Opisał o dysk szyfrowy, podobny do tego na obrazku, umozliwiający wiele podstawień.



Szyfr Vigenera - XVI w.

- 2, 3, 1, 4
- A B C D E F G H I J K L M ...
- C D E F G H I J K L M N O ...
- D E F G H I J K L M N O P ...
- B C D E F G H I J K L M N ...
- E F G H I J K L M N O P Q...

- GALLIA EST OMNIS DIVISA
- IDMPKD FWV RNRKV EMXLTE

Tablica Vigenere`a

Jawny	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
1	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
2	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
3	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
4	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
5	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
6	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
7	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	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	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
13	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
14	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	N
15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	Z	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
26	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

Szyfr Vigenera (model matematyczny)

Klucz

$$K = (k_1, k_2, \ldots, k_n)$$

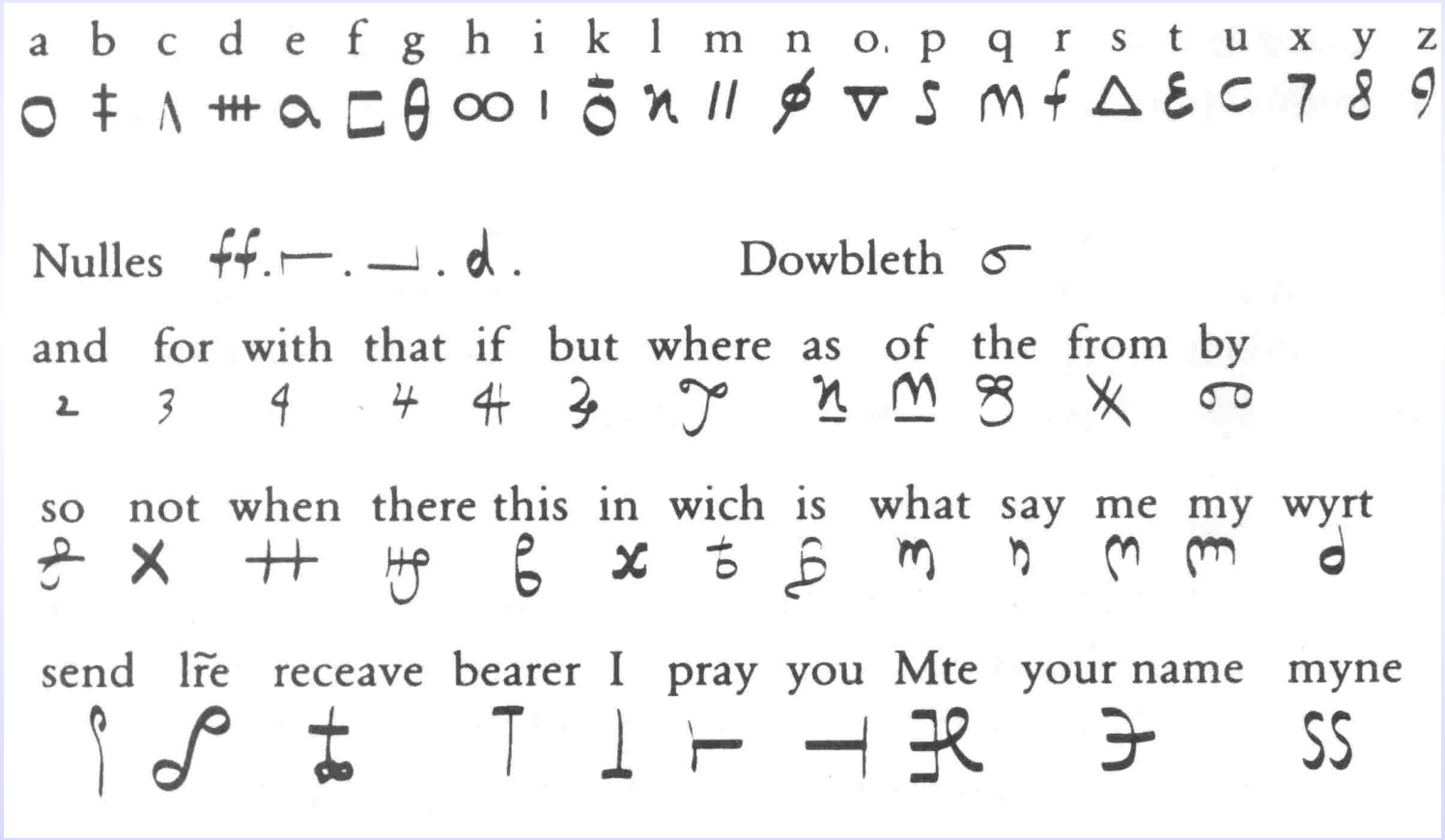
Szyfrowanie

$$E_K(x_1, \ldots, x_n) = (x_1 +_{26} k_1, \ldots, x_n +_{26} k_n)$$

Deszyfrowanie

$$D_K(y_1, \ldots, y_n) = (y_1 -_{26} k_1, \ldots, y_n -_{26} k_n)$$

Szyfr Marii Stuart



Ofiara udanej kryptoanalizy

Maria Stuart i Elżbieta królowa Anglii

Szyfr Playfaira

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

Wiadomość **LICEUM**

LI

Szyfr Playfaira

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

Wiadomość **LICEUM**

LI

Szyfr Playfaira

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

Wiadomość **LICEUM**

LI

NL

Szyfr Playfaira

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

Wiadomość **LICEUM**

LI **CE**

NL

Szyfr Playfaira

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

Wiadomość **LICEUM**

LI **CE**

NL

Szyfr Playfaira

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

Wiadomość **LICEUM**

LI **CE**

NL **DT**

Szyfr Playfaira

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

Wiadomość **LICEUM**

LI **CE** **UM**

NL **DT**

Szyfr Playfaira

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

Wiadomość **LICEUM**

LI **CE** **UM**

NL **DT**

Szyfr Playfaira

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

Wiadomość **LICEUM**

LI **CE** **UM**

NL **DT** **MK**

Szyfr Playfaira

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

Wiadomość **LICEUM**

LI **CE** **UM**

NL **DT** **MK**

Kryptogram **NLDTMK**

ADFGVX – najsłynniejszy szyfr okresu I wojny światowej

	A	D	F	G	V	X
A	8	p	3	d	1	n
D	l	t	4	o	a	h
F	7	k	b	c	5	z
G	j	u	6	w	g	m
V	x	s	v	i	r	2
X	9	e	y	0	f	q

SZYFROWANIE 1

Poniatowski										
p	o	n	i	a	t	o	w	s	k	i

ADFGVX – najsłynniejszy szyfr okresu I wojny światowej

	A	D	F	G	V	X
A	8	p	3	d	1	n
D	l	t	4	o	a	h
F	7	k	b	c	5	z
G	j	u	6	w	g	m
V	x	s	v	i	r	2
X	9	e	y	0	f	q

ADFGVX – najsłynniejszy szyfr okresu I wojny światowej

	A	D	F	G	V	X
A	8	p	3	d	1	n
D	l	t	4	o	a	h
F	7	k	b	c	5	z
G	j	u	6	w	g	m
V	x	s	v	i	r	2
X	9	e	y	0	f	q

SZYFROWANIE 1

Poniatowski										
p	o	n	i	a	t	o	w	s	k	i
AD	DG	AX	VG	DV	DD	DG	GG	VD	FD	VG

SZYFROWANIE 2

ADDGAXVGDVDDDGGGVDFDVGXX

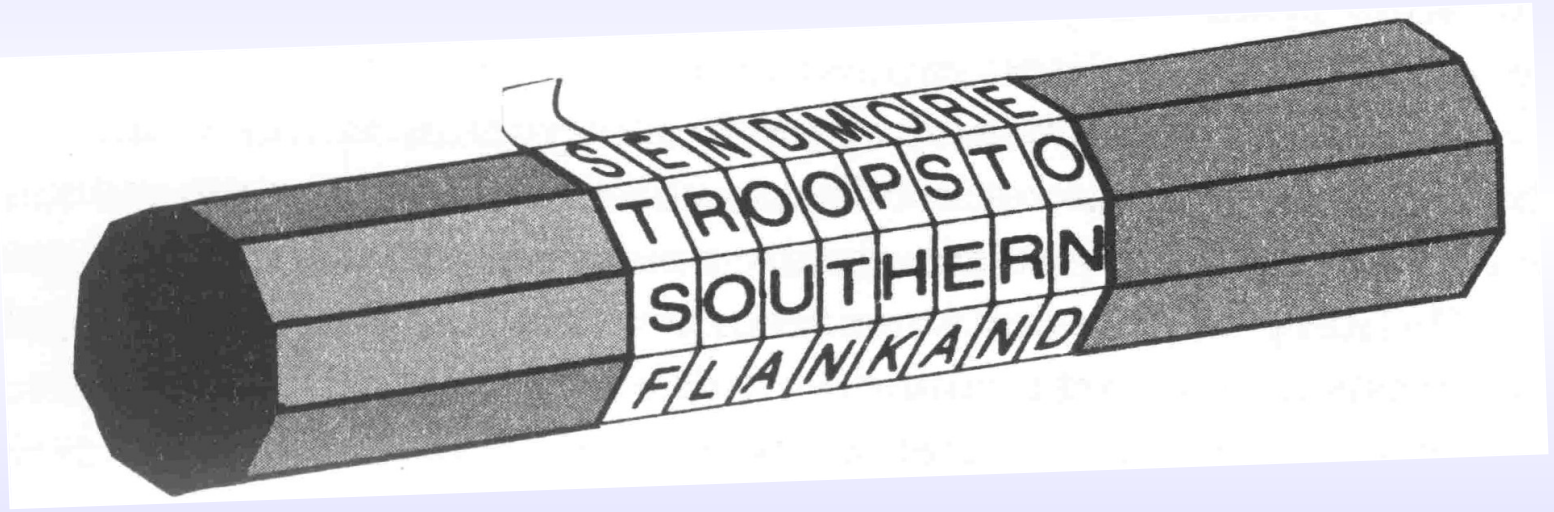
R	O	K
A	D	D
G	A	X
V	G	D
V	D	D
D	G	G
G	V	D
F	D	V
G	X	X

挻

K	O	R
D	D	A
X	A	G
D	G	V
D	D	V
G	G	D
D	V	G
V	D	F
X	X	G

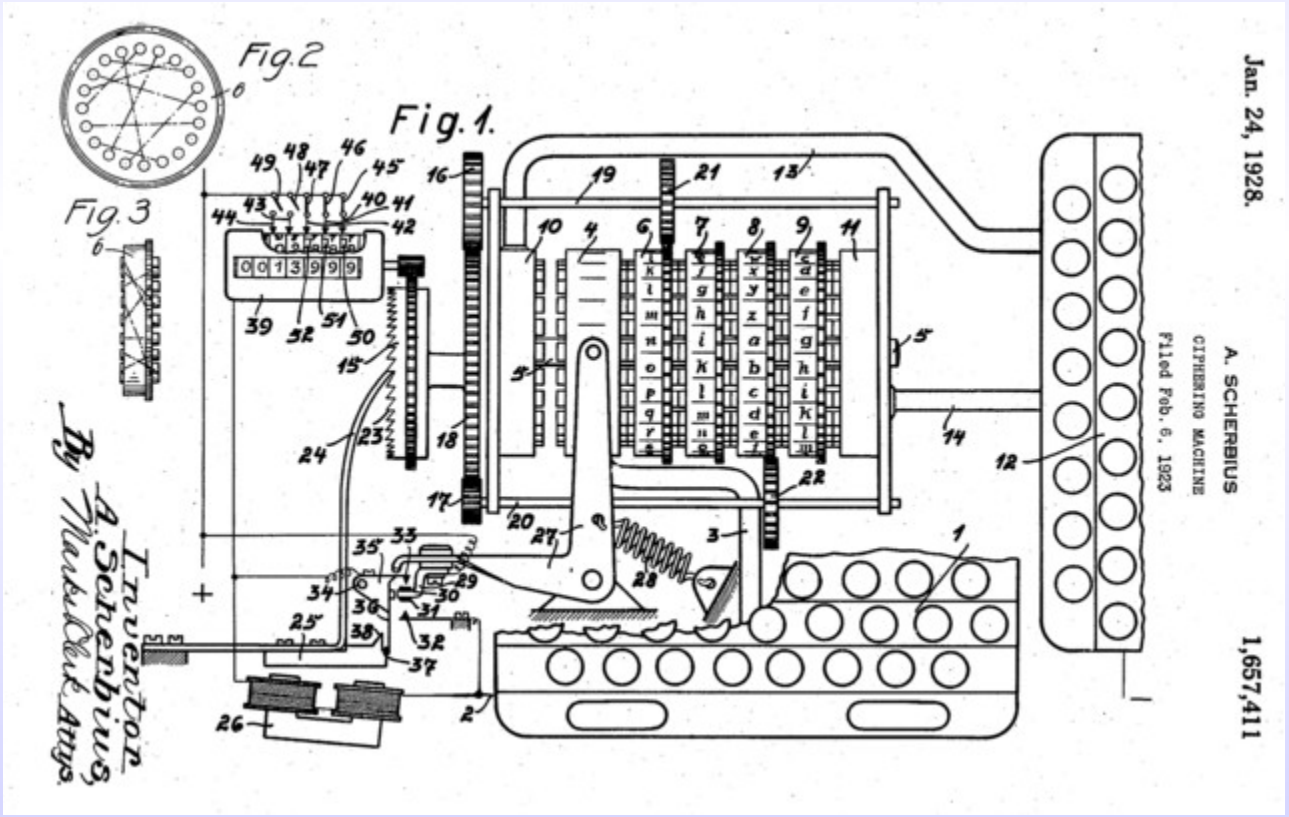
DDAXAGDGVDDVGGDDVGVDFXXG

Scytale urzadzenie szyfrujące



Enigma

Hugo Koch projekt 1918 r maszyna szyfrująca ze zmiennym szyfrem podstawieniowym

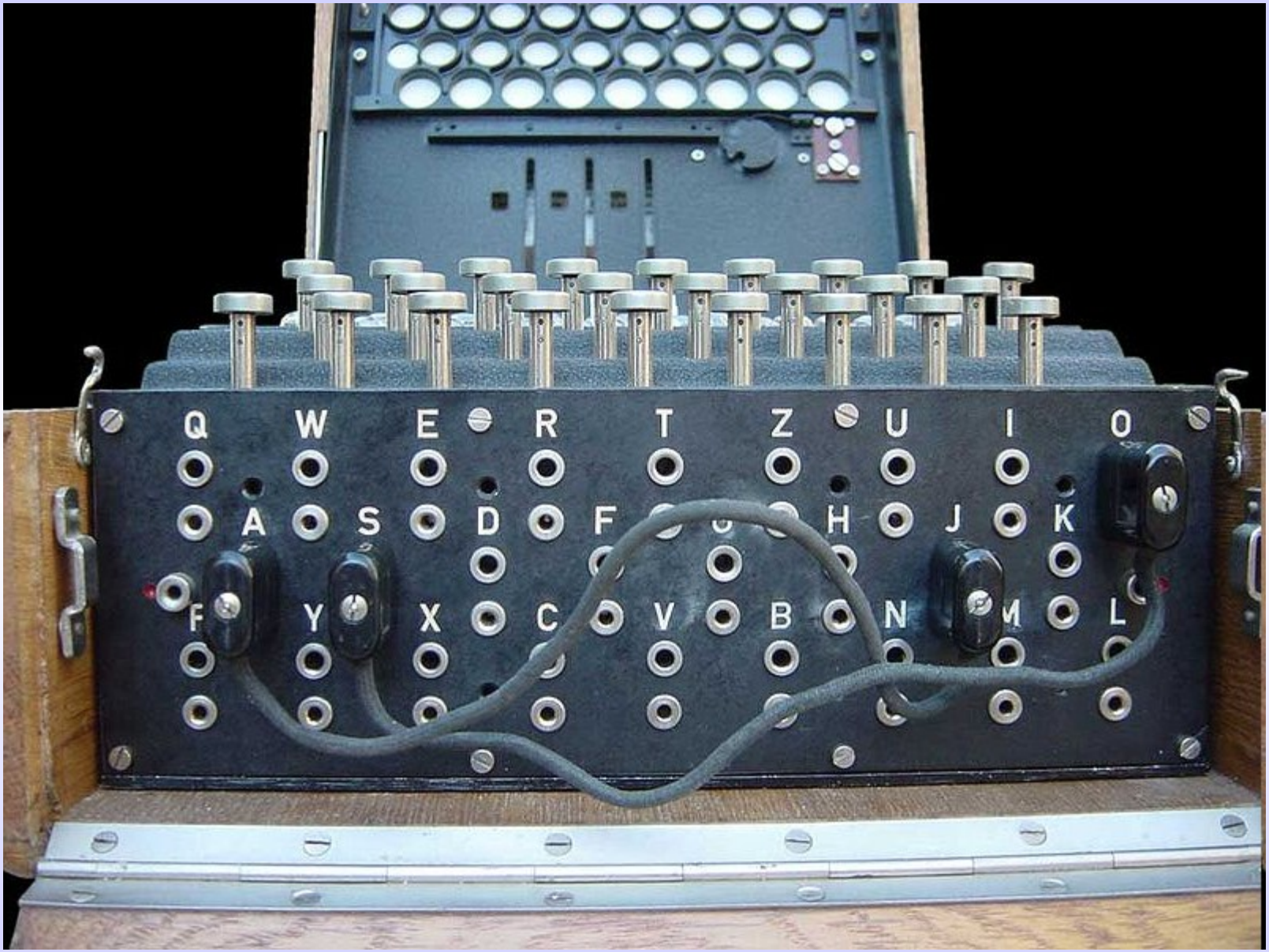


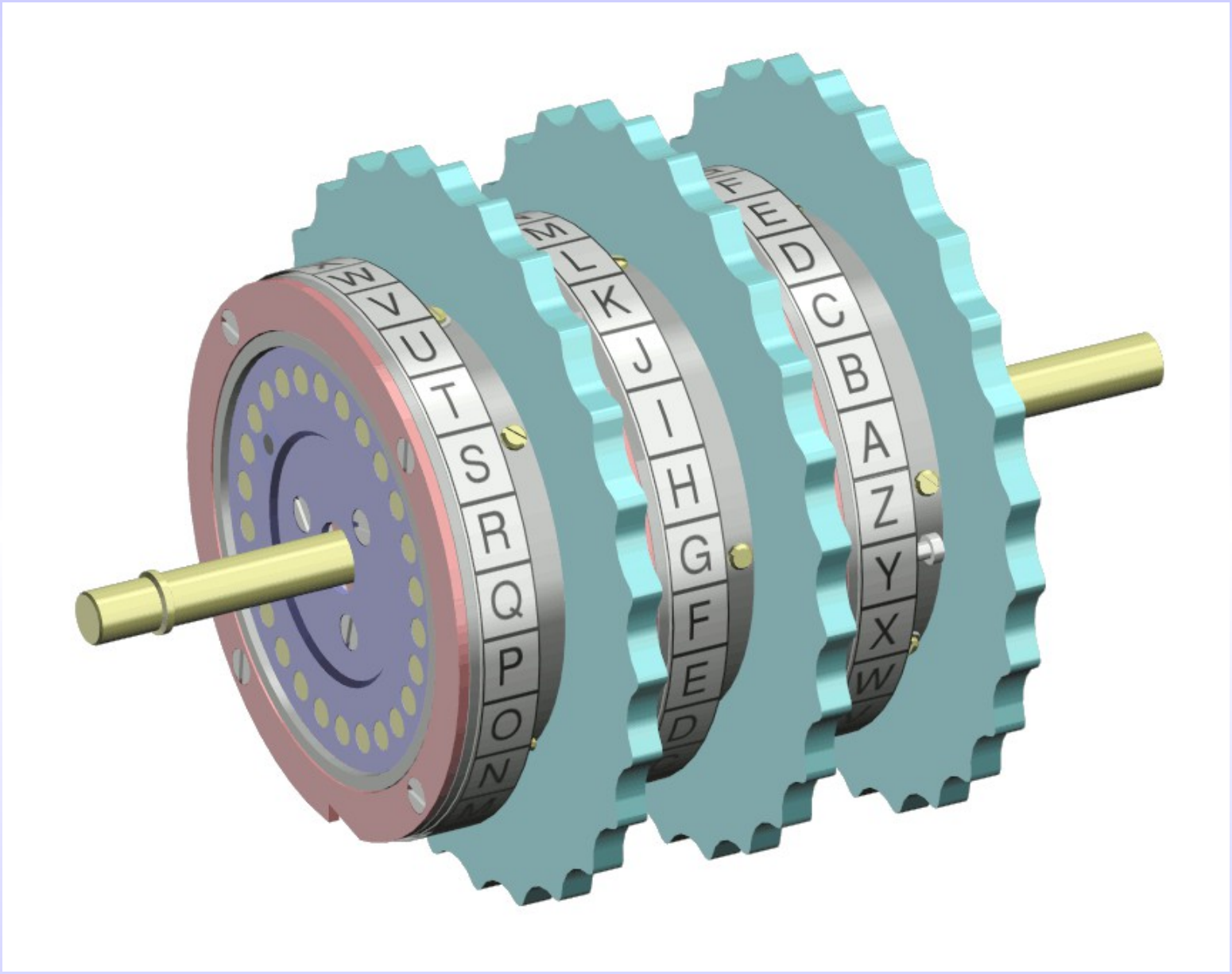
Enigma

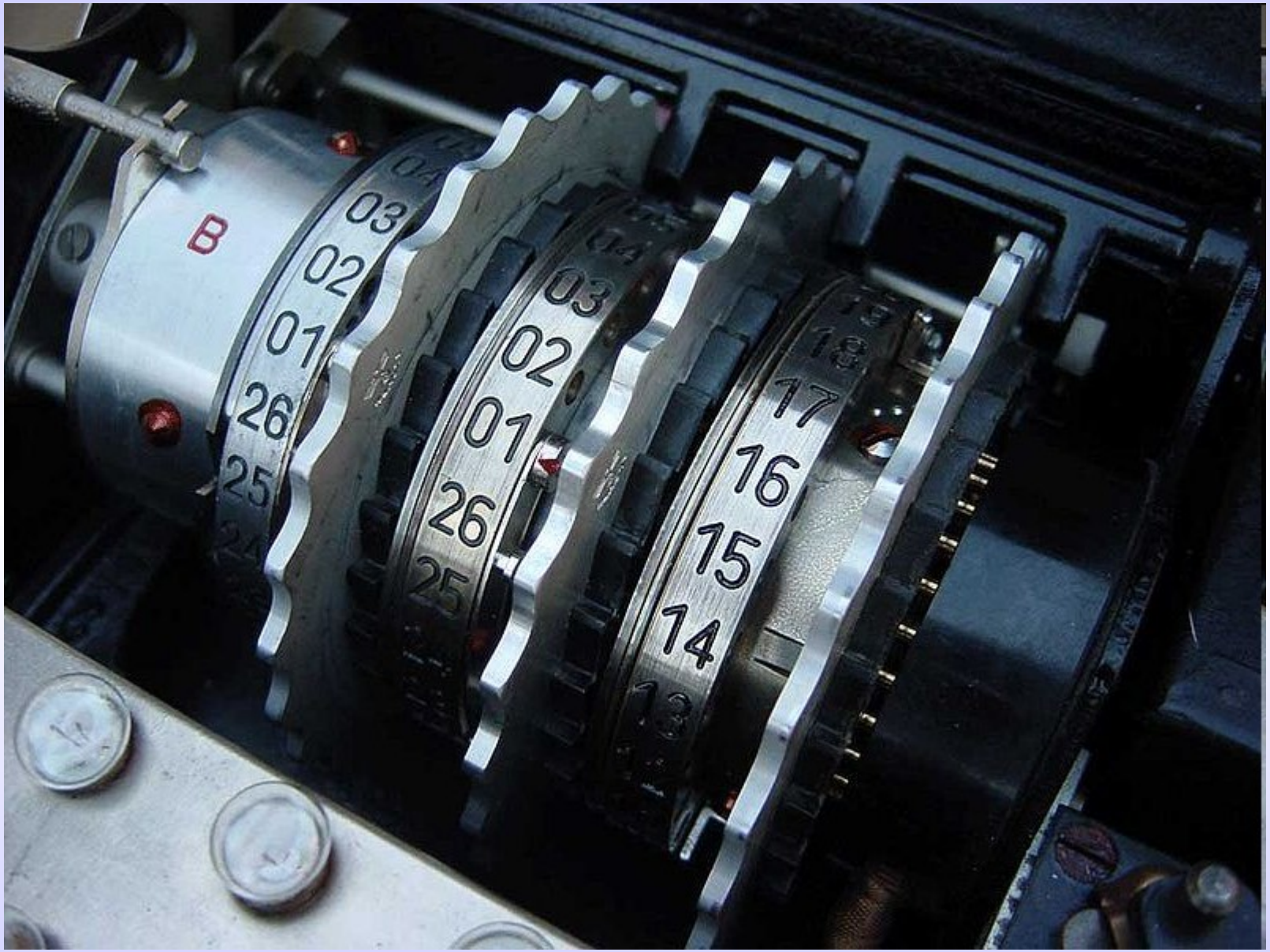
Enigma – używana w kilku wersjach w niemieckiej armii od końca lat 20. XX w. do zakończenia II wojny światowej

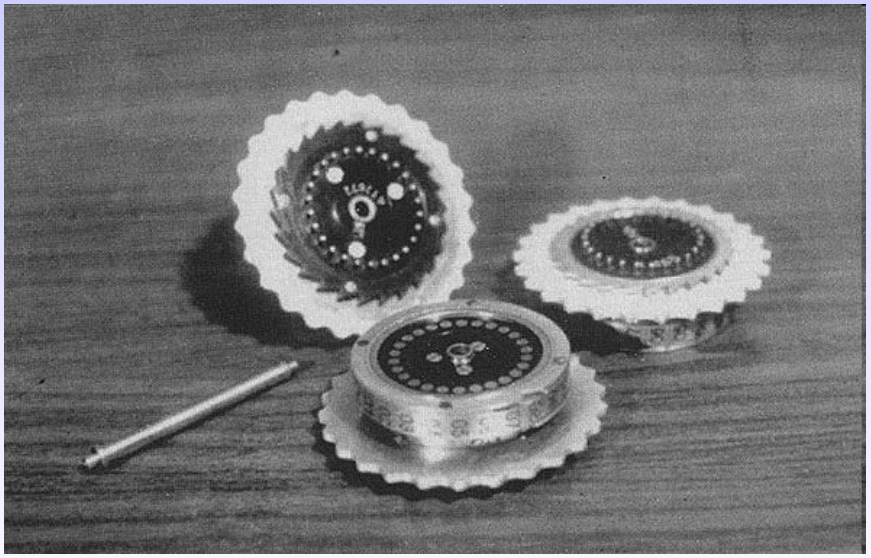
Budowa

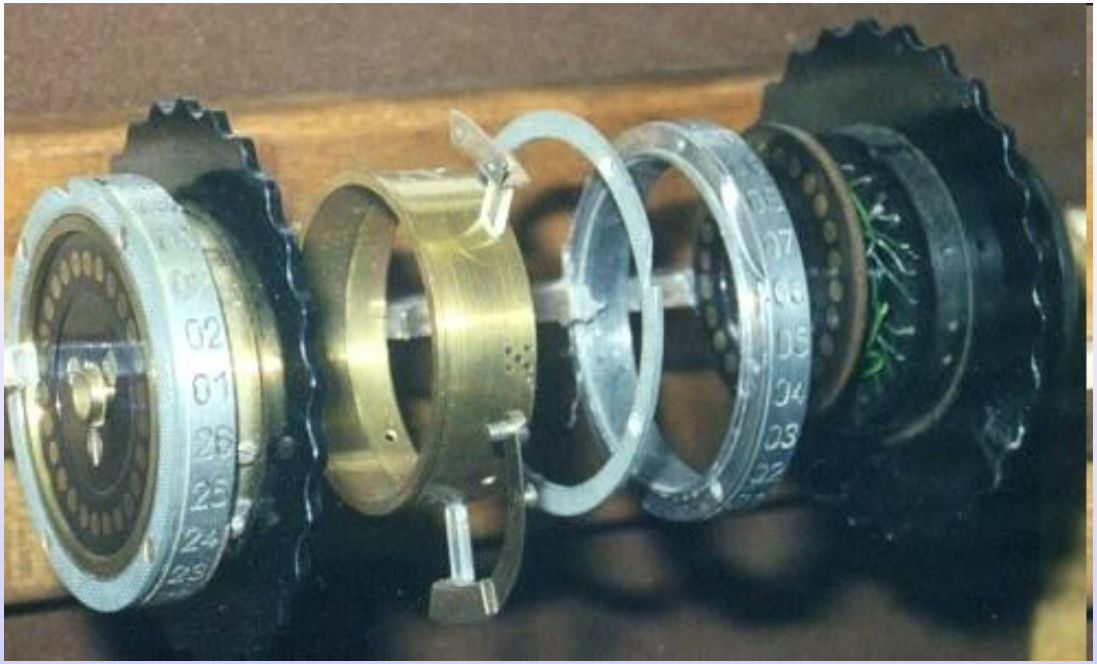
- rotory (wirniki)
- łącznica
- bęben odwracający (reflektor)

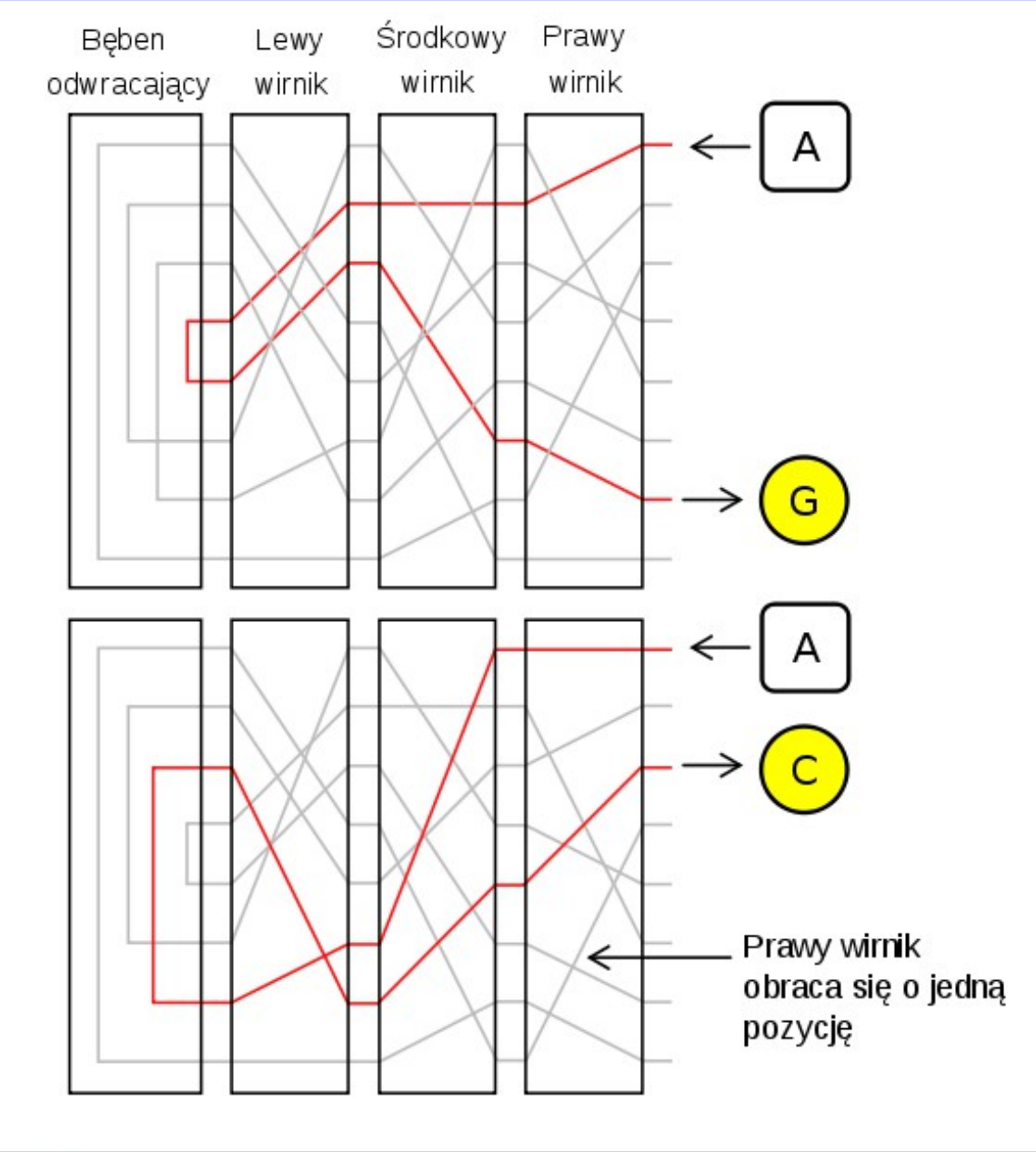

Q W E R T Z U I O
A S D F H J K
F Y X C V B N M L


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


B
03
02
01
26
25
03
02
01
26
25
18
17
16
15
14
13




02
01
26
25
24


Bęben odwracający
Lewy wirnik
Środkowy wirnik
Prawy wirnik
A
G
A
C
Prawy wirnik obraca się o jedną pozycję

Szyfrowanie

Z klucza dziennego: wirniki II,III,I;
reflektor B, pozycja początkowa BEC

A D K A D K → O W F W E C

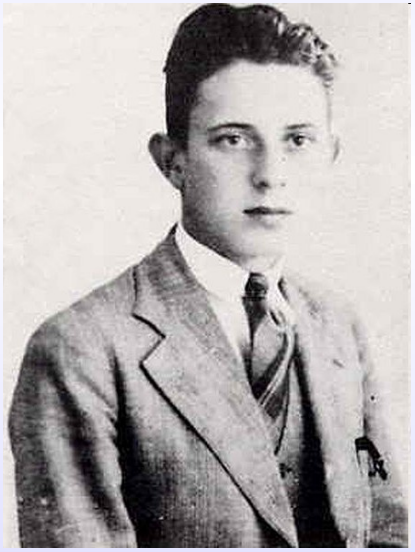
Zmiana pozycji początkowej na ADK

E N I G M A → V E A B S X

Szyfrogram: OWFWECVEABSX

Łamanie szyfru

- Polacy – Marian Rejewski, Jerzy Różycki, Henryk Zygalski – 1932, Biuro Szyfrów



- słynne Bletchley Park

Ocalałe egzemplarze w Polsce

- Muzeum Techniki
- Muzeum Wojska Polskiego
- Muzeum Wojska w Białymstoku
- Muzeum Oręża Polskiego w Kołobrzegu