Tajemnice szyfrów

Barbara Roszkowska Lech

MATEMATYKA DLA CIEKAWYCH ŚWIATA

marzec 2017

WYDZIAŁ
MATEMATYKI I NAUK
INFORMACYJNYCH

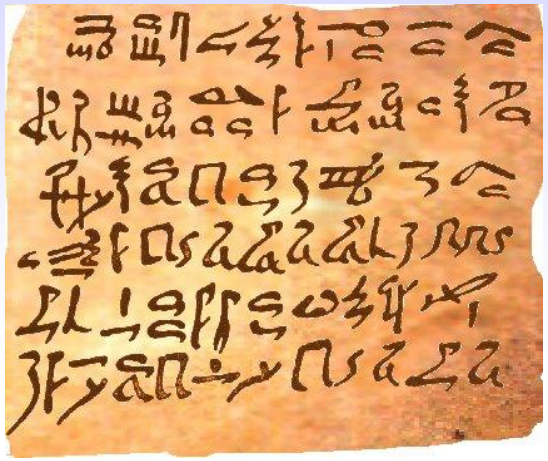
Dążenie do odkrywania tajemnic tkwi głęboko w naturze człowieka,
a nadzieja dotarcia tam, dokąd inni nie dotarli, pociąga umysły najmniej nawet skłonne do dociekań.
Niektórym udaje się znaleźć zajęcie polegające na rozwiązywaniu tajemnic... Ale większość z nas musi zadowolić się rozwiązywaniem zagadek ułożonych dla rozrywki: powieściami kryminalnymi i krzyżówkami. Odczytywaniem tajemniczych szyfrów pasjonują się nieliczne jednostki.

John Chadwick

Historia kryptografii

- Początek

Na początku było pismo

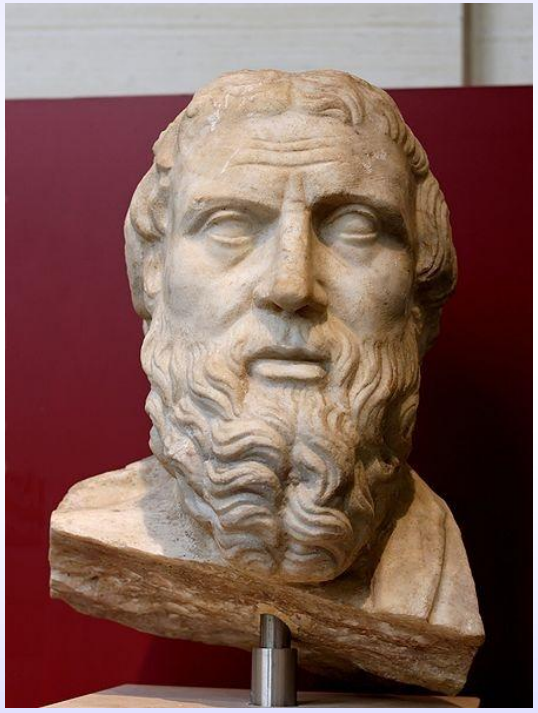


- Steganografia

(steganos- zakryty)

zajmuje się ukrywaniem istnienia 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.	Everest zdobyty.
Wiatr nadal dokuczliwy.	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

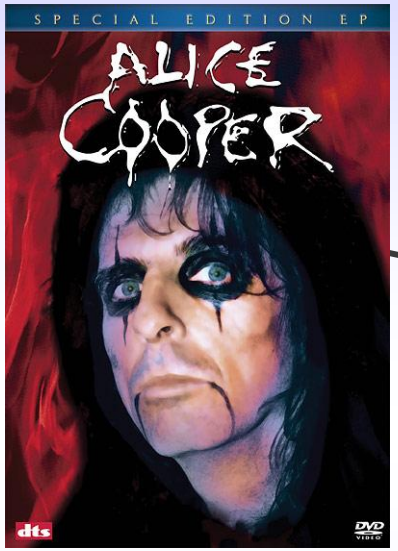
Kryptologia

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

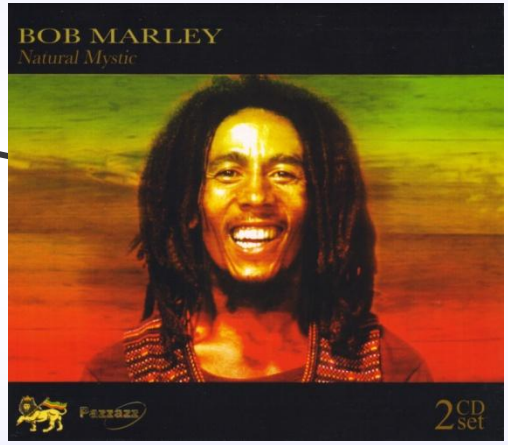
Kryptografia

- 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

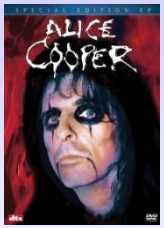


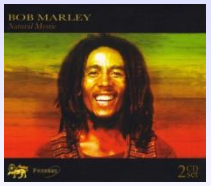
Bolek

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
(kryptosystem symetryczny)

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

Kryptografia

- Kryptografia (kryptos)
  zajmuje się ukrywaniem znaczenia wiadomości

- Starożytny Egipt 2000BC

- Mezopotamia – 1900 p.n.e. zapiski o stosowaniu szyfrów
- II wiek p.n.e. Polibiusz

Tablica Polibiusza

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

- Kryptografia w celach politycznych
  Indie IV w p.n.e.
- Szyfr z Kamasutry

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

SPOTKANIE
NYQZJVSGU

Szyfry symetryczne

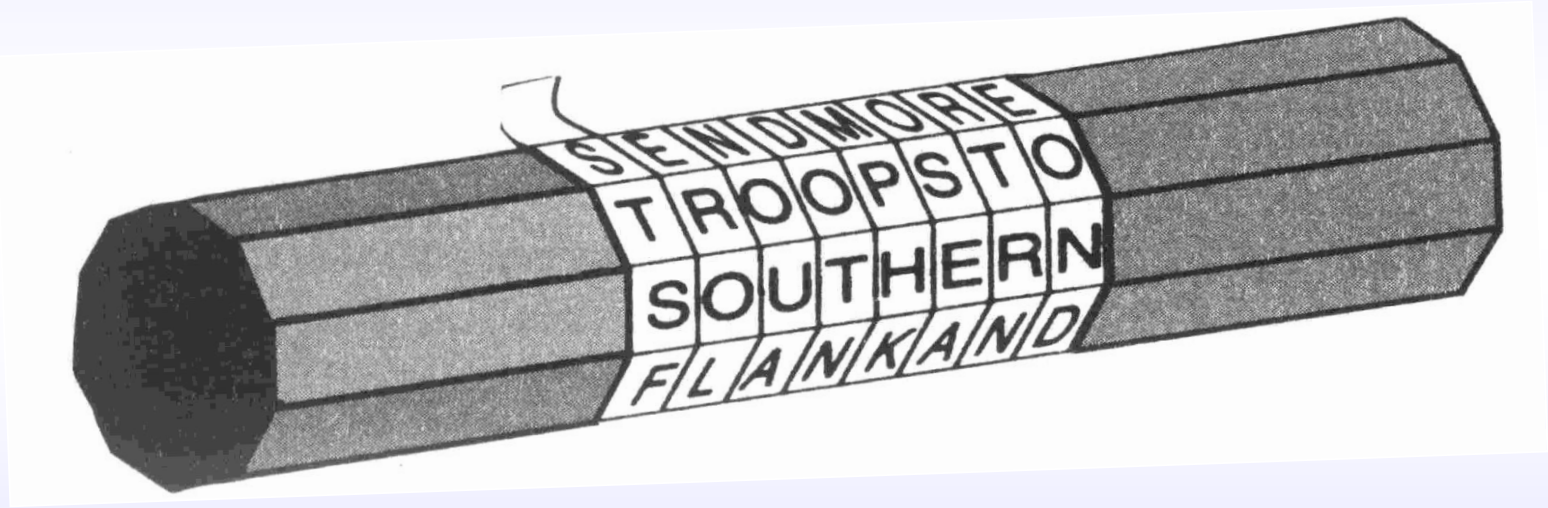
- Przestawieniowe (permutacyjne)

  tekst jawny i szyfrogram składają się z tych samych znaków tylko w innej kolejności

- Podstawieniowe

  tekst jawny i szyfrogram składają się z różnych symboli

Scytale urzadzenie szyfrujące



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

Wróg zna nasz system tylko nie zna klucza

Kolejnym literom alfabetu łacińskiego przyporządkujemy liczby od 0 do 25.

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

Kongruencje, czyli arytmetyka zegarowa

$$a \equiv b \pmod{n} \leftrightarrow n \text{ dzieli } a-b$$

Warunek $a \equiv b \pmod{n}$ jest spełniony wtedy i tylko wtedy gdy a oraz b dają te same reszty z dzielenia przez n

Przykład: $111 \equiv 7 \pmod{8}$

Odwracanie mod n

- Liczba odwrotna do liczby a modulo n jest liczbą b spełniającą kongruencję $a \cdot b \equiv 1 \pmod{n}$

Obliczmy odwrotność 3 mod 4:

$3 \cdot 0 \equiv 0 \pmod{4}$ nie

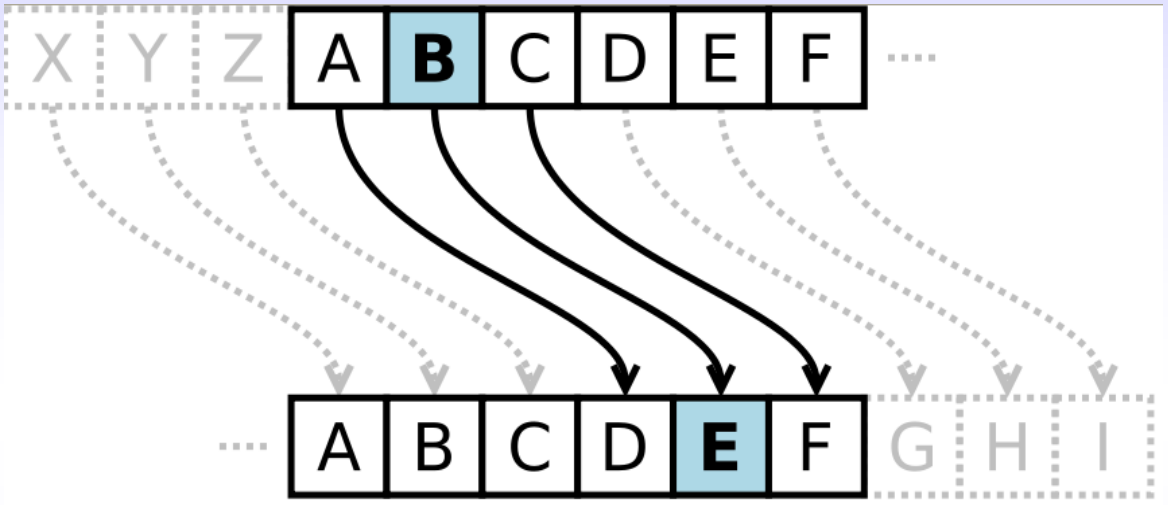
$3 \cdot 1 \equiv 3 \pmod{4}$ nie

$3 \cdot 2 \equiv 2 \pmod{4}$ nie

$3 \cdot 3 \equiv 1 \pmod{4}$ tak

Czyli liczbą odwrotną do 3 mod 4 jest 3.

Szyfr Cezara



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

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

Inne przykłady szyfrowania

- $E(m) = am \pmod n$

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

- $E(m) = am+b \pmod n$

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

Kryptologia

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

Narodziny kryptoanalizy

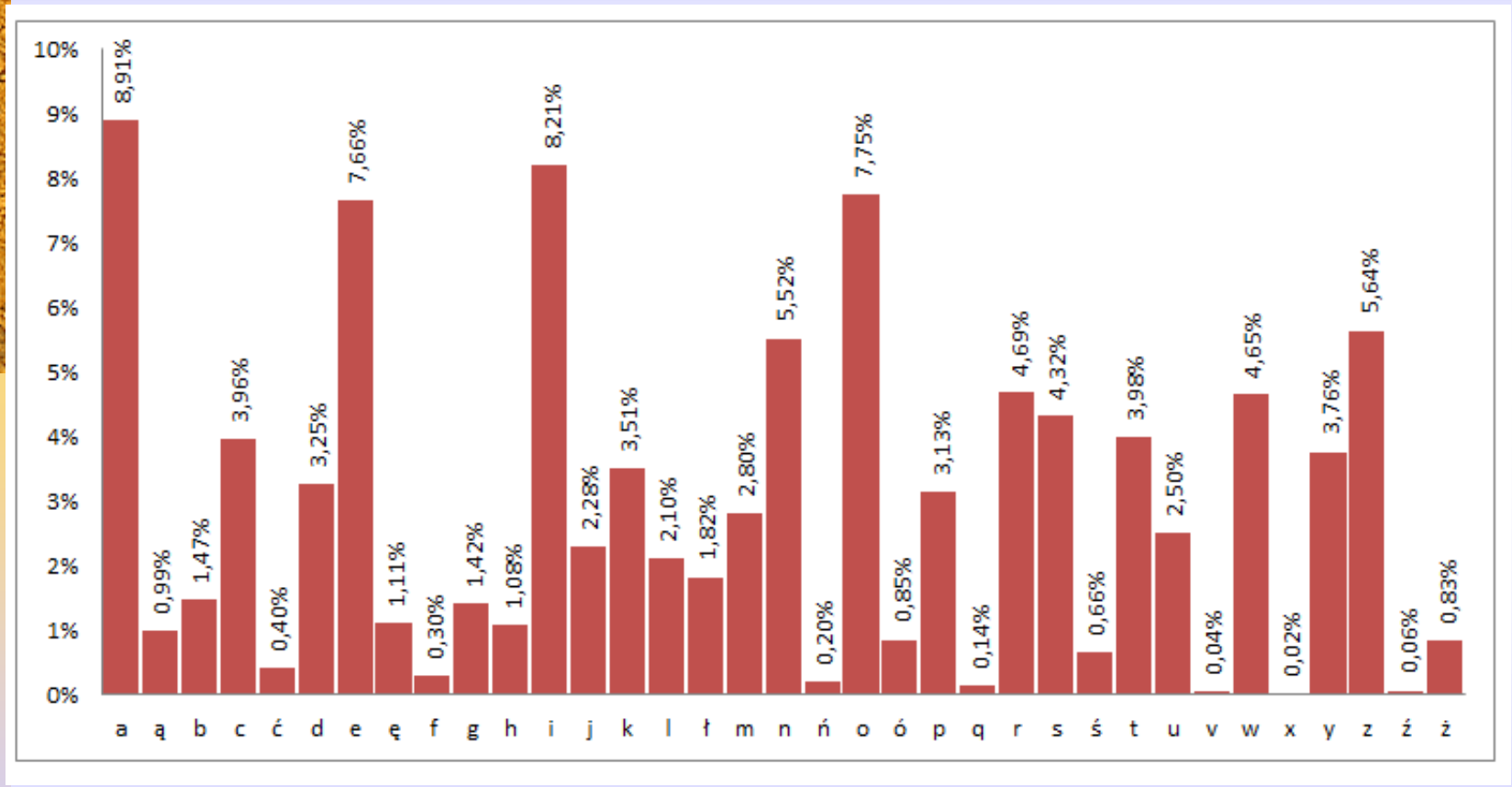
Al Kindi IX

- Filozof Arabów
- 29 traktatów (matematyka, medycyna, muzyka, astronomia, lingwistyka)
- „O odczytywaniu zaszyfrowanych listów”
- Opisuje metodę analizy częstości

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		

Częstość występowania liter w alfabecie polskim

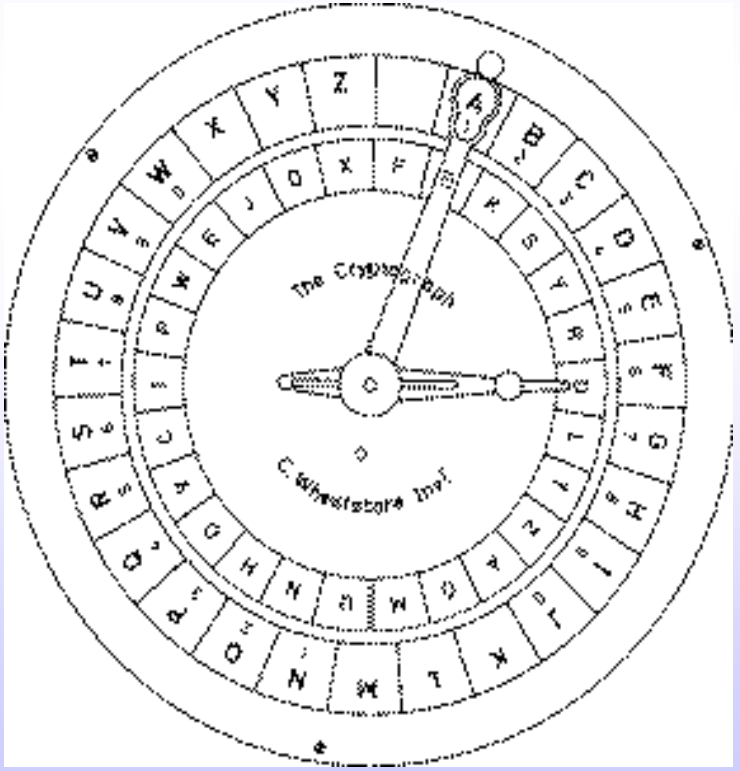


Szyfry wieloalfabetowe

Leon Battista Alberti
(1404-1472)

Człowiek renesansu

Autor traktatu kryptograficznego



Szyfry wieloalfabetowe

Johanes Trithemius

1462-1516

Autor pierwszego podręcznika kryptografii

Jeden z prekursorów szyfrów wieloalfabetowych

Tabula recta

Tabula recta

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

Szyfry wieloalfabetowe

- Francuski dyplomata, tłumacz, chemik, kryptograf
- Przypisuje mu się autorstwo kryptosystemu Vigenera
- Autor „Traktatu o szyfrach”

Blaise de Vigenere
(1523-1596)

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

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

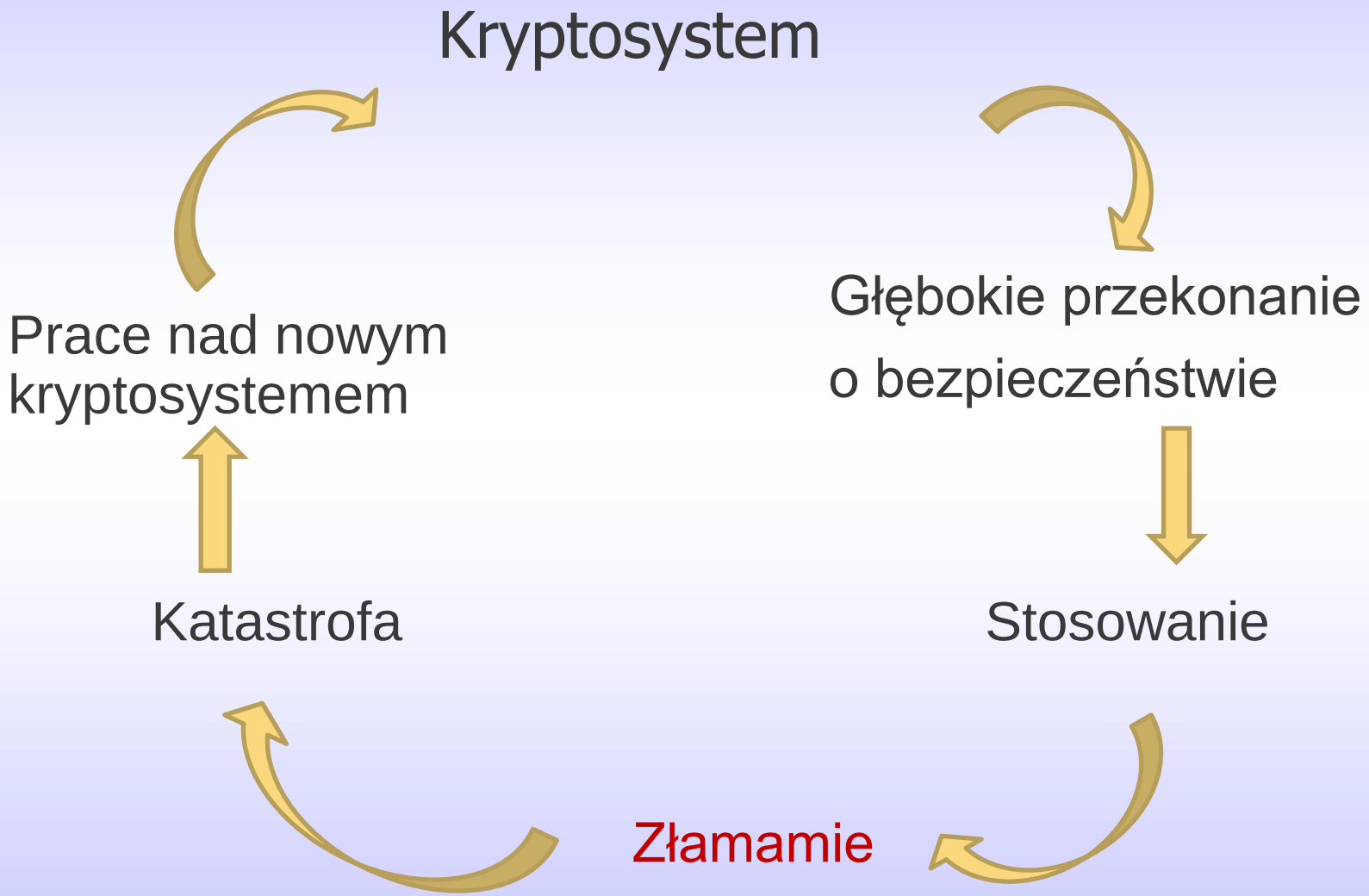
Szyfrowanie

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

Deszyfrowanie

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

Historia Kryptografii 2000 BC-1976



Szyfr Marii Stuart

Złamany dzięki analizie częstości

Ofiara udanej kryptoanalizy

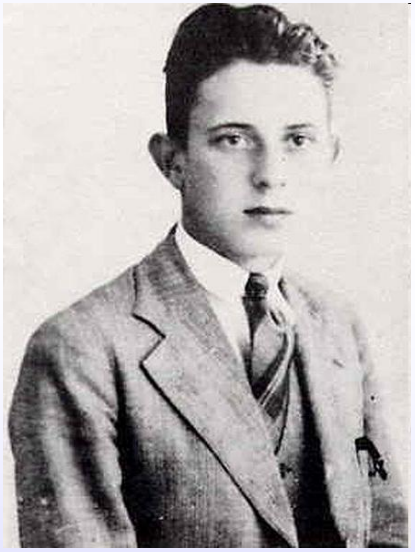
Maria Stuart i Elżbieta królowa Anglii

Enigma

- Enigma używana w niemieckiej armii od końca lat 20. XX w do zakończenia II wojny światowej
- Ponad 100^{13} możliwych ustawień wirników i bębenków
- Super komputer potrzebuje więcej niż 10^{17} lat aby sprawdzić wszystkie możliwości
- Kryptosystem złamany

Łamanie szyfru

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



- słynne Bletchley Park

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**

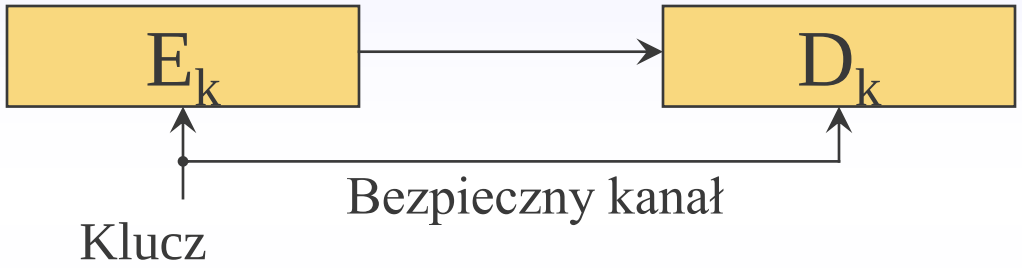
LI **CE** **UM**

NL **DT** **MK**

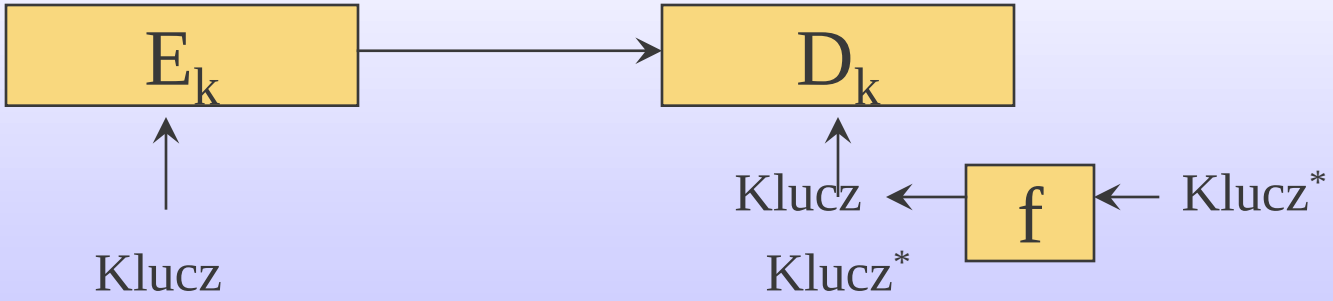
Kryptogram **NLDTMK**

Systemy kryptograficzne

- Symetryczny system kryptograficzny (z kluczem tajnym)

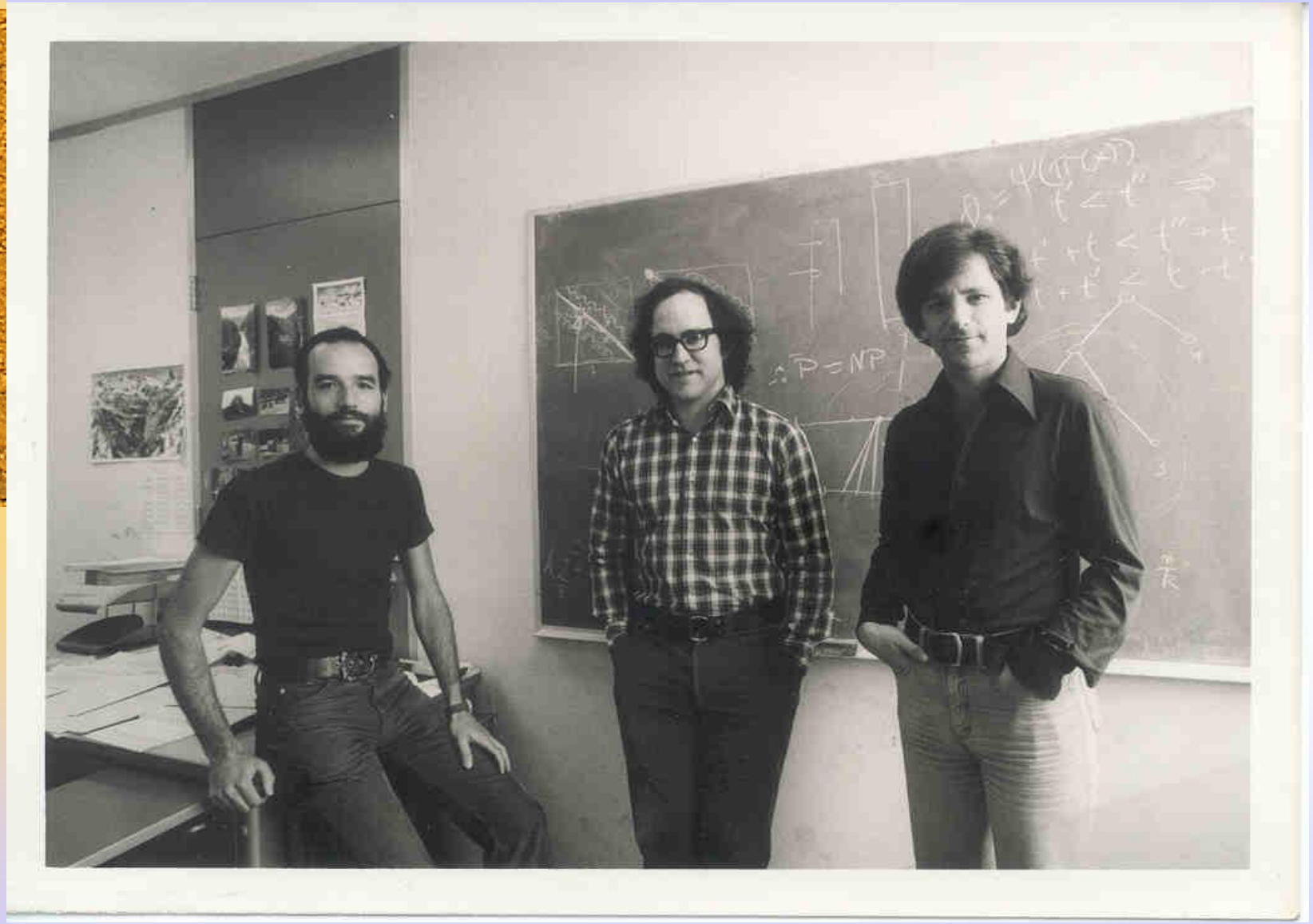


- Asymetryczny system kryptograficzny (z kluczem publicznym)



RSA (tryumf matematyki)

- Ron Rivest, Adi Shamir, Leonard Adleman, "A Method for Obtaining Digital Signatures and Public Key Cryptosystems", *Communications of the ACM*, Vol. 21, no. 2, February 1978, 120-126.
- Rewolucja w kryptografii!!!
- www.rsa.com



Adi Shamir,Ron Rivest, Leonard Adleman MIT

Liczby pierwsze na straży naszych tajemnic

Razem z ojcami, którzy na spłodzili
Pochwalmy teraz liczby pierwsze:
Ich moc, ich przedziwna sława
Stąd płynie, że nikt ich nie spłodził;
Nie mają przodków i czynników
Adamowie wśród mnożących się pokoleń
Skąd przybywają –nie wie nikt
Nie rezerwują sobie miejsc
wśród innych naturalnych liczb
Przychodzą nie oczekiwane

Helen Spalding

Dziękuję za uwagę!