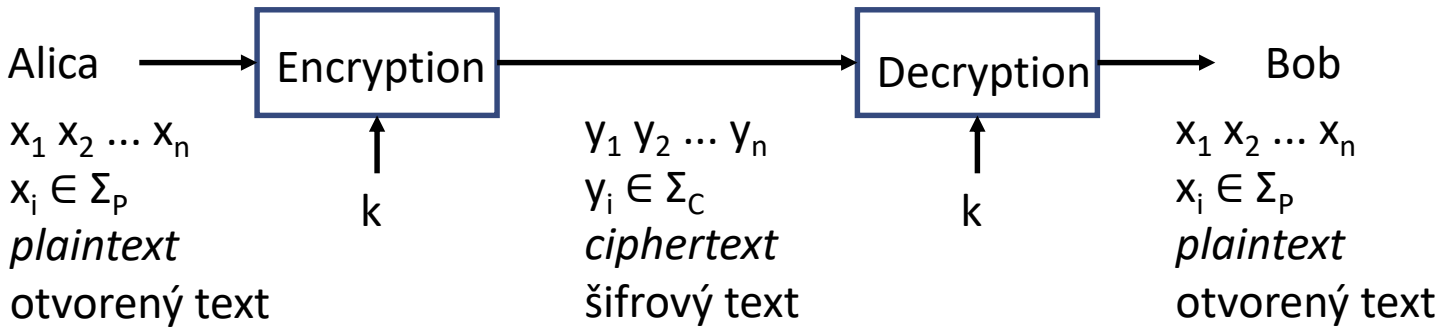
Kryptografické systémy
Klasické šifry a šifrovacie stroje

doc. RNDr. Jozef Jirásek, PhD.

ZS 2023

Klasické symetrické šifrovacie systémy



- posuvná šifra
- monoalfabetická (jednoduchá) substitúcia (*simple substitution*)
- bigramová šifra (Playfair, Hill)

kryptoanalýza

Polyalfabetické šifry

využívajú viacero abecied – šifrovacia a dešifrovacia funkcia závisí aj od pozície znaku v texte

sťaží sa tak možnosť využitia frekvenčnej analýzy

Polyalfabetické šifry

využívajú viacero abecied – šifrovacia a dešifrovacia funkcia závisí aj od pozície znaku v texte

sťaží sa tak možnosť využitia frekvenčnej analýzy

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

Vigenèrova šifra

- Giovan Battista Bellaso (1553)
- tabula recta (Trithemius 1508)
- neskôr omylom pripísaná Blaise de Vigenèrovi

	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
A	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	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	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	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	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	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	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
H	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
I	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
J	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
K	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
L	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
M	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
N	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
O	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
P	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
Q	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
R	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
S	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
T	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
U	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
V	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
W	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
X	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
Y	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
Z	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

posuvná šifra s posunom, závislým od pozície znaku v texte

posun určuje kľúčové slovo (expandované na dĺžku otvoreného textu)

Vigenèrova šifra

PT	K	R	Y	P	T	O	G	R	A	F	I	A
K	U	P	J	S	U	P	J	S	U	P	J	S
	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓

PT	N	A	U	P	J	S	J	E
K	U	P	J	S	U	P	J	S
	↓	↓	↓	↓	↓	↓	↓	↓

PT	S	U	P	E	R
K	U	P	J	S	U
	↓	↓	↓	↓	↓

	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
A	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	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	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	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	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	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	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
H	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
I	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
J	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
K	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
L	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
M	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
N	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
O	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
P	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
Q	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
R	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
S	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
T	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
U	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
V	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
W	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
X	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
Y	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
Z	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

Vigenèrova šifra - šifrovanie

PT	K	R	Y	P	T	O	G	R	A	F	I	A
K	U	P	J	S	U	P	J	S	U	P	J	S
	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
CT	E											

PT	N	A		U	P	J	S		J	E
K	U	P		J	S	U	P		J	S
	↓	↓		↓	↓	↓	↓		↓	↓

PT	S	U	P	E	R
K	U	P	J	S	U
	↓	↓	↓	↓	↓

	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
A	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	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	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	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	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	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	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
H	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
I	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
J	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
K	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
L	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
M	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
N	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
O	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
P	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
Q	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
R	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
S	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
T	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
U	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
V	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
W	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
X	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
Y	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
Z	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

Vigenèrova šifra - šifrovanie

PT	K	R	Y	P	T	O	G	R	A	F	I	A
K	U	P	J	S	U	P	J	S	U	P	J	S
	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
CT	E	G										

PT	N	A		U	P	J	S		J	E
K	U	P		J	S	U	P		J	S
	↓	↓		↓	↓	↓	↓		↓	↓

PT	S	U	P	E	R
K	U	P	J	S	U
	↓	↓	↓	↓	↓

	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
A	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	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	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	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	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	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	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
H	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
I	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
J	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
K	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
L	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
M	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
N	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
O	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
P	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
Q	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
R	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
S	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
T	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
U	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
V	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
W	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
X	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
Y	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
Z	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

Vigenèrova šifra - šifrovanie

PT	K	R	Y	P	T	O	G	R	A	F	I	A
K	U	P	J	S	U	P	J	S	U	P	J	S
	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
CT	E	G	H	H								

PT	N	A	U	P	J	S	J	E
K	U	P	J	S	U	P	J	S
	↓	↓	↓	↓	↓	↓	↓	↓

PT	S	U	P	E	R
K	U	P	J	S	U
	↓	↓	↓	↓	↓

	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
A	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	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	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	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	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	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	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
H	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
I	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
J	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
K	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
L	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
M	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
N	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
O	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
P	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
Q	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
R	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
S	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
T	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
U	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
V	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
W	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
X	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
Y	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
Z	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

Vigenèrova šifra - šifrovanie

PT	K	R	Y	P	T	O	G	R	A	F	I	A
K	U	P	J	S	U	P	J	S	U	P	J	S
	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
CT	E	G	H	H	N	D	P	J	U	U	R	S

PT	N	A		U	P	J	S		J	E
K	U	P		J	S	U	P		J	S
	↓	↓		↓	↓	↓	↓		↓	↓
CT	H	P		D	H	D	H		S	W

PT	S	U	P	E	R
K	U	P	J	S	U
	↓	↓	↓	↓	↓
CT	M	J	Y	W	L

	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
A	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	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	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	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	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	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	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
H	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
I	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
J	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
K	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
L	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
M	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
N	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
O	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
P	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
Q	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
R	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
S	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
T	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
U	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
V	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
W	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
X	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
Y	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
Z	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

Vigenèrova šifra - dešifrovanie

CT	E	G	H	H	N	D	P	J	U	U	R	S
K	U	P	J	S	U	P	J	S	U	P	J	S
	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
PT	K											

CT	H	P		D	H	D	H		S	W
K	U	P		J	S	U	P		J	S
	↓	↓		↓	↓	↓	↓		↓	↓

CT	M	J	Y	W	L
K	U	P	J	S	U
	↓	↓	↓	↓	↓

	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
A	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	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	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	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	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	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	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
H	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
I	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
J	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
K	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
L	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
M	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
N	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
O	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
P	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
Q	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
R	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
S	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
T	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
U	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
V	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
W	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
X	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
Y	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
Z	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

Vigenèrova šifra - dešifrovanie

CT	E	G	H	H	N	D	P	J	U	U	R	S
K	U	P	J	S	U	P	J	S	U	P	J	S
	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
PT	K	R										

CT	H	P	D	H	D	H	S	W
K	U	P	J	S	U	P	J	S
	↓	↓	↓	↓	↓	↓	↓	↓

CT	M	J	Y	W	L
K	U	P	J	S	U
	↓	↓	↓	↓	↓

	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
A	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	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	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	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	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	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	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
H	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
I	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
J	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
K	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
L	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
M	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
N	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
O	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
P	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
Q	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
R	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
S	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
T	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
U	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
V	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
W	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
X	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
Y	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
Z	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

Vigenèrova šifra - dešifrovanie

CT	E	G	H	H	N	D	P	J	U	U	R	S
K	U	P	J	S	U	P	J	S	U	P	J	S
	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
PT	K	R	Y									

CT	H	P		D	H	D	H		S	W
K	U	P		J	S	U	P		J	S
	↓	↓		↓	↓	↓	↓		↓	↓

CT	M	J	Y	W	L
K	U	P	J	S	U
	↓	↓	↓	↓	↓

	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
A	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	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	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	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	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	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	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
H	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
I	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
J	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
K	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
L	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
M	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
N	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
O	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
P	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
Q	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
R	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
S	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
T	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
U	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
V	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
W	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
X	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
Y	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
Z	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

Vigenèrova šifra - dešifrovanie

CT	E	G	H	H	N	D	P	J	U	U	R	S
K	U	P	J	S	U	P	J	S	U	P	J	S
	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
PT	K	R	Y	P	T	O	G	R	A	F	I	A

CT	H	P		D	H	D	H		S	W
K	U	P		J	S	U	P		J	S
	↓	↓		↓	↓	↓	↓		↓	↓
PT	N	A		U	P	J	S		J	E

CT	M	J	Y	W	L
K	U	P	J	S	U
	↓	↓	↓	↓	↓
PT	S	U	P	E	R

	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
A	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	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	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	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	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	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	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
H	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
I	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
J	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
K	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
L	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
M	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
N	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
O	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
P	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
Q	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
R	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
S	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
T	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
U	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
V	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
W	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
X	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
Y	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
Z	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

Vigenèrova šifra – kryptoanalýza

postupujeme v dvoch krokoch:

- nájdeme dĺžku kľúča
- nájdeme kľúč

Vigenèrova šifra – kryptoanalýza

postupujeme v dvoch krokoch:

- nájdeme dĺžku kľúča
- nájdeme kľúč

ak vieme dĺžku kľúča r – stačí analyzovať postupnosti $(y_1\ y_{r+1}\ y_{2r+1}\ y_{3r+1}\ ..)$, $(y_2\ y_{r+2}\ y_{2r+2}\ y_{3r+2}\ ..)$, ... $(y_r\ y_{2r}\ y_{3r}\ ..)$ šifrového textu pomocou frekvenčnej analýzy ...

postupne nájdeme posuny, z ktorých rekonštruujeme kľúč

Vigenèrova šifra – hľadanie dĺžky kľúča

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

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

Kasiského metóda (1863, tiež Babbage 1846)

- vzdialenosti medzi opakujúcimi sa reťazcami znakov v šifrovom texte sú s veľkou pravdepodobnosťou násobkami dĺžky kľúča
- gcd týchto vzdialeností je hľadaná dĺžka (jej násobok)

Vigenèrova šifra – kryptoanalýza koincidenciou

miera nerovnomernosti pravdepodobností výskytov znakov –
stredná kvadratická odchýlka (MSE) od rovnomernej prevdepodobnosti 1/26

$$\sum_{i=1}^{26}(p_i - \frac{1}{26})^2 = \sum_{i=1}^{26}(p_i)^2 - 2 \cdot \sum_{i=1}^{26} p_i \cdot \frac{1}{26} + \sum_{i=1}^{26}\left(\frac{1}{26}\right)^2 = \sum_{i=1}^{26}(p_i)^2 - \frac{1}{26}$$

kde $IC = \sum_{i=1}^{26}(p_i)^2$ nazývame **index koincidencie**
(tiež pravdepodobnosť, že 2 náhodne vybraté znaky textu budú rovnaké)

pre náhodný text $IC_R = \sum_{i=1}^{26}(\frac{1}{26})^2 = 1/26 \approx 0.0385$

text so známymi pravdepodobnosťami p_i výskytov i-tych znakov
$IC_E = \sum_{i=1}^{26} p_i^2 = (0.082^2 + 0.015^2 + \dots) \approx 0.066$ pre angličtinu

pre slovenčinu bez diakritiky ≈ 0.06, s diakritikou a interpunkciou ≈ 0.055

postupne pre r = 1, 2, ... počítame IC pre texty (y_1 y_{r+1} y_{2r+1} y_{3r+1} ..), (y_2 y_{r+2} y_{2r+2} y_{3r+2} ..), ... (y_r y_{2r} y_{3r} ..), pokiaľ budú nadobúdať hodnoty, blízke 0.066 (teda frekvencia výskytu znakov bude približne odpovedať anglickému textu) – príslušné r bude pravdepodobne dĺžka kľúča (resp. jeho násobok)

Vigenèrova šifra – dĺžka kľúča koincidenciou

```
  E G H H L F A G J X A R M E X D M J E G H H L F U C J D Q Q I J S
E G H H L F A G J X A R M E X D M J E G H H L F U C J D Q Q I J S W

W N P O R X N S E U K N D E Z E G H H L F A G J X A T E N Y J W J H T
N P O R X N S E U K N D E Z E G H H L F A G J X A T E N Y J W J H T


            E G H H L F A G J X A R M E X D M J E G H H L F U C J D
E G H H L F A G J X A R M E X D M J E G H H L F U C J D Q Q I J S W

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

jednoduchý test (s využitím pravdepodobnosti výberu zhodnej dvojice) – počet zhôd pri posúvaní šifrovaného textu – pri posunutí o násobok dĺžky kľúča budú pod sebou znaky anglického textu (index koincidencie 0.066), inokedy náhodné znaky (index 0.04)

prejaví sa až pri dostatočne dlhom šifrovanom texte ...

Vigenèrova šifra – analýza vektormi pravdepodobností

A_0 = (0.082, 0.015, ...) postupnosť pravdepodobností výskytov jednotlivých znakov v anglickej abecede

A_1 = (0.01, 0.082, 0.015, ...) postupnosť pravdepodobností posunutá o 1

... tvoria vektory pravdepodobností so skalárnym súčinom
$A_0 \,.\, A_0 = 0.082^2 + 0.015^2 + \ldots \approx 0.066 \approx A_i \,.\, A_i$ (odpovedá IC)

pre rôzne i, j bude $A_i \,.\, A_j = |A_i|.|A_j|.\cos\varphi < A_i \,.\, A_i$
(pre texty s rovnomerným rozdelením 26 rôznych znakov
$T_1 \,.\, T_2 \approx 26 * (1/26)^2 = 1/26 \approx 0.04 \approx A_i \,.\, A_j$ pre $i \neq j$)

pstupne pre r = 1, 2, ... počítame pre postupnosti
$(y_1\ y_{r+1}\ y_{2r+1}\ y_{3r+1}\ ..)$, $(y_2\ y_{r+2}\ y_{2r+2}\ y_{3r+2}\ ..)$, ... $(y_r\ y_{2r}\ y_{3r}\ ..)$
s rozdelením pravdepodobností W súčin W . W a porovnáme s invariantom (pre anglický text 0.066) ($W \,.\, W \approx IC$)

Vigenèrova šifra – analýza vektormi pravdepodobností

pre nájdenú dĺžku kľúča r analyzujeme postupnosti
$(y_1\ y_{r+1}\ y_{2r+1}\ y_{3r+1}\ ..)$, $(y_2\ y_{r+2}\ y_{2r+2}\ y_{3r+2}\ ..)$, ... $(y_r\ y_{2r}\ y_{3r}\ ..)$

W = (0.001, 0.03, 0.01, ...) - pravdepodobnosti výskytov znakov v analyzovanej postupnosti

- W je posunutá postupnosť výskytov znakov v zdrojovom texte, teda pre A_j , kde j odpovedá dĺžke posunu, bude $A_j \approx W$
- skalárny súčin $(A_i\ .\ W)$ bude maximálny pre i = j

Autokey (Vigenèr)

PT	K	R	Y	P	T	O	G	R	A	F	I	A
K	U	P	J	S	K	R	Y	P	T	O	G	R
	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓

PT	N	A	U	P	J	S	J	E
K	A	F	I	A	N	A	U	P
	↓	↓	↓	↓	↓	↓	↓	↓

PT	S	U	P	E	R
K	J	S	J	E	S
	↓	↓	↓	↓	↓

kľúč sa neopakuje, ale kľúčom sa postupne stáva otvorený text, posunutý o dĺžku kľúča

Autokey (Vigenèr) - šifrovanie

PT	K	R	Y	P	T	O	G	R	A	F	I	A
K	U	P	J	S	K	R	Y	P	T	O	G	R
	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
	E	G	H	H	D	F	E	G	T	T	O	R

PT	N	A		U	P	J	S		J	E
K	A	F		I	A	N	A		U	P
	↓	↓		↓	↓	↓	↓		↓	↓
	N	F		C	P	W	S		D	T

PT	S	U	P	E	R
K	J	S	J	E	S
	↓	↓	↓	↓	↓
	B	M	Y	I	J

kľúč sa neopakuje, ale kľúčom sa postupne stáva otvorený text, posunutý o dĺžku kľúča

Autokey (Vigenèr) - dešifrovanie

CT	E	G	H	H	D	F	E	G	T	T	O	R
K	U	P	J	S	K	R	Y	P				
	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
PT	K	R	Y	P								

CT	N	F		C	P	W	S		D	T
K										
	↓	↓		↓	↓	↓	↓		↓	↓

CT	B	M	Y	I	J
K					
	↓	↓	↓	↓	↓

najskôr dešifrujeme podľa kľúča,
potom podľa dešifrovaného textu

Autokey (Vigenèr) - dešifrovanie

CT	E	G	H	H	D	F	E	G	T	T	O	R
K	U	P	J	S	K	R	Y	P	T	O	G	R
	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
PT	K	R	Y	P	T	O	G	R	A	F	I	A

CT	N	F		C	P	W	S		D	T
K	A	F		I	A	N	A		U	P
	↓	↓		↓	↓	↓	↓		↓	↓
PT	N	A		U	P	J	S		J	E

CT	B	M	Y	I	J
K	J	S	J	E	S
	↓	↓	↓	↓	↓
PT	S	U	P	E	R

najskôr dešifrujeme podľa kľúča, potom podľa dešifrovaného textu

COA kryptoanalýza zložitejšia – možno využiť charakteristiky konvolúcie otvoreného textu

KPA – stačí poznať dešifrovaný reťazec o dĺžke kľúča niekde v šifrovanom texte ...

Možnosti kryptoanalýzy

- poznám len šifrovaný text, algoritmus šifrovania a charakteristiku otvoreného textu -
  COA – *ciphertext only attack*
- poznám aspoň jednu dvojicu otvoreného a šifrovaného textu
  KPA – *known-plaintext attack*
- môžem si nechať niečo zašifrovať
  CPA – *chosen-plaintext attack*
- môžem si nechať niečo dešifrovať
  CCA – *chosen-ciphertext attack*
- adaptívne varianty CPA a CCA

Entropia (binárna) otvoreného textu

- Entropia – miera neusporiadanosti pre systém, ktorý nadobúda hodnoty $x_1 \dots x_n$ z X s pravdepodobnosťami $p_1 \dots p_n$
  $\mathrm{H}(X) = -\sum_{i=1}^{n} p_i \log(p_i)$ (pre rovnomerné rozdelenie $H(X) = \log n$)
- $\mathrm{I}(x_i) = -\log_2(p_i)$ (binárny) informačný príspevok hodnoty x_i (počet bitov na reprezentáciu hodnoty x_i - pre rovnomerné rozdelenie 26 hodnôt $-\log_2(1/26) = \log_2(26) \approx 4.7$ bitov)
- H(náhodný reťazec znakov) $= -\sum_{i=1}^{26} \left(\frac{1}{26}\right) \log_2(\frac{1}{26}) \approx 4.7$
- H_{SK}(reťazec znakov podľa výskytov v SK texte) ≈ 4.23 bitov/znak
- $\mathrm{H}_{\mathrm{EN}}(\dots)$ ≈ 4.15 bitov/znak
- $\mathrm{H}_{\mathrm{EN}}(dvojice)$ ≈ 3.65 bitov/znak (podmienené pravdepodobnosti)
- $\mathrm{H}_{\mathrm{EN}}(trojice)$ ≈ 3.22 bitov/znak
- $\mathrm{H}_{\mathrm{EN}}(l \rightarrow inf)$ ≈ 1.5 bitov/znak (cca 75 % bitov z 8b kódu textu je navyše)

Vzdialenosť jednoznačnosti (*unicity distance*)

aký dlhý šifrový text potrebujem na COA analýzu ?

redundancia textov Y dĺžky n znakov:

$$D_n = n \cdot \log_2(26) - H(Y)$$

≈ o koľko bitov je PT dlhší ako binárny reťazec potrebný na jeho zápis

vzdialenosť jednoznačnosti : $n_0 = \min\{n \mid D_n \geq H(K)\}$

„nadbytočné“ bity PT umožňujú jednoznačne určiť kľúč

(pre menšie n by pre texty jazyka Y bolo viac riešení)

- pre jednoduchú substitučnú šifru (EN)
  - H(K) = $\log_2(26!)$ ≈ 88.38 (ak sú kľúče rovnako pravdepodobné)
  - $D_n = n \cdot 4.7 - n \cdot 1.5 = 3.2\,n$ ($H(Y) \approx n \cdot H_{EN}$)
  - $3.2n \geq 88.38 \Rightarrow n \geq 28$ stačí pre jednoznačné riešenie
    (s jednoduchou f.a. H(Y) ≈ n · 4.15 potom n ≥ 161)
- pre Vigenèrovu šifru s dĺžkou kľúča m $\approx 1{,}5m$

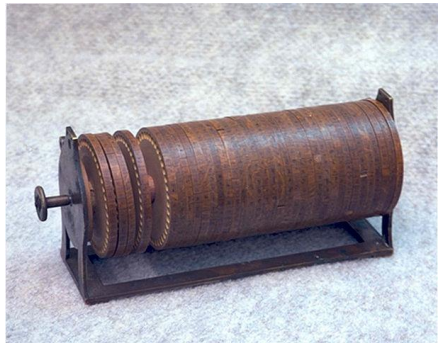
Šifrovacie stroje

Zariadenia na uľahčenie šifrovania

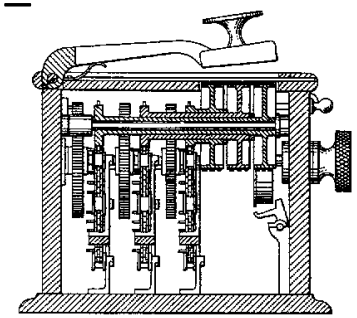
- Albertiho disk (1467)
  (znaky pre zmenu abecedy)

- Jeffersonov disk – 10 otáčacích valcov kľúčom je ich usporiadanie
  (v riadku sa nastaví otvorený text, iný riadok potom bude šifrový text)

  https://en.wikipedia.org/wiki/Jefferson_disk



- Hillov polygrafický šifrátor



Kerckhoffs (1883) - La cryptographie militaire

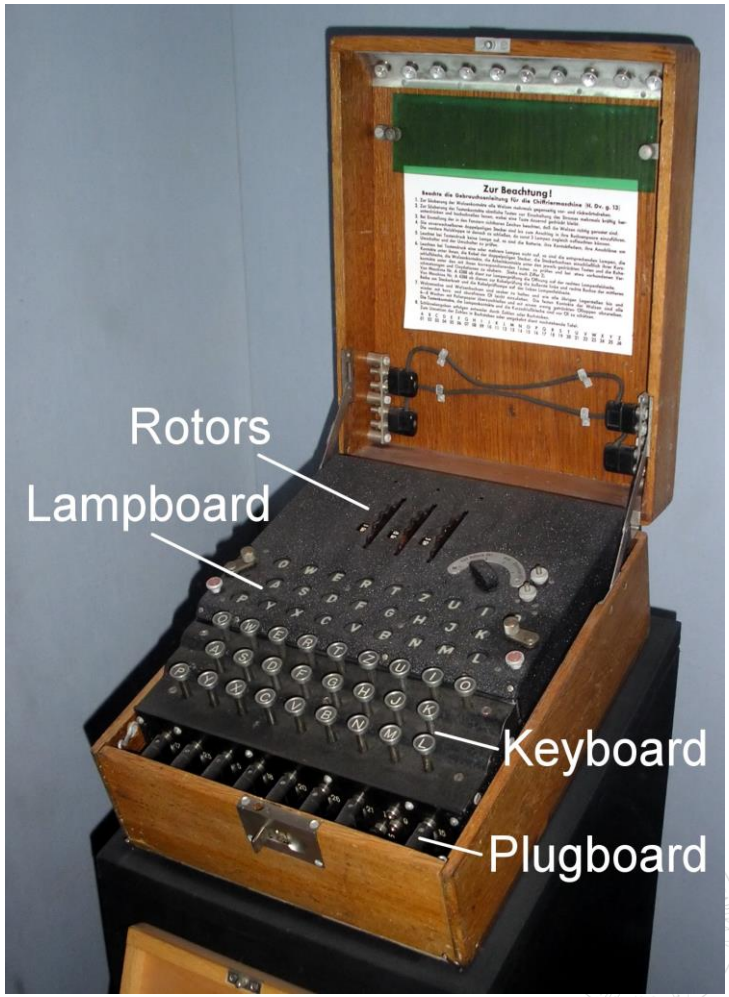
- kryptografický systém je bezpečný, ak útočník nie je schopný dešifrovať text ani vtedy, keď dokonale pozná postup šifrovania

Dôvernosť komunikácie je zabezpečená len znalosťou kľúča

- kľúč je zapamätateľný a ľahko modifikovateľný
- šifrovaný text je možné prenášať telegraficky
- šifrovacie/dešifrovacie zariadenia musia byť prenosné a ľahko používateľné a nemali by vyžadovať od používateľa dodržiavanie dlhého zoznamu pravidiel
- systém by mal byť prakticky nedešifrovateľný

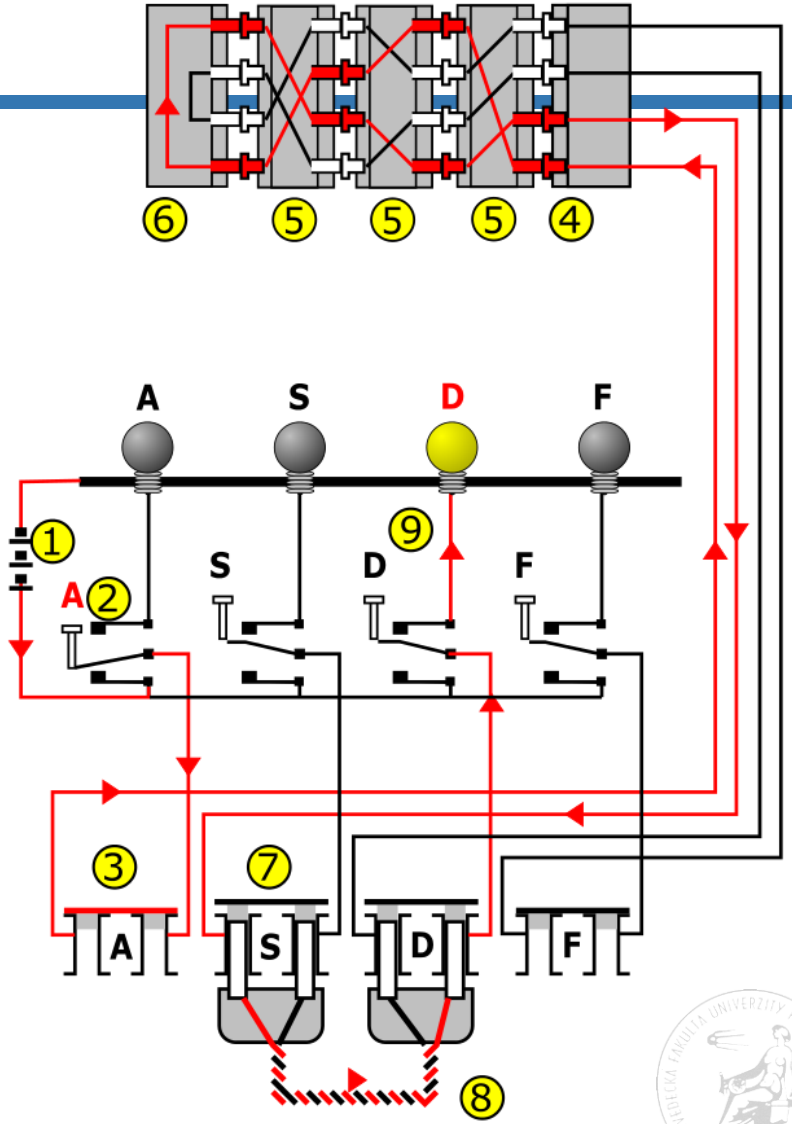
Enigma

- elektromechanický rotorový šifrátor
- Arthur Scherbius (1918) komerčne dostupný (cca 100000 kusov)
- vojenské modely s rôznymi vylepšeniami
- šifra prelomená tesne pred začiatkom vojny (30 rokov v utajení)

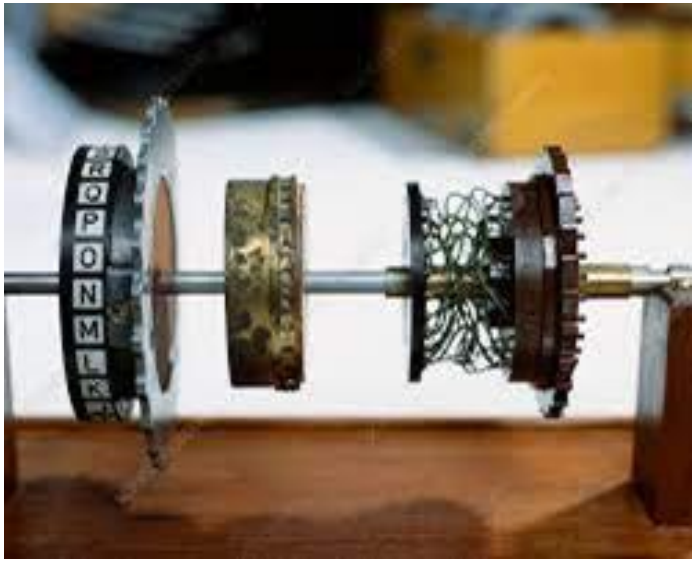


Enigma

- 3 rotory s vymeniteľným poradím (5)
  - 1 rotor sa otáča po napísaní každého písmena
  - 2 rotor sa otáča po 26 písmenách
  - 3 rotor sa otáča po 26*26 písmenách
- postupnosť 26^3 = 17576 rôznych substitúcií

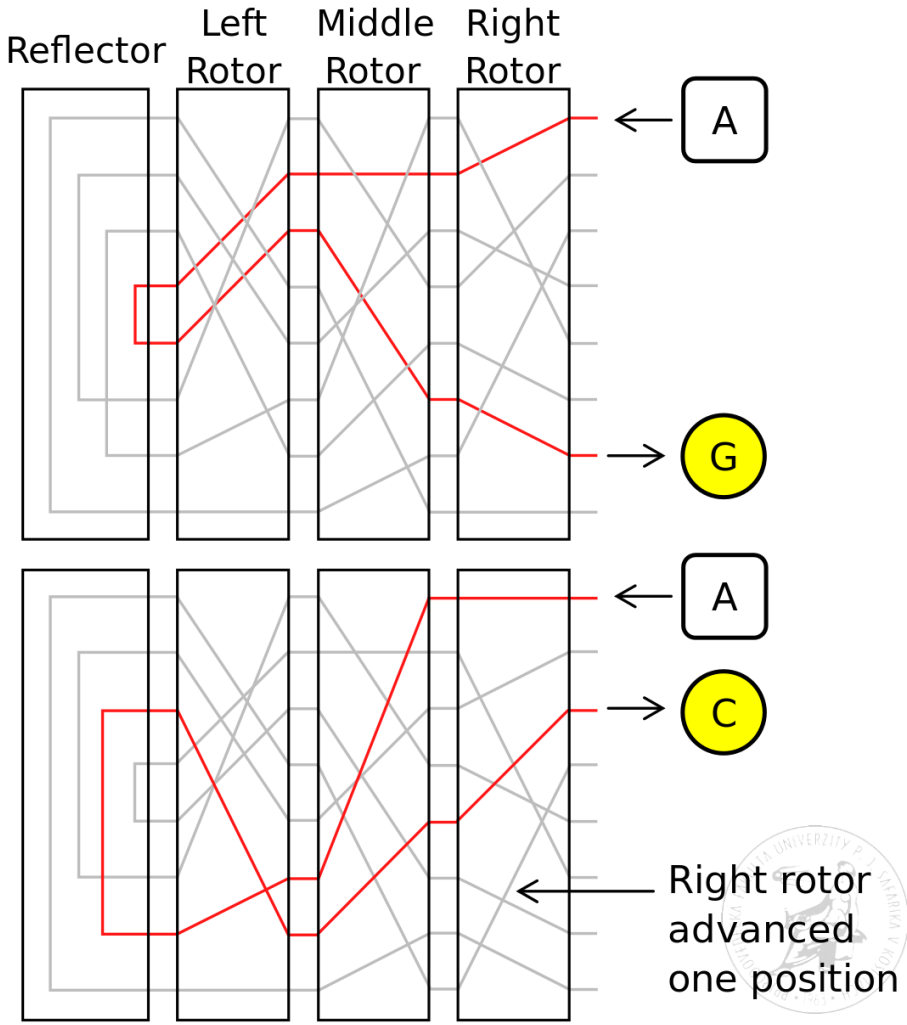


Enigma - rotory



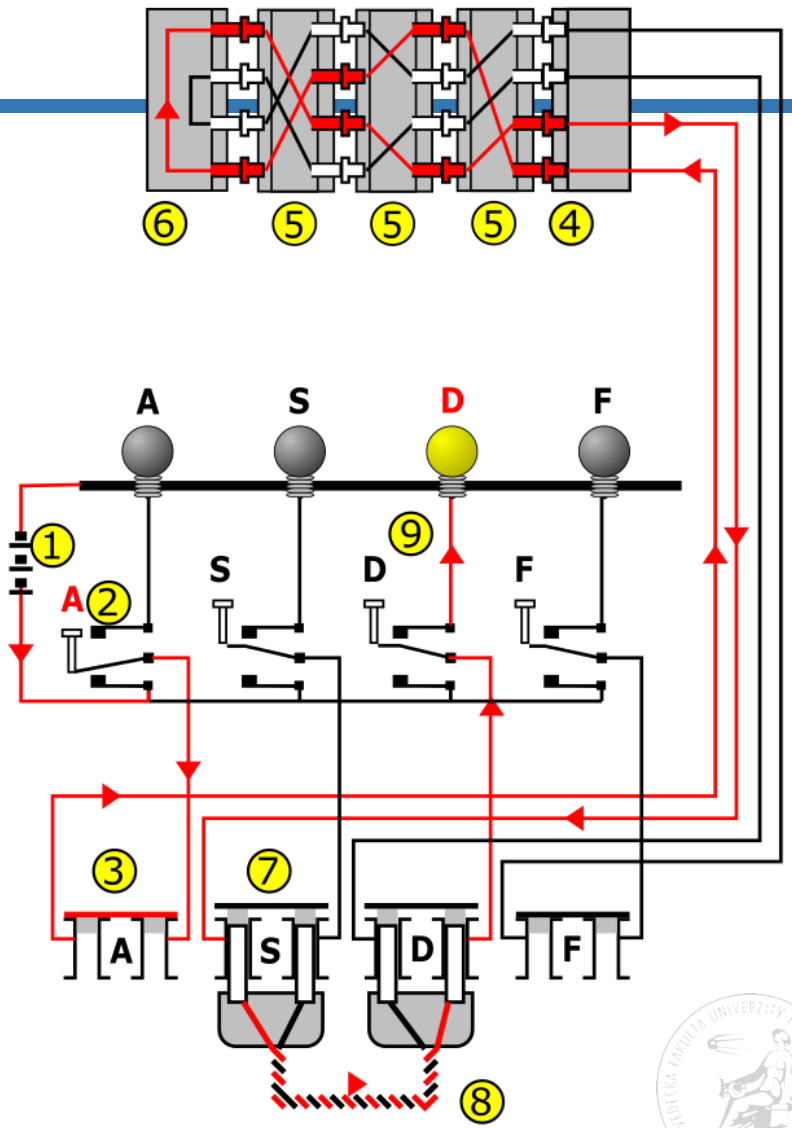
Enigma - reflektor

- reflektor – umožní používať jedno zariadenie na šifrovanie aj dešifrovanie
- nikdy sa nezobrazí znak na seba
- nevýhoda - sú možné len tzv. slabé substitúcie (e(x)=y, e(y)=x, teda e(e(x))=x)



Enigma - plugboard

- pridaný prepojovací panel ⑧
  6 párov prepojení
  100 391 791 500 možností
  (ale pre celé šifrovanie rovnaké – možno použiť frekvenčnú analýzu resp. odhadnúť výmeny)



Enigma – kľúče pred vojnou

- záleží na usporiadaní rotorov – 6 možností
- celkom 6*26*26*26*100391791500 možností nastavenia zariadenia (poradie, začiatočné pozície rotorov a prepojenia)
- denný kľúč – poradie, pozícia rotorov, prepojenia – jednoznačne určujú šifrovanie – ak by sa použilo na viacero správ, pre každú sa použije tá istá postupnosť substitúcií - hrozí frekvenčná analýza !!!
- operátor zvolil pre každú správu trojpísmenový kľúč a ten zašifroval denným kľúčom – ten potom použil na nastavenie rotorov

Enigma – kľúč správy

- pre istotu (!) bolo stanovené, že kľúč správy sa má zašifrovať dvakrát za sebou

napr. kľúč správy HGX zašifroval operátor ako HGXHGX pomocou denného kľúča na DSWEWQ, odoslal DSWEWQ, nastavil rotory na HGX a pokračoval šifrovaním správy

Pri dešifrovaní nastavil Enigmu podľa denného kľúča, dešifroval prvých 6 znakov. Keď dostal dva rovnaké trojpísmenové kľúče, nastavil podľa nich rotory a pokračoval v dešifrovaní.

Geheim!

Sonder-Maschinenschlüssel BGT

Datum	Walzenlage			Ringstellung			Steckerverbindungen										Kenngruppe		
31.	I	V	III	06	20	24	UA	PF	RQ	SO	NI	EY	BG	HL	TX	ZJ	jou	nyq	aqm
30.	V	II	III	01	07	12	GF	KV	JM	;B	UW	LX	TD	QS	NA	ZH	azs	zds	kck
29.	IV	I	V	11	17	26	CI	OK	PV	ZL	HX	NB	AW	DJ	FE	ST	kap	gwh	lyx

Enigma – Rejewského kryptoanalýza

- HGX sa zašifrovalo ako DSW EWQ
  - Zašifrované denným kľúčom
- H je zašifrované 2 krát
  - H -> D ale tiež D -> H
  - H -> E ale tiež E -> H
  - ak zložíme substitúciu na 1. pozícii so substitúciou na 4. pozícii, dostaneme D -> H -> E
    (tu už záleží na poradí, takže nemusí platiť E -> D)
- pokiaľ mám k dispozícii ďalšie správy, začínajúce opakovanou trojicou znakov – budem vedieť o zložení substitúcie 1. a 4. oveľa viac

Enigma – Rejewského kryptoanalýza

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

pre zloženie 1. a 4. substitúcie platí:

B -> G -> P -> D -> O -> F -> W -> H -> Q -> B

A -> C -> I -> K -> E -> T -> M -> L -> X -> A

S -> Z -> R -> Y -> S

V -> U -> J -> N -> V

charakteristika (10,10,5,5) tohoto zloženia nezávisí od plugboardu a je rovnaká pre všetky Enigmy v tento deň

podobne zistíme charakteristiku zloženia 2. a 5. substitúcie a zloženia 3. a 6. substitúcie

Enigma – Rejewského kryptoanalýza

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

Rejewski spočítal charakteristiky zloženia permutácií pre všetky pozície rotora

6*26*26*26 = 105456 možností

a usporiadal ich tak, aby sa dalo podľa charakteristík permutácií rýchle vyhľadať nastavenie rotorov

potom ostala už len substitučná šifra pre plugboard ...

Enigma – počas 2. svetovej vojny

- ďalšie 2 rotory (z 5 sa vyberali 3 – v závislosti na poradí - celkom 60 možností
- ďalšie prepojovacie káble – celkovo 10
- $159 * 10^{18}$ možností - Rejewského prístup nestačil
- kryptoanalýza z Poľska s presunula do Francúzska a potom do Anglicka (Bletchley Park)
- smulátory Enigmy

Enigma – Turingova strojová kryptoanalýza

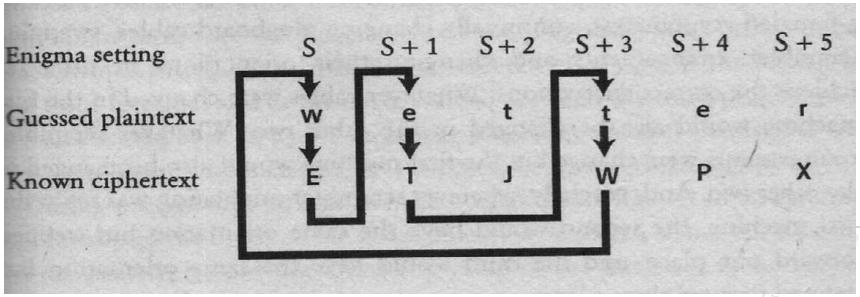
- KPA analýza podľa „ťahákov“ (*cribs*)
- zrána posielali Nemci správy o počasí, v ktorých sa na rovnakých miestach šifroval reťazec WETTER

ak sa reťazec WETTER v daný deň zašifroval napr. na ETJWPX, potom v nejakej pozícii S Enigmy sa zobrazilo W -> E, v pozícii S+1 E -> T a v pozícii S+3 T -> W

vezmem 3 Enigmy a výstup z prvej vo výstupe E napojím na vstup E druhej, výstup T z druhej na vstup T tretej a výstup W z tretej na vstup W prvej

druhú Enigmu posuniem o 1 krok od prvej, tretiu o 3 kroky

pustím paralelne Enigmy a čakám, kedy za uzavrie okruh

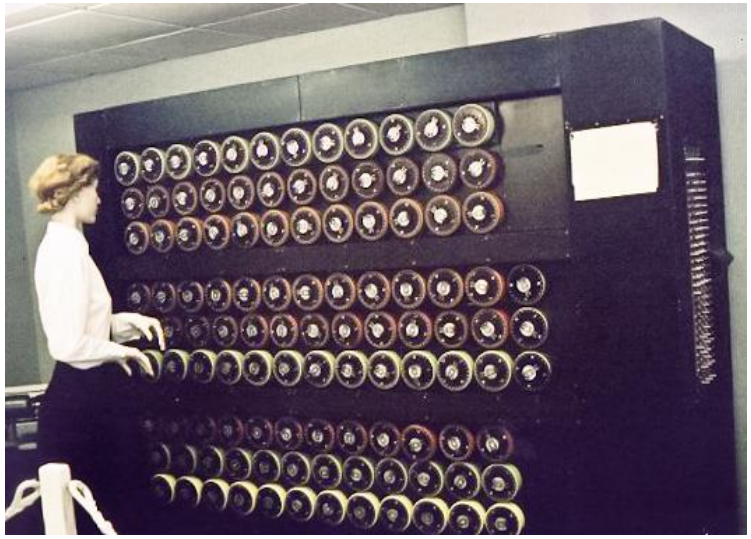


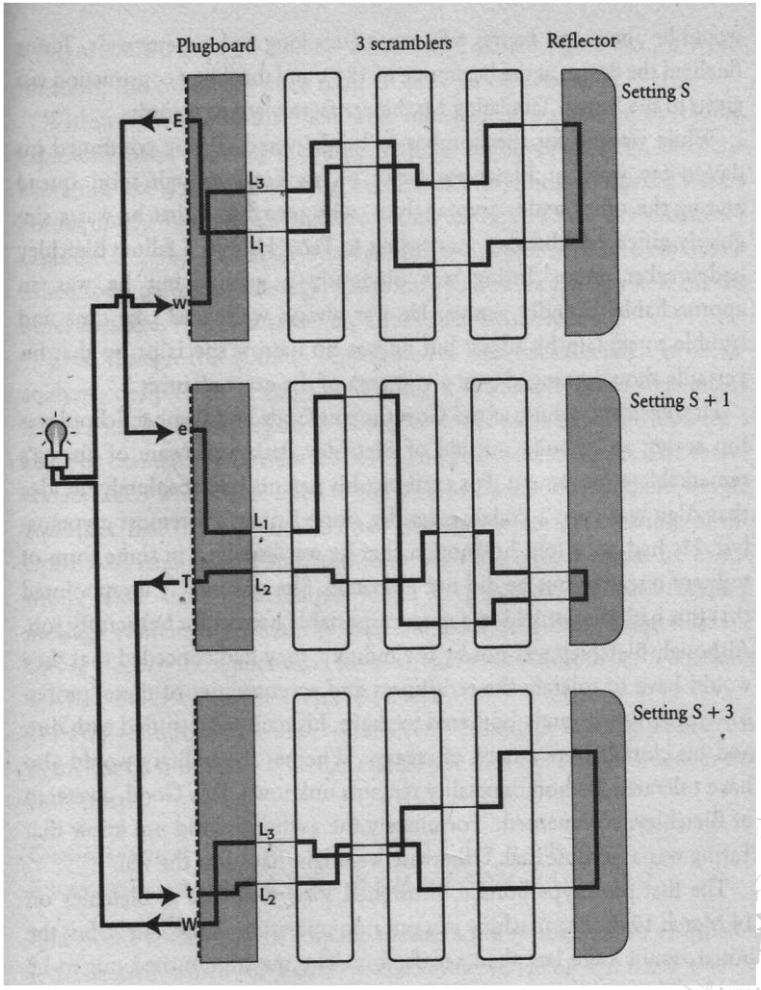
(najviac 17576 krokov pre 3 rotory)

Enigma – Turingove bomby

eliminácia prepojovacej dosky – prepojenie všetkých 26 pozícií priamo na doske (L_1 odpovedá L_1 v druhom stroji, L_2 v druhom L_2 v treťom)

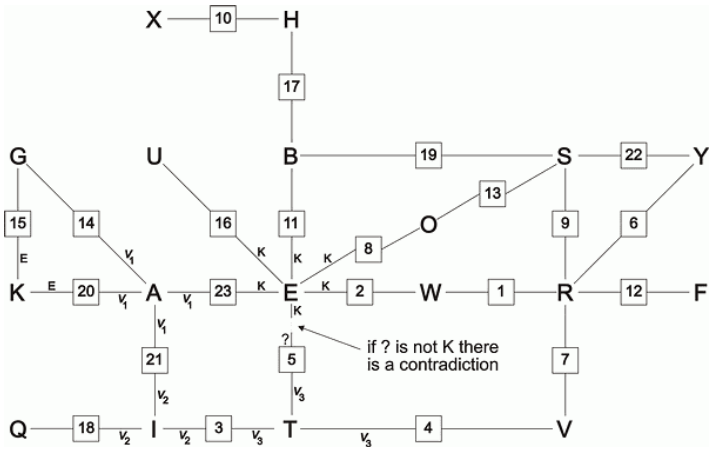
všetko 60 x pre všetky možné kombinácie rotorov





Enigma – zložitejšie ťaháky

- vyhľadávanie viacerých cyklov – paralelné testovanie (šifru je potrebné prelomiť v krátkom čase)

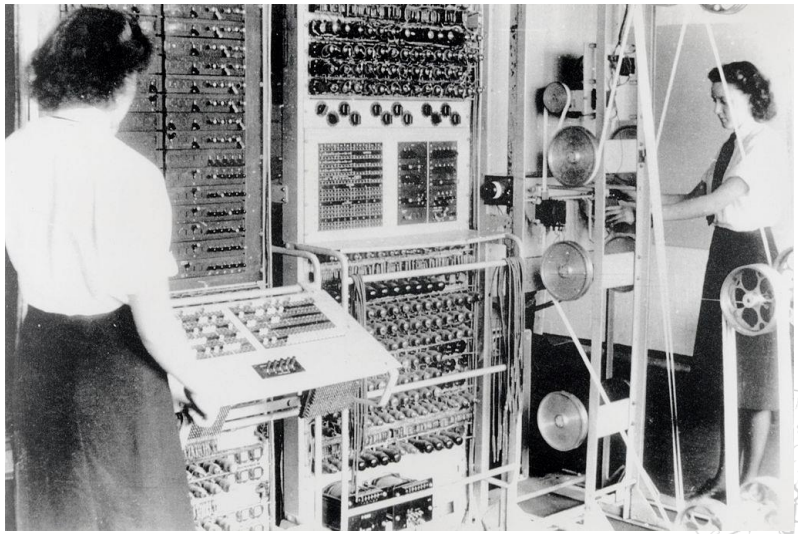



```
Q F Z W R W I V T Y R E S X B F O G K U H Q B A I S E Z
W E T T E R V O R H E R S A G E B I S K A Y A

Q F Z W R W I V T Y R E S X B F O G K U H Q B A I S E Z
  W E T T E R V O R H E R S A G E B I S K A Y A

Q F Z W R W I V T Y R E S X B F O G K U H Q B A I S E Z
    W E T T E R V O R H E R S A G E B I S K A Y A

Q F Z W R W I V T Y R E S X B F O G K U H Q B A I S E Z
      W E T T E R V O R H E R S A G E B I S K A Y A

Q F Z W R W I V T Y R E S X B F O G K U H Q B A I S E Z
        W E T T E R V O R H E R S A G E B I S K A Y A

        R W I V T Y R E S X B F O G K U H Q B A I S E
        W E T T E R V O R H E R S A G E B I S K A Y A
```

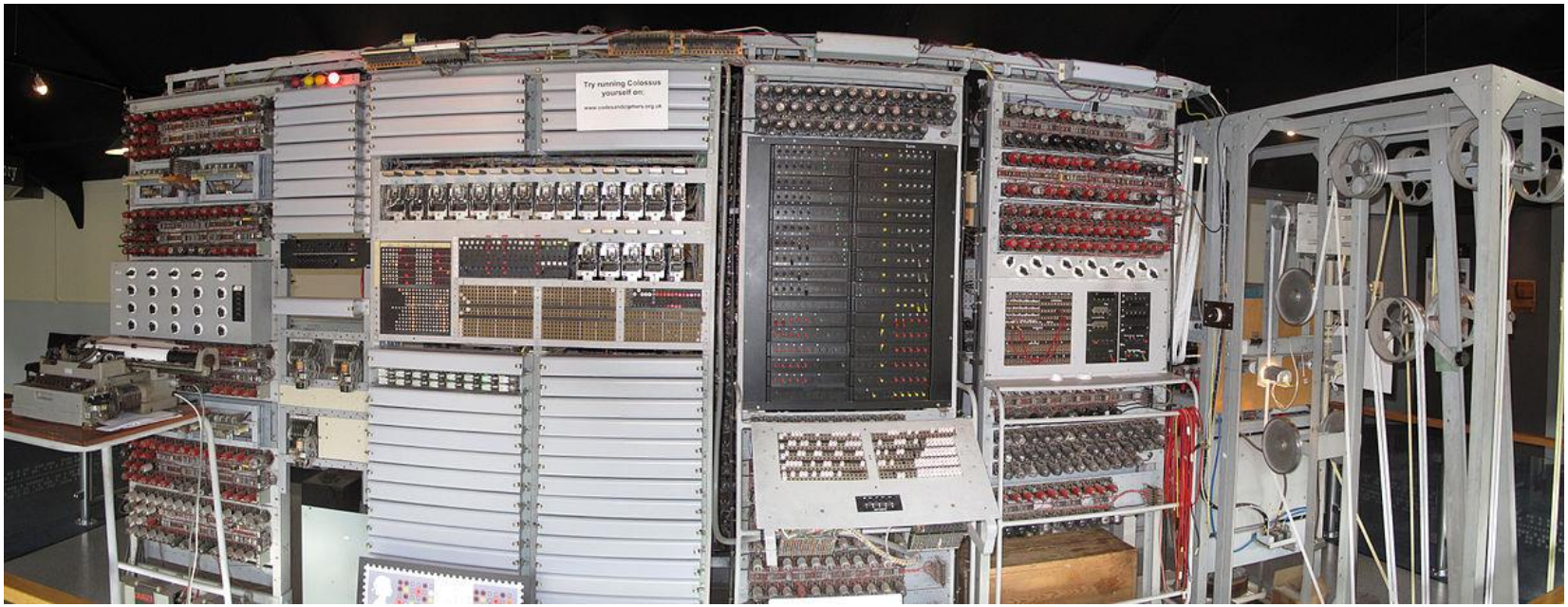
Zdroj:http://www.ellsbury.com/bombe1.htm

Enigma – problémy

- častokrát spor - nemožné riešenia
- mechanické chyby a poškodenia
- pri väčšom počte rotorov už boli krokové relé pomalé
- elektronické riešenie Colossus – kryptoanalýza Lorenzovho šifrátora (12 rotorov)



Colossus - rekonštrukcia



Ďakujem za pozornosť.

jozef.jirasek@upjs.sk