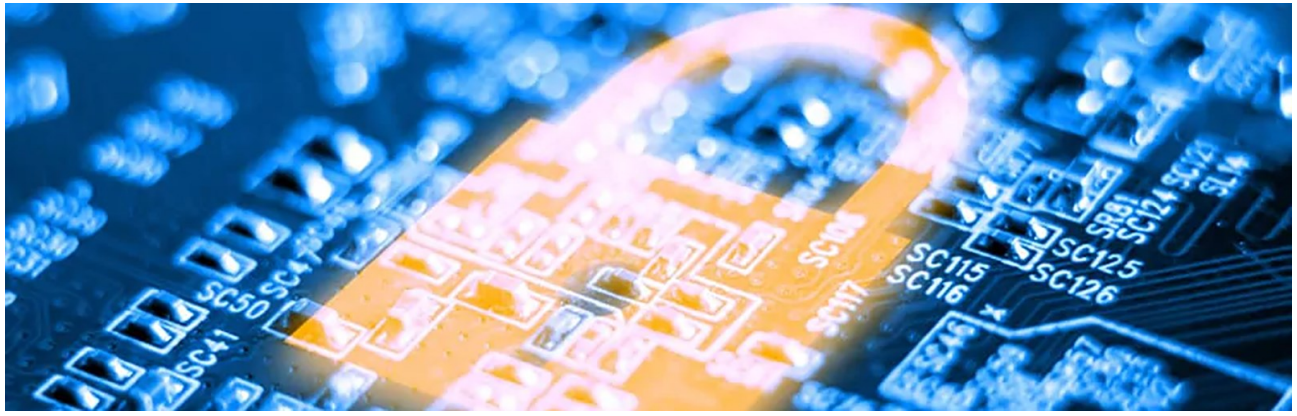
VIEM, ŽE ŠIFRY CHRÁNIA TAJOMSTVÁ...

Soňa Krenická, V.OA

Obsah



Čo je to šifrovanie?

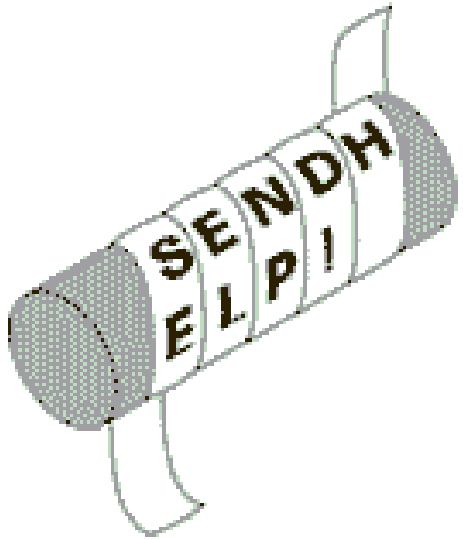
- Šifrovanie – „znečitateľnenie" obsahu správy
- Na dešifrovanie je potrebné poznať kľúč
- Používa sa na utajenie obsahu správ
- Veda – kryptológia

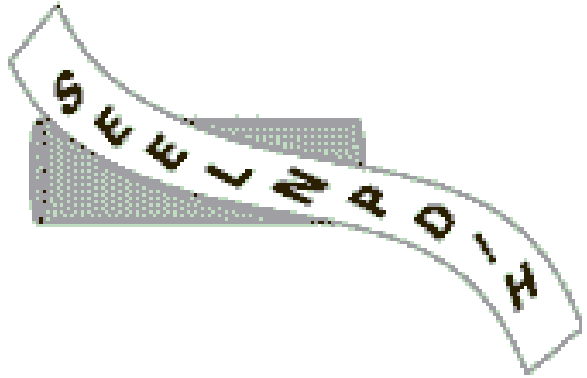
História - Grécko

- stúpanie gramotnosti medzi ľuďmi → utajiť obsah správ
- Prvé šifry spočívali v prehodení písmen v slovách
  - pr. ahoj → ahjo
- Neskôr ľahšie verzie Cézarovej šifry (n+k; k=1)
  - pr. ahoj → bipk
- Cézar (n+k; k=3)

História – Grécko, Sparta

- Scytale
- Kľúčom je valec (rovnaký priemer)
- Správa sa omotá okolo valca
- Samotný text na rozvinutom pásiku nedáva zmysel





História - Izrael

- Atbaš
- Hebreji
- Poradie písmen v abecede

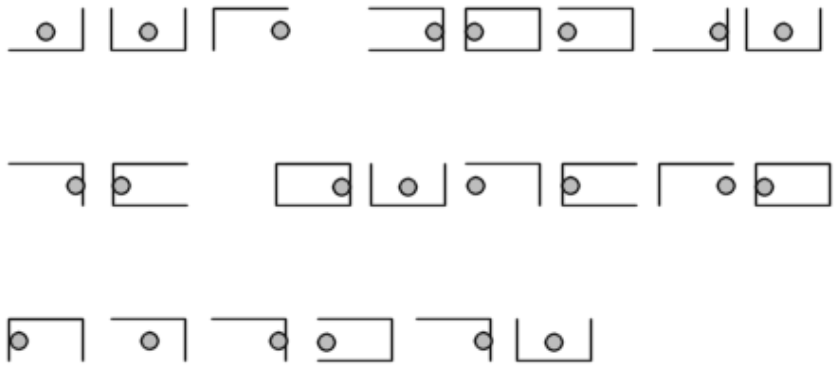
A	B	C	D	E	F	G	H	I	J	K	L	M
Z	Y	X	W	V	U	T	S	R	Q	P	O	N

- pr. ahoj → zslq vietor → ervgli

Šifry

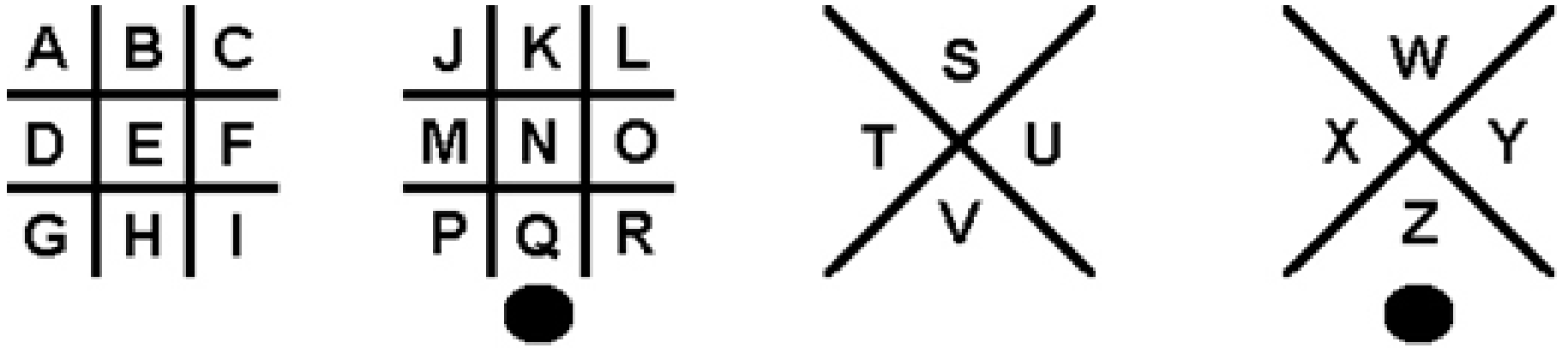
- Veľký poľský kríž

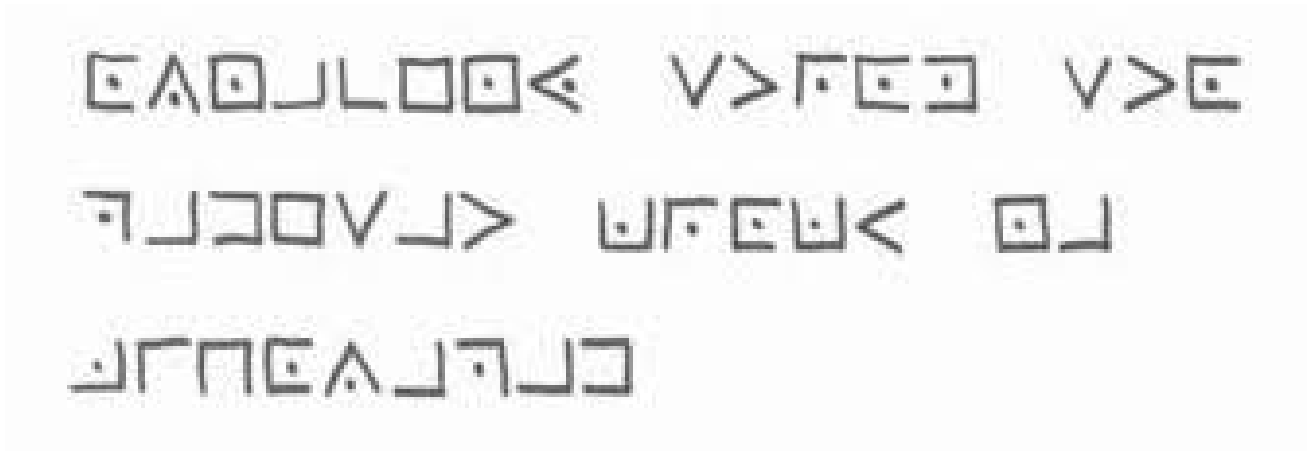
A B C	D E F	G H CH
I J K	L M N	O P Q
R S T	U V W	X Y Z



Šifry

- Malý poľský kríž





Šifry

- „Mobilová šifra"

1	2 abc	3 def
4 ghi	5 jkl	6mno
7 pqrs	8 tuv	9wxyz
*	0	#

44 666 3 66 666 8 2 7 444
7777 6 33 66 33 2 5 33 3
33 888 33 8 6 444 66 88

7777 3 888 2

Šifry

- Vigenèrova šifra
- Kľúč – dohodnuté slovo

text: DOVOLENKAPRIMORI

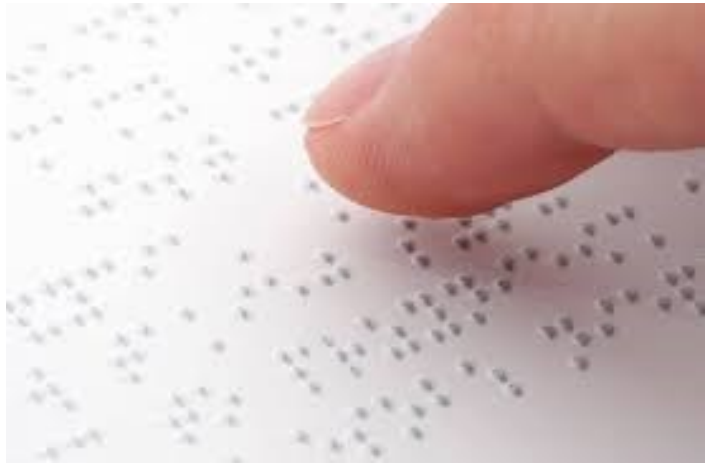
kľúč: MOBILMOBILMOBILM

PCWWWQBLIADWNWCU

	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

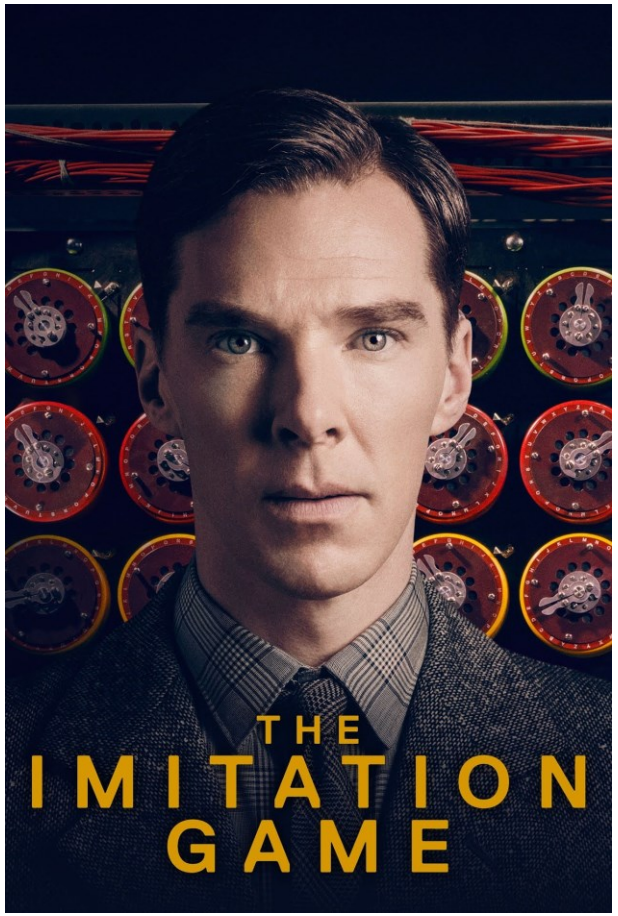
Využitie šifier v súčasnosti

- Morseova abeceda
- Braillovo písmo
- Binárny kód (Aikenov, Grayov...)
- Bitcoin a iné kryptomeny
- TLS (Transport Layer Security)
- TCP (Transmission Control Protocol)



Zaujímavosť

- Enigma – nemecký šifrovací stroj



Kód Enigmy

Zdroje

- https://lnk.sk/ecpq
- https://lnk.sk/tvct
- https://lnk.sk/wkpy
- https://lnk.sk/ha46
- https://lnk.sk/ux12
- https://lnk.sk/mnh5
- https://lnk.sk/eqw7
- https://lnk.sk/elqq
- https://lnk.sk/v267
- https://lnk.sk/xeq5
- https://lnk.sk/kex4
- https://lnk.sk/inoo
- https://lnk.sk/pur1
- https://lnk.sk/xenx
- https://lnk.sk/eny7
- https://lnk.sk/chyx
- https://lnk.sk/czb3
- https://lnk.sk/ydgx
- https://lnk.sk/jnf5
- https://lnk.sk/encg
- https://lnk.sk/jmp9
- https://lnk.sk/xgjm
- Https://lnk.sk/tcr0
- https://lnk.sk/aucs
- https://lnk.sk/jbkr
- https://lnk.sk/hufv

ĎAKUJEM ZA POZORNOSŤ