

A thick black L-shaped frame is positioned on the left and bottom edges of the slide, framing the central text.

ŘEŠENÍ ŠIFER A LOGICKÝCH ÚLOH

Karel Pazourek

Třeboň, 14. 11. 2018

Druhy šifer a logických úloh

- Hádanky, rébusy...
- Znakové šifry:
 - *Substituční*
 - *Transpoziční*
- Grafické šifry
- Asociační šifry

Substituční šifry

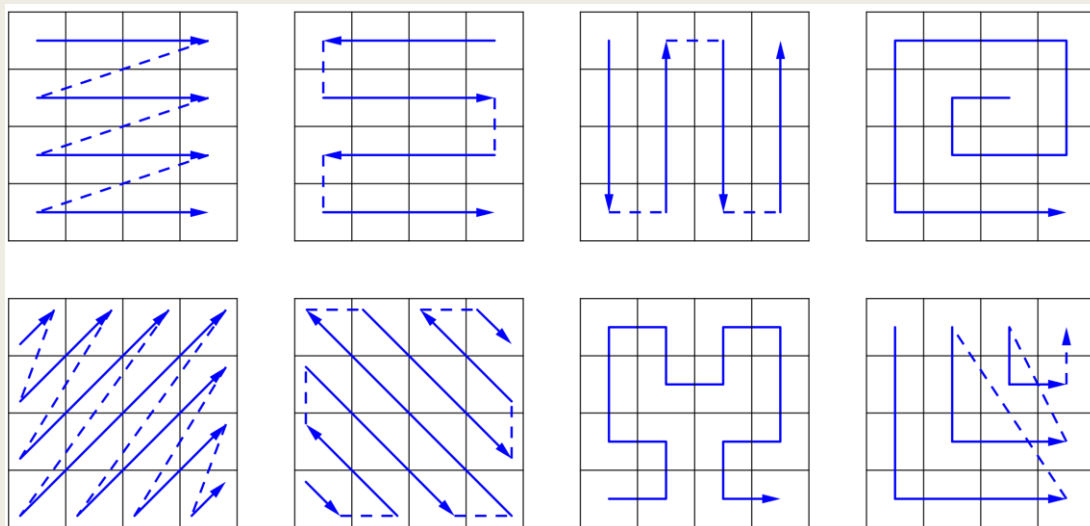
- Nahrazení znaku za jiný znak (obrázek, ...)
- Posuny v abecedě
- Přičítání hesla
- Nahrazování dvojic znaků, slov,...

Substituční šifry

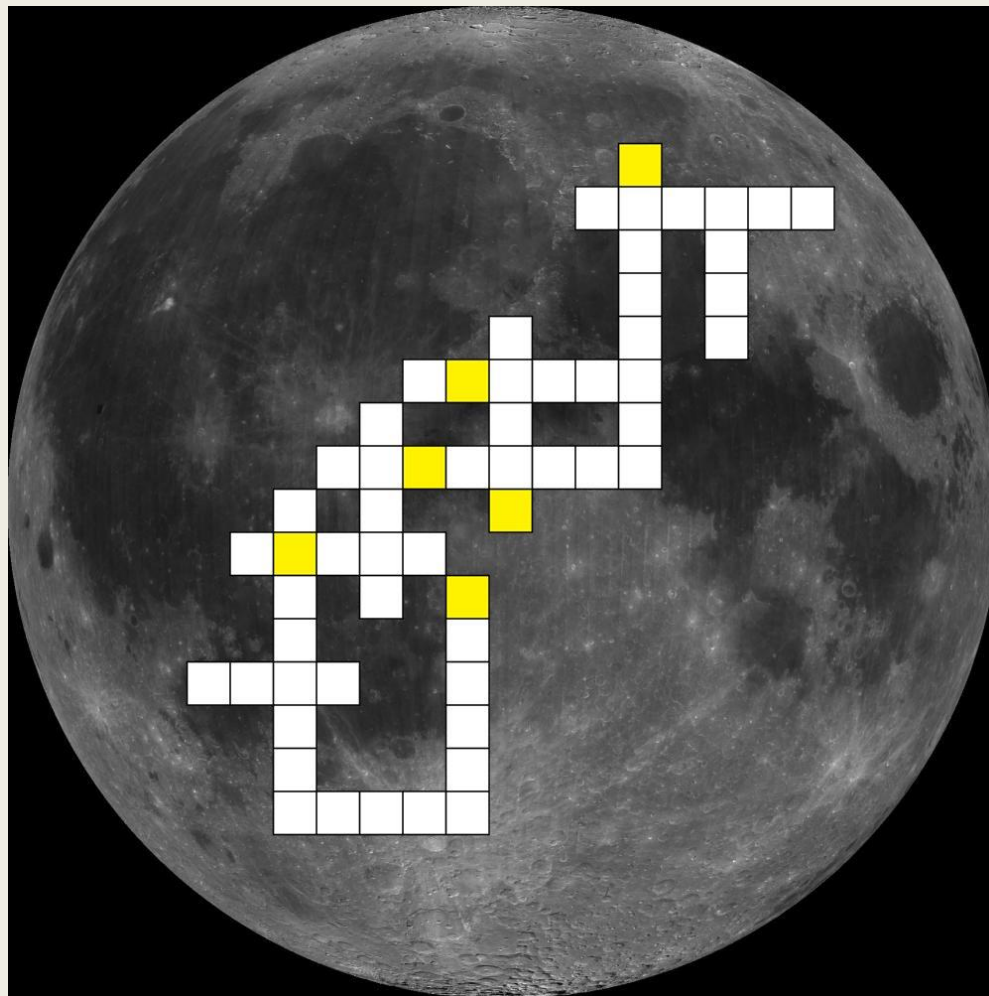
PÁREK – OKURKA – ČOČKA – IBALGIN – TOPINKA – ARTYČOK – ČESNEČKA

Transpoziční šifry

- Změna pořadí znaků
- Čtení od konce
- Procházení tabulky



Asociační šifry



Kódování

- Na rozdíl od šifry je způsob přepisu do „normálního“ textu známý
- Morseova abeceda
- Braillovo písmo
- ASCII kód
- Čárové kódy, QR kód

Typy pro šifrování

- Vytrvalost
- Trpělivost
- Nemít přílišná očekávání
- Týmová práce. Brainstorming
- Vhodné pomůcky

Klíčové otázky

- Z jakých částí se šifra skládá? Co je uprostřed, co na kraji?
- Co se v šifře opakuje? Najdeme pravidelné skupiny? Z kolika prvků se skládají?
- Co si je v šifře podobné? Co se liší?
- Čemu se šifra nebo její část podobá? Kde už jste to viděli?
- Co přebývá? Co chybí?
- Vyluštili jste šifru až do konce?

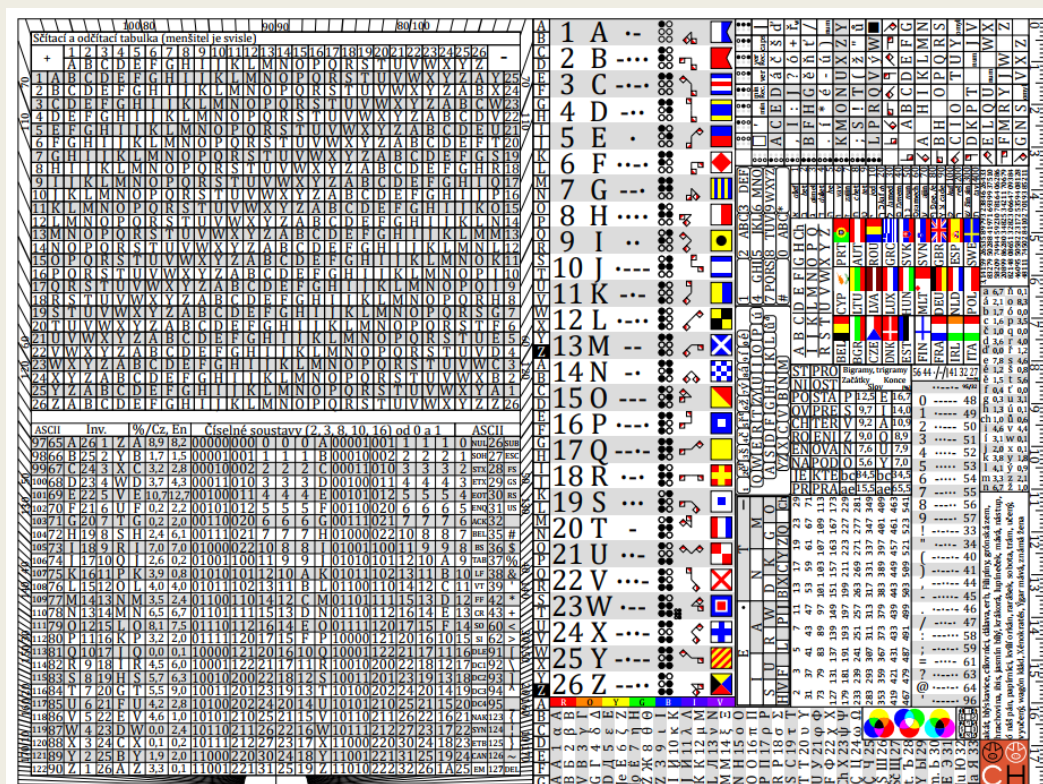
Brainstorming

- Generování nápadů – žádný není tak šílený, aby se nezkusil
- Nezavrhuj nápad, protože se ti napoprvé nezdá.
- Podporujte se.
- Poslouchajte se.

Šifrovací pomůcky

■ <https://chlyftym.cz/pomucky/>

- Pomůcky dané orgy
- Tužky
- Pastelky
- Nůžky
- Izolepa
- Lepidlo
- Počítač, internet, tiskárna



Typy pro luštění: Obecně

- Složení týmu
- Důslednost – dotahujte nápady do konce
- Týmová práce, rozdělování úkolů, týmový duch, týmová morálka
- Podezíravost a paranoia (šifry – trojské koně), zdravá pochybnost
- Interpretace výsledku

Typy pro luštění: Smysluplný text

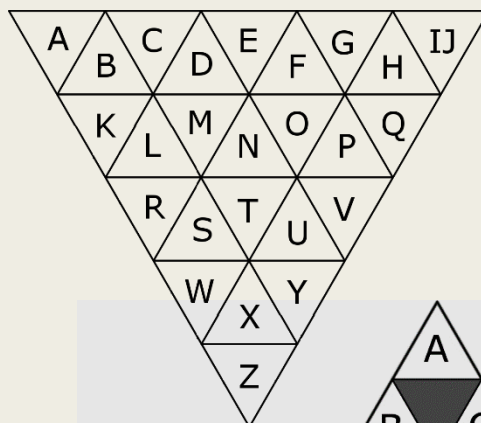
- Kostrbatý text – jazykové skrývání v textu (kolikáté písmeno či slovo, zvláštní slova či obraty, čísla v textu)
- Stylistické a pravopisné chyby, typografické odchylky
- Faktografické údaje

Typy pro luštění: Čísla

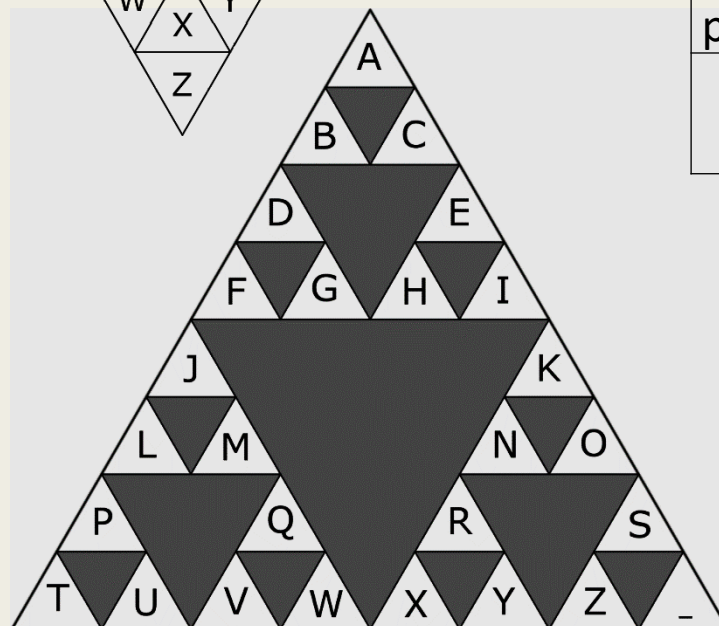
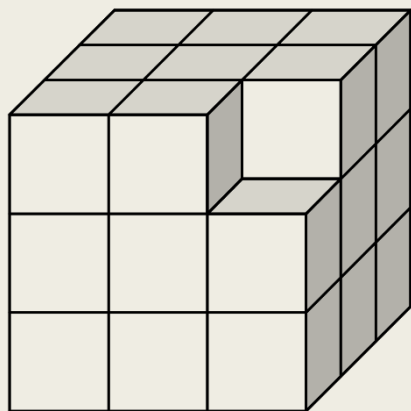
- Čísla v intervalu 0–25, 1–26
- Jiné rozmezí – jaké má vlastnosti?
- V šifře jsou pouze čísla? Vlastnosti čísel (desítková soustava, cifry; dělitelnost, zbytky; velikost čísel, frekvence)
- Která čísla sousedí? Pravidelnost zápisu? Tvoří řadu?
- Aritmetické operace: +, -, *, /, průměr, zaokrouhlování, rozklad na prvočísla

Očíslování písmen abecedy

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



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



Typy pro luštění: Velikost skupin

Velikost skupin	Kandidát na šifru
V rozmezí 1-4	Morseovka, klávesnice mobilního telefonu
V rozmezí 1-5	Římská čísla
V rozmezí 2-6	Grafická šifra (písmeno se dá vykreslit 2-6 body)
V rozmezí 1- 12	12 hodin na hodinách, 12 měsíců, znamení zvěrokruhu
V rozmezí 1- 31	Dny v měsíci, kalendář
25, 26, 27	Použití celé mezinárodní abecedy
Vždy 3	Kódy států. SPZ aut. Polský kříž
Vždy 4	Grafická šifra (světové strany, nahoru/dolů/vlevo/vpravo)
Vždy 5	Grafická šifra (mřížku o 5 řádcích lze použít na vykreslení písmen). Binární abeceda
Vždy 6	Braillovo písmo
Vždy 9	Polský kříž
Jiný konstantní počet	Přepsat skupiny do tabulky (zvláště když počet znaků je roven 2. mocnině)

Typy pro luštění: Když nic nefunguje

- Nasad'te morseovku nebo Braillovo písmo
- Posloupnosti čísel převádějte na písmena – a naopak!
- Zkuste první/poslední/prostřední písmena zadání/mezivýsledku/čehokoli
- Jde o předmět? Rozložte ho/rozbijte ho/přeměňte ho – ale předtím si z něj opište všechny údaje, ať nic neztratíte

Šifrovací sbírka



<http://www.gymtrebon.cz/UserFiles/pazourek/sifra1415/Prirucka3.pdf>

Soutěže

- [Brloh](#)
- [Dětská šifrovací liga](#)
- [Želvování](#)

