

# Využití šifer ve výuce

Radek Pelánek



INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Modulární systém dalšího vzdělávání pedagogických pracovníků JmK  
v přírodních vědách a informatice CZ.1.07/1.3.10/02.0024

# Motivace: proč se šiframi zabývat?

- názorná ilustrace matematických konceptů
- vztah k moderní kryptologii
- zajímavé programátorské cvičení
- trénink řešení problémů
- lidi to baví

- šifrovací hry
- šifry
  - klasické
  - nekonvenční (herní)
- šifry a řešení problémů

# Šifrovací hry

- týmové hry (cca 5 lidí)
- nekomerční, bez (významných) odměn pro vítěze
- většinou pro dospělé
- rozsáhlé – až 1000 účastníků
- příklady:
  - Tmou lineární, terénní, noční, 18 hodin
  - Exit město+internet, recesní, paralelní úkoly, 8 hodin
  - Sendvič Internetová, 5 hodin, okamžitá výsledkovka

# Šifry klasické

substituce nahrazení písmen za jiné

transpozice změna pořadí písmen

steganografie skrytí existence zprávy



# Substituce II

## substituce podle hesla

|       |   | zpráva |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
|-------|---|--------|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
|       |   | 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 |
| heslo | 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 |

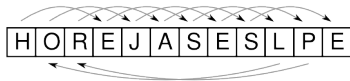
h  
l  
e  
d  
e  
j  
p  
o  
d  
l  
i  
p  
o  
u  
  
s  
l  
o  
n  
s  
l  
o  
n  
s  
l  
o  
n  
s  
l  
  
Z  
W  
S  
Q  
W  
U  
D  
B  
V  
W  
W  
C  
G  
F

# Transpozice I

pozpátku



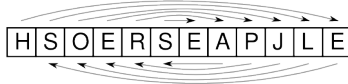
ob tři



trojice pozpátku

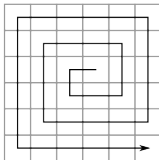


dopředu dozadu



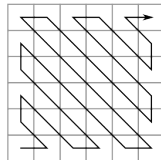
# Transpozice II

šnek



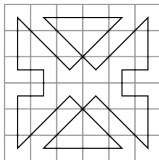
|   |   |   |   |   |   |
|---|---|---|---|---|---|
| L | B | A | K | I | N |
| I | C | S | E | J | B |
| Z | H | O | P | D | Y |
| K | O | K | L | A | R |
| O | V | A | N | Y | U |
| U | H | R | A | Z | E |

cik-cak



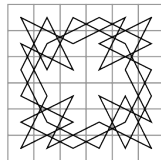
|   |   |   |   |   |   |
|---|---|---|---|---|---|
| N | I | O | U | Z | E |
| H | B | K | K | H | A |
| C | O | Y | A | Z | R |
| L | S | V | R | B | I |
| K | A | E | A | U | L |
| P | O | D | J | N | Y |

královská procházka



|   |   |   |   |   |   |
|---|---|---|---|---|---|
| P | E | J | D | A | O |
| E | O | S | L | H | V |
| Z | A | K | C | N | A |
| H | R | Z | N | Y | U |
| U | K | I | I | B | R |
| O | K | A | B | L | Y |

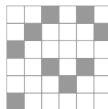
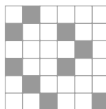
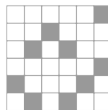
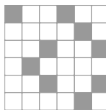
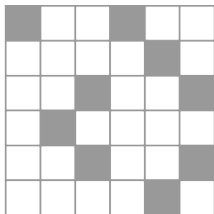
jezdcova procházka



|   |   |   |   |   |   |
|---|---|---|---|---|---|
| P | A | Z | D | K | Z |
| O | J | O | I | A | A |
| N | E | V | L | K | L |
| E | H | I | U | R | R |
| K | Y | S | B | B | O |
| C | N | A | U | H | Y |

# Transpozice III: Šifrovací mřížka

šifrovací mřížka



|   |   |   |   |   |   |
|---|---|---|---|---|---|
| P | Y | Z | O | K | C |
| B | O | H | N | K | U |
| H | O | L | V | I | A |
| K | D | R | A | A | A |
| N | B | J | Z | Y | E |
| E | U | L | R | S | I |

# Programátorská cvičení

- základní substituční/transpoziční šifry vhodné jako programátorské příklady
- stačí relativně málo syntaxe (řetězce, pole, cykly)
- myšlenkově zajímavé
- inspirace: Šifrátor  
<http://www.radekpelanek.cz/?sifrator>

# Nekonvenční (herní) šifry

- využití kódování (morseovka, Braillovo písmo, semafor)
- zakódování grafického zápisu zprávy
- využití znalostí

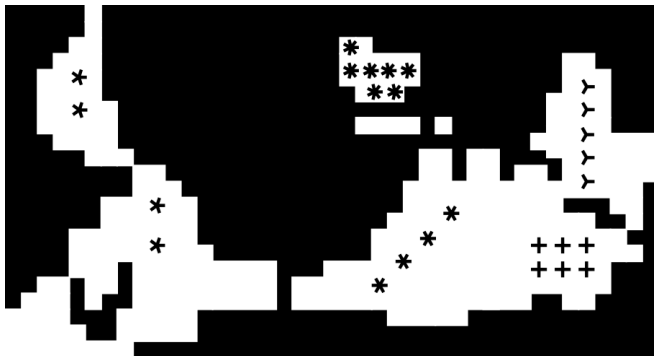
# Příklad: Seznam

přistávací plocha, autoškola, stan, pozice skokana, blesk,  
informace, stanice podzemky, první člen Evropské Unie, had,  
příjezd na hlavní, závodíště běžce, anglické sprosté slovo,  
ochranná známka, počátek většiny kontinentů, zkrácený and,  
autorská práva, úsečka, Samuelova tečka

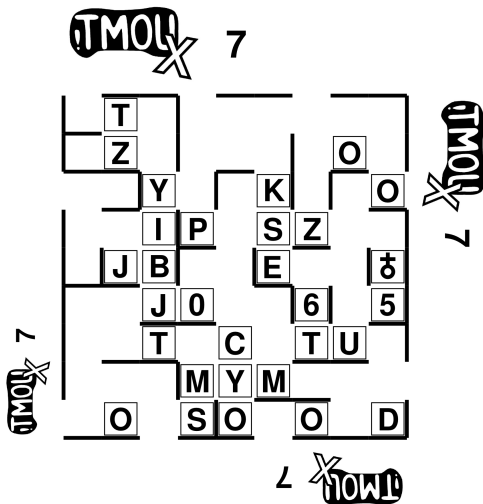
# Příklad: Písmena a čísla

vě-1-osa, hu-2-no, mora-2-šek, ko-2-hrada, sto-2-dlo, vej-2-sta,  
poled-2-moc, stá-2-zor, dlou-2-ra, ran-2-zko

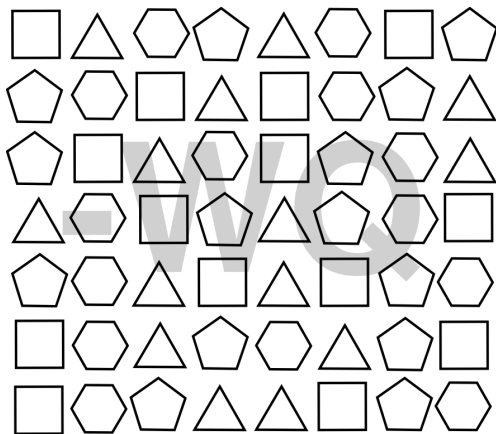
# Příklad: Hvězdičky



# Příklad: Bludiště



# Příklad: Tvary



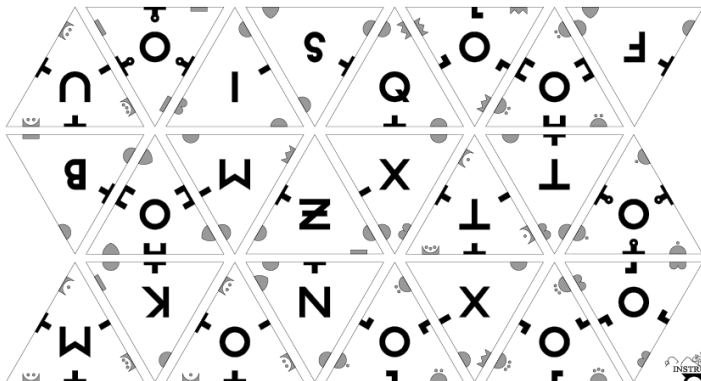
# Příklad: SudSub

17IIV4GZ9L6E2WV4LQWC5LCACH6G48C92U302  
M38U79J4F1X54G82X8LGUVN1NYEM4WG1ZFF5U  
Z4RJT63

# Příklad: Trojúhelníky



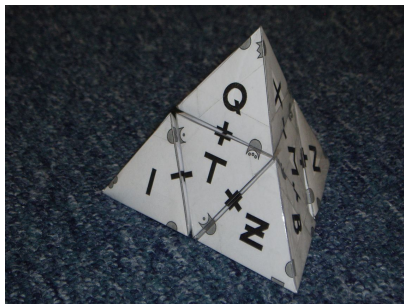
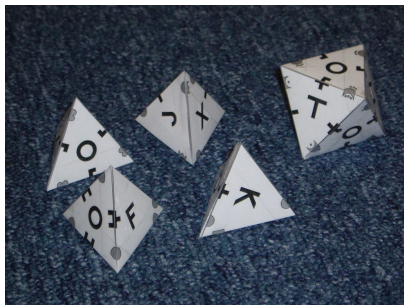
13



V následujícím textu nehledejte šifru: Upřesnění umístění dalšího stanoviště: následující šifra je umístěna u seniku poblíž místa, kam ukazuje tato šifra. Upozornění: nevstupujte do prostorů těžebních lomů, dodržujte noční klid, nerušte prosím zvěř a neza nechávejte odpadky. Děkujeme.



# Příklad: Trojúhelníky řešení



$$Q + T = K$$

$$I - T = O$$

$$Z + T = T$$

$$N + M = A$$

$$X - M = K$$

$$B + M = O$$

$$K + O = Z$$

$$X - O = I$$

$$S + O = H$$

$$T + U = O$$

$$M - U = R$$

$$F + U = A$$

# Šifry a trénink řešení problémů

- obecná schopnost **řešit problémy** (bez vazby na konkrétní problém) je důležitá
- tradiční školní problémy – velmi „dobře strukturované“
  - jasný cíl
  - všechny potřebné informace a žádné redundantní
  - znalost postupu
- reálné problémy – méně strukturované

# Šifry a trénink řešení problémů

šifry – vhodný kompromis strukturovanosti:

- existuje „správné řešení“
- není jasný postup
- není jasné, které informace jsou důležité
- nejasný „okraj problému“

# Dovednosti trénované na šifrách

## týmová práce

spolupráce, sdílení nápadů, dělba práce

## analýza problému

hledání pravidelností, systematická práce

## různé pohledy, laterální myšlení

podívat se na problém z nového pohledu, vnést do problému nové informace

## kontrola postupu

zhodnotit dosavadní postup, nezaseknout se na slepé větvi, neopustit správnou větev

# Shrnutí: Co s tím?

- 1 výklad principů šifrování: substituce, transpozice, moderní kryptologie
- 2 šifry jako programátorský příklad
- 3 šifrovací hry a trénink řešení problémů