Šifry, hry a řešení problémů

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

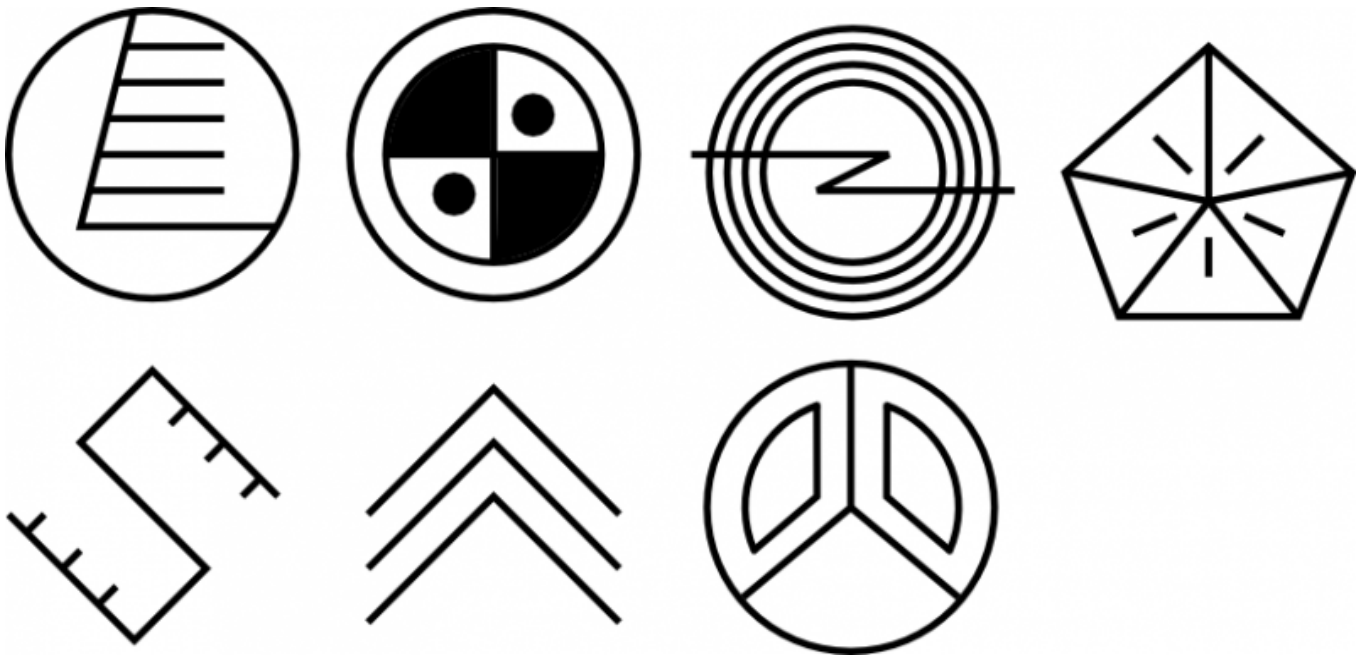
„Herní“ šifry

- klasická kryptografie:
  - Kerckhoffův princip: bezpečnost šifry nesmí stát na utajení principu
  - cílem je, aby šifru nešlo prolomit
- herní šifry:
  - tajný princip
  - cílem je, aby šifra byla luštitelná (a zajímavá)

Příklad: Binární selektor

KRAVA.24 NENI.4 STASTNA.98 BRECI.1 DOJI.2 MLEKO.20
JENOM.6 TROSKU.33 TELE.0 URCITE.20 ZACNE.2
GRKAT.18

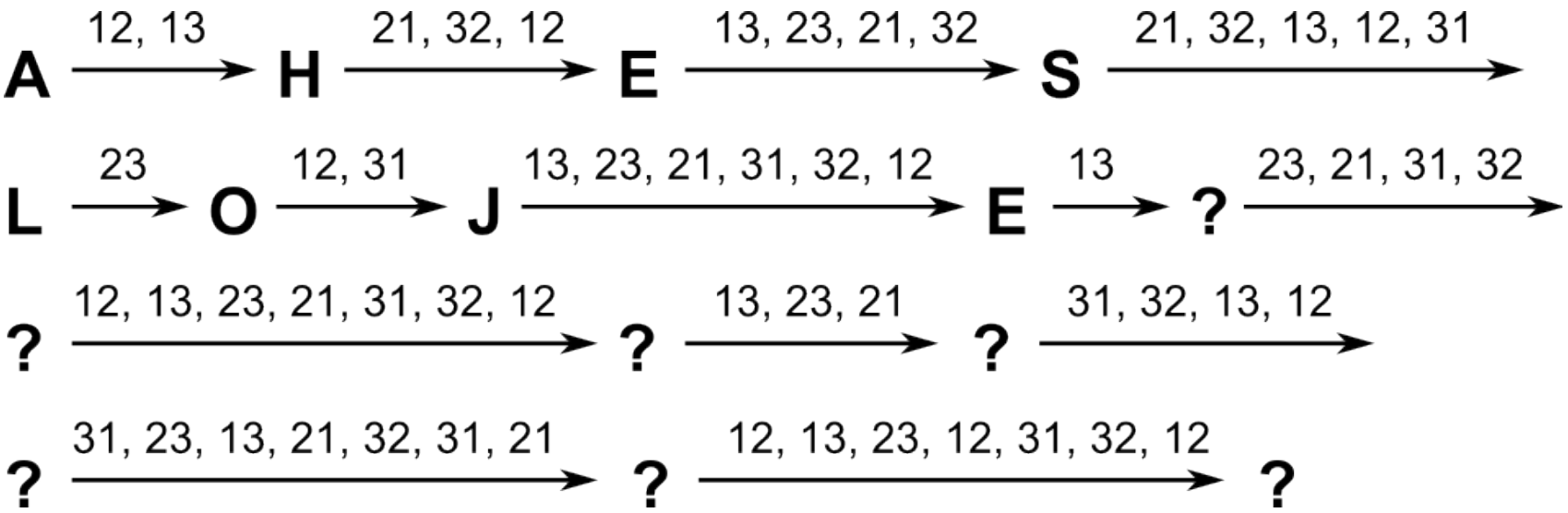
Příklad: Schémata



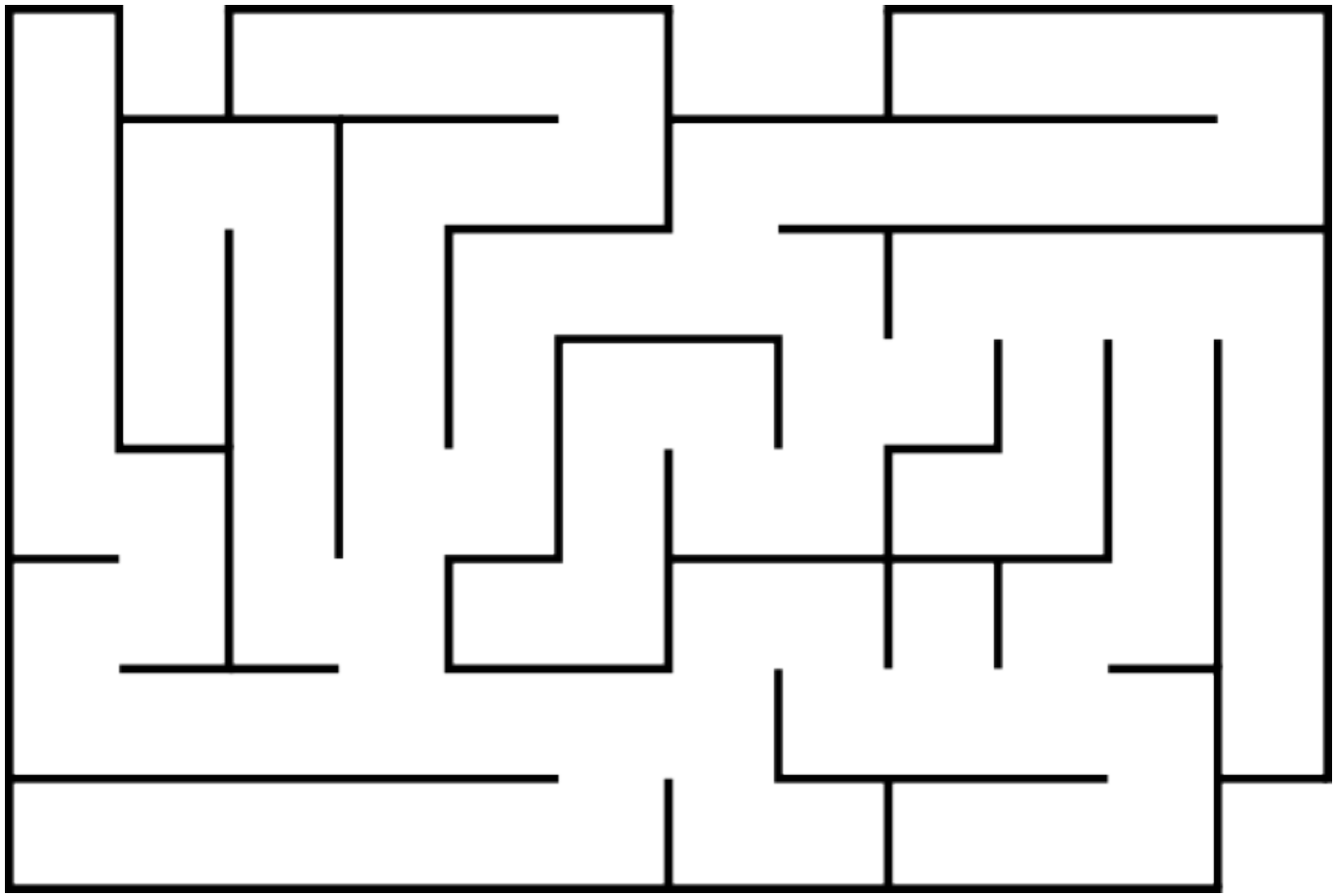
Příklad: OZ kvíz

Sponzor sklípku, sněhulákův smysl, adjektivum v pejorativním deskriptoru určitých republik. Pták, celulitida, sortiment k sehnání od 12 měsíců. Veřejný činitel, milión, třetí do party. Komplic vlka a kozy, Stevova práce, červení horcí hudebníci. Eviny bikiny, poselství konce potopy, předmět slupnutí. Trojice plovoucí na hladině, Skácelova chyba. Spouštěč breku, objekt veršované prosby na horizontální proudění vzduchu. Popelčin trumf, neblahá vzpomínka Irů. Příloha mamuta. Upírova fobie, zkažený spoluletec vejce, nepohodlí princezny. Otočený olemop, hrdina Halloweenu, osazenstvo Mojita, námořníkova síla. Výbava komunisty, film na sněhu, počáteční místo dezorientačního pádu.

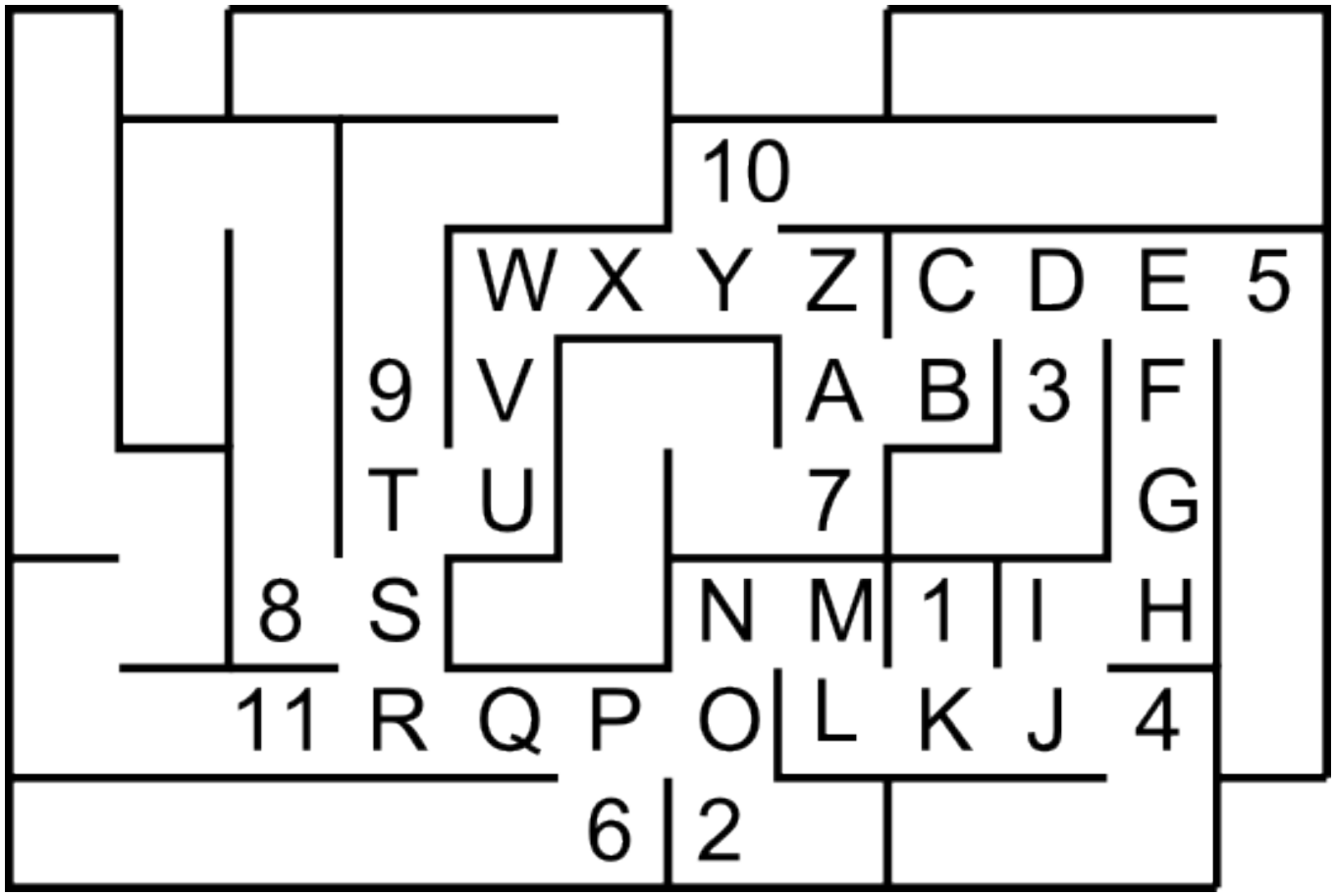
Příklad: CHanojské věže



Příklad: Bludiště



Příklad: Bludiště



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

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, paralelní úkoly, 8 hodin
Sendvič	Internetová, 5 hodin, okamžitá výsledkovka

Šifrovací hry: typy her

- lineární struktura
- hvězdicovitá struktura
- (kombinace)

Lineární hra

- vždy jen jedna šifra, po vyluštění další
- ideální do terénu
- šifra $\longrightarrow$ identifikace místa $\longrightarrow$ přesun $\longrightarrow$ šifra $\longrightarrow$ ...
- důležité (a náročné) správně odhadnout obtížnost šifer, dobře zvolit „dramaturgii“
- nápovědy: telefon, obálky, terén

Hvězdicovitá hra

- jednotlivé šifry nezávislé, více šifer současně
- šifry $\longrightarrow$ body $\longrightarrow$ výsledková listina
- obtížnost šifer může být rozmanitá
- provedení:
  - internetový vyhodnocovací systém
  - systém „tabule“
- práce s časem: postupné zveřejňování, zohlednění při bodování, deadliny
- nápovědy spíš nedávat

Poř.	Název týmu	Úkolů	Čas	Špat.	101	102	103	104	105	106	201	202	203	204	205	301	302	303	304	305	306	401	402	403	404	405
1.	Proudoví krtci	20	14:37:35	3	1				1		1															
2.	Tykadla	19	10:38:08	4					1		2									1						
3.	Pralinky zvlášť	18	12:17:03	4								1														3
4.	Priskoro na nárek	17	09:58:07	1																						1
5.	Chlýftým rypák	17	10:13:15	2							2															
6.	DuJour a spol.	17	10:31:52	2	1	1																				
7.	Deformační Extraktor	17	11:46:23	3							1	1										1				
8.	Fčeličky	16	09:44:10	5					3	1												1				
9.	Drahoš forever	16	10:22:14	6	1				3														2			
10.	Vlhká jáma	16	10:49:14	2	1				1																	
11.	Velký skok vpřed	16	11:09:42	3																	1					2
12.	Oberna behen	16	12:01:10	6	2				1													1				2
13.	Tučňák s tučňákem	16	13:18:01	11					4									1	2			1				3
14.	MUPY MUP!	16	13:55:54	4					4																	
15.	FIMAN++	15	08:57:32	6	1		1		1	1	1									1						
16.	Biohazard	15	09:18:33	1																1						
17.	Kundratka	15	09:21:10	1							1															
18.	Náhodná procházka	15	09:52:06	2							1															1
19.	Corn Flakes	15	10:10:07	4					3											1						
20.	MLHA	15	10:10:09	6					1	1		1	1								1	1				
21.	HALUZná ORGanizácia	15	11:01:59	3		1														1						1
22.	Squeak!	15	12:31:14	8	3				1		1		1									2				
23.	Čert už nemůže	15	13:07:17	3																			2			1
24.	Ferne Sterne	14	09:25:05	1	1																					
25.	Hvězdná pěchota	14	09:43:08	7	1				1	1									1			1		1	1	

Šifrovací hry: tipy

- hrát po týmech (3-5 lidí)
- strukturu zvolit co nejjednodušší, obtížnost dát do šifer
- pestrost šifer: obtížnost, princip, vzhled, ...
- otestovat, nepřestřelit obtížnost
- hvězdicovitá hra je výrazně jednodušší na přípravu

Konkrétní tip

- 4 členné týmy, čas: 1 hodina
- na začátku: šifrovací pomůcky + cca 5 šifer
- po 30 minutách: další cca 3 šifry
- průběžná výsledka na tabuli, body podle pořadí vyluštění šifry
- šifry lze převzít, zvolit spíš jednoduché, 1-2 trochu těžší
- pustit hudbu, aby se týmy mohli bavit a nenapovídali ostatním
- vhodnou volbou šifer lze propojit s výukovými tématy

Zdroje

- kniha Šifry a hry s nimi
- Šifrovací cvičebnice
- Šifrátor
- Kalendář šifrovacích her
  $\longrightarrow$ stránky her
- `http://radekpelanek.cz/`