



GYMNÁZIUM
JÍROVCOVA



Přírodovědecká
fakulta
Faculty
of Science

Jihočeská univerzita
v Českých Budějovicích
University of South Bohemia
in České Budějovice

Šifry jako didaktický neřád

Karel Pazourek

Kódování

= způsob zápisu nebo reprezentace informace

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
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26



Šifrování

= kódování, u kterého není obecně známý převod do čitelné podoby

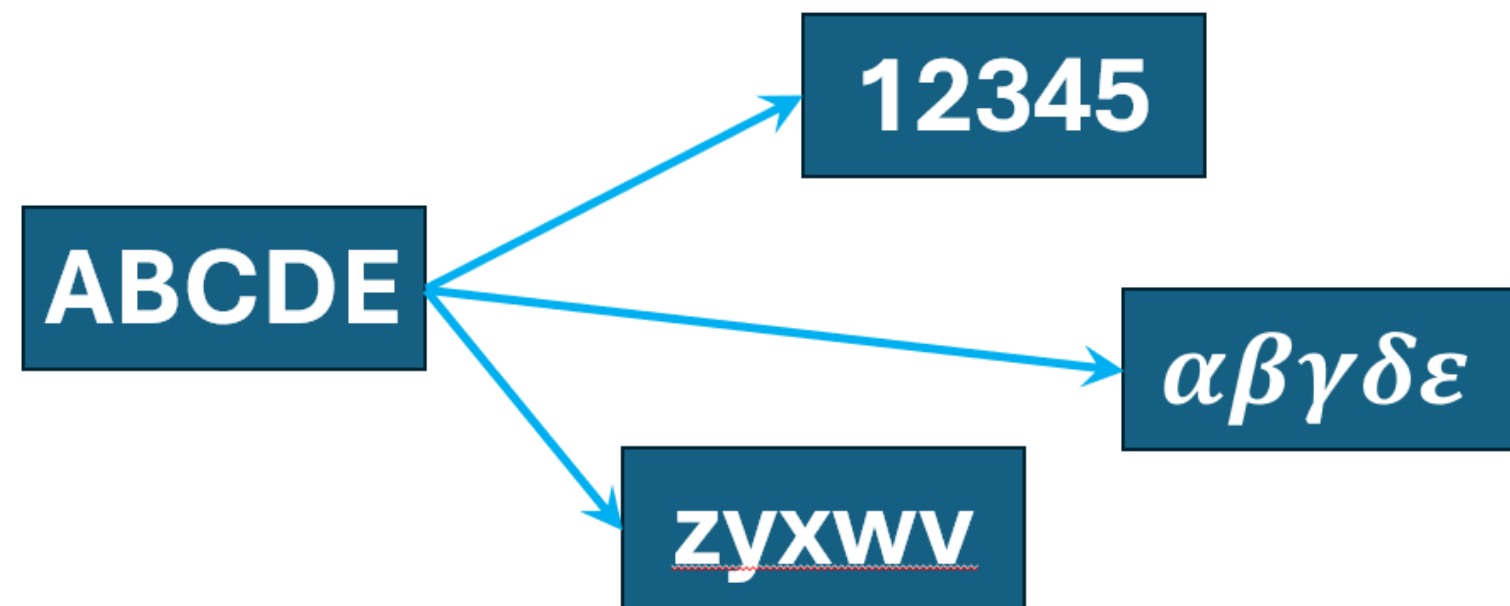
- jednoduché šifry
- historické šifry
- neznámé zápisy



Dva principy šifrování

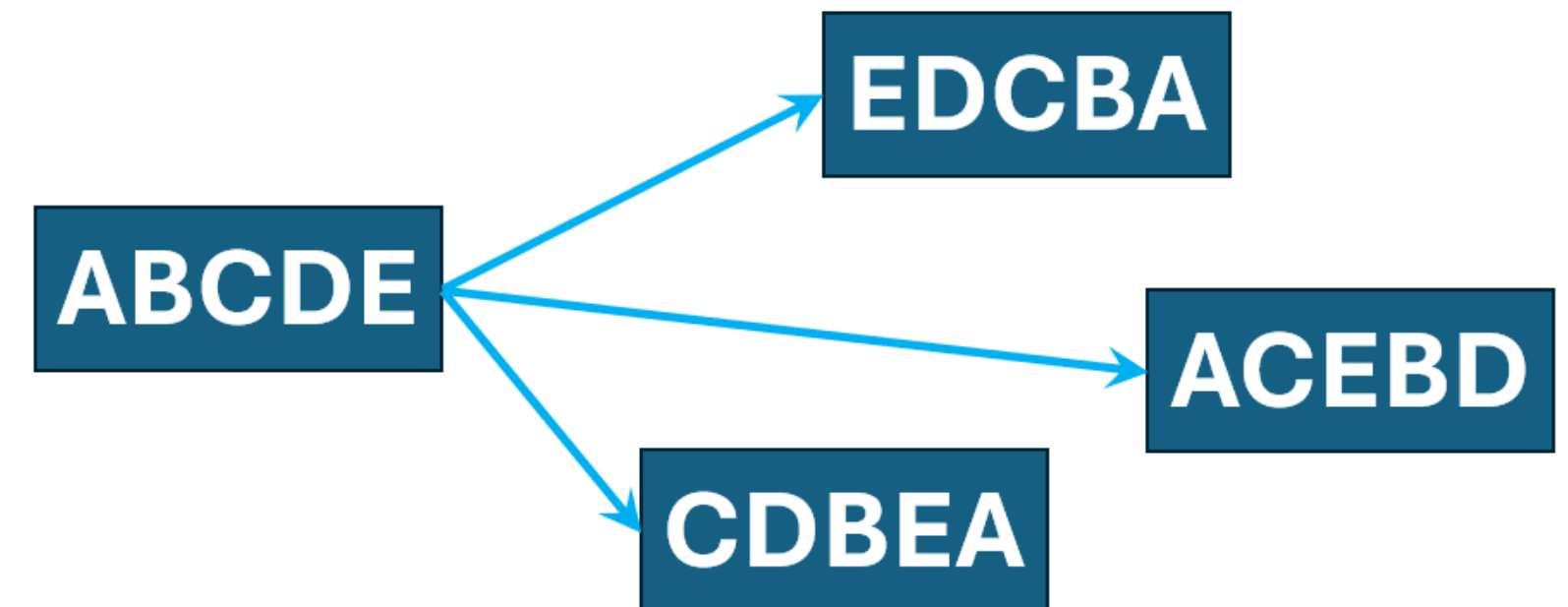
Substituce

= nahrazení znaků, jejich skupin atp.
za jiné podle stanoveného pravidla



Transpozice

= změna pořadí nebo pozice znaků,
jejich skupin atp. podle stanoveného
pravidla

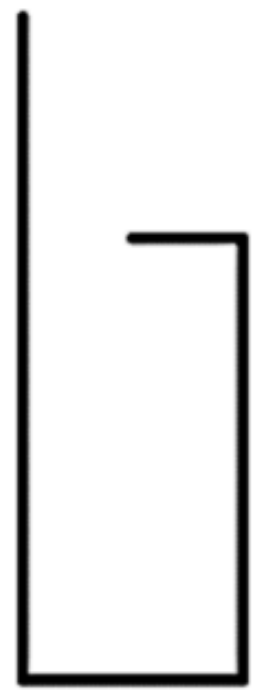


Substituční šifra

W U S W I L R S)



Substituční šifra



— — — —

CH



— — —

O



— . . .

B



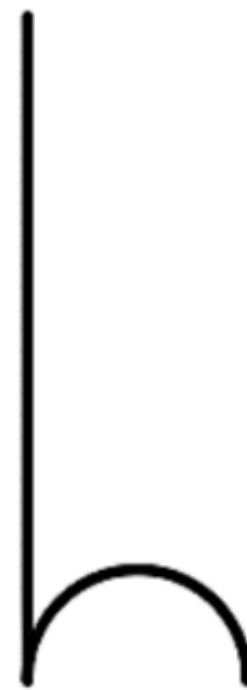
— — —

O



—

T



— .

N



. . .

I



— . — .

C



.

E



Substituční šifra

$$\frac{1}{2} \frac{21}{26}^1 \frac{5}{26} \frac{21}{26} \frac{1}{2}$$



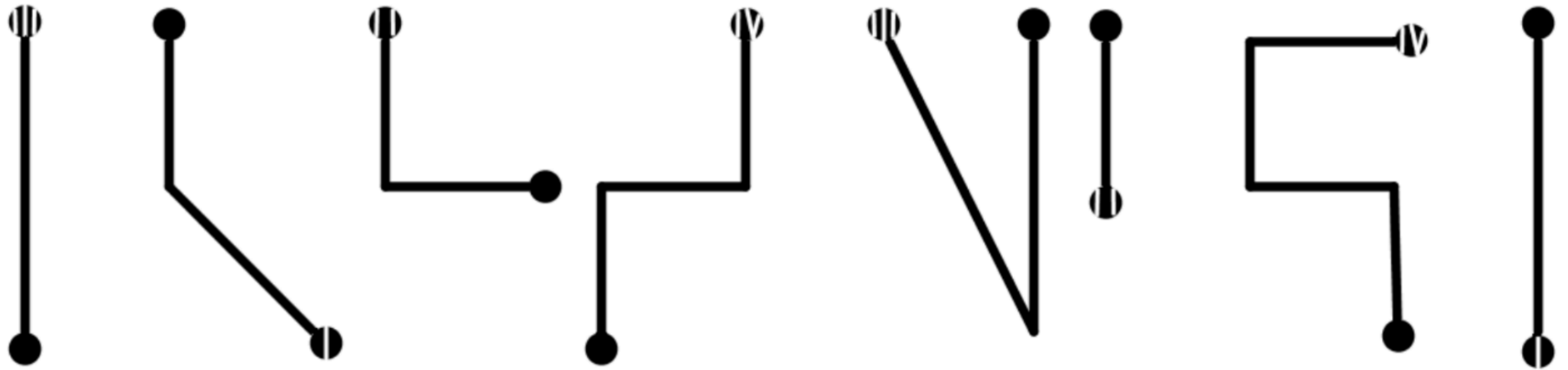
Substituční šifra

$$\begin{array}{cccccc} 1 & 21 & & 5 & 21 & 1 \\ \hline 2 & 26 & 1 & 26 & 26 & 2 \end{array}$$
$$\begin{array}{cccccc} 13 & 21 & 26 & 5 & 21 & 13 \\ \hline 26 & 26 & 26 & 26 & 26 & 26 \end{array}$$

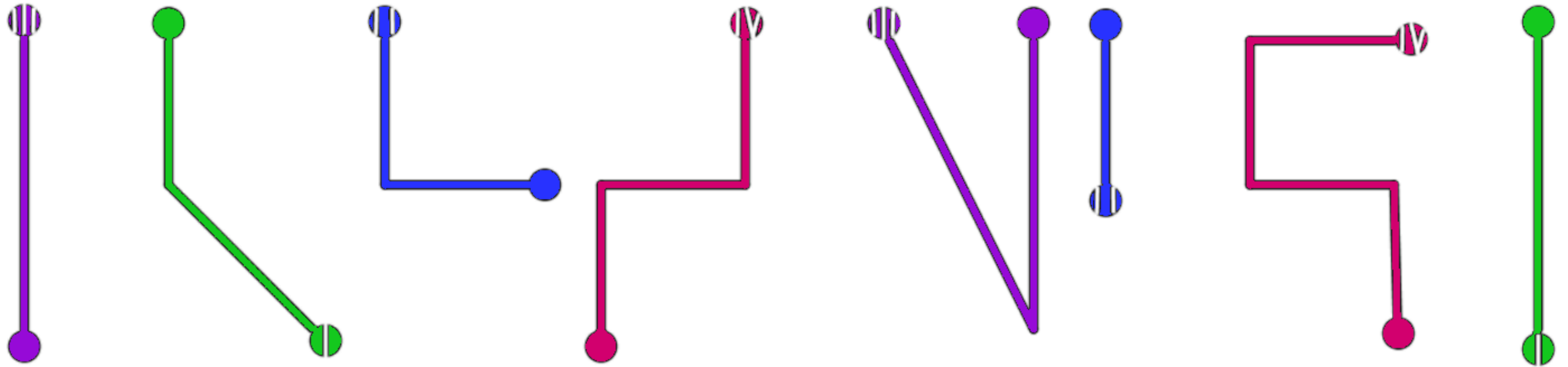
M U Z E U M



Transpoziční šifra



Transpoziční šifra

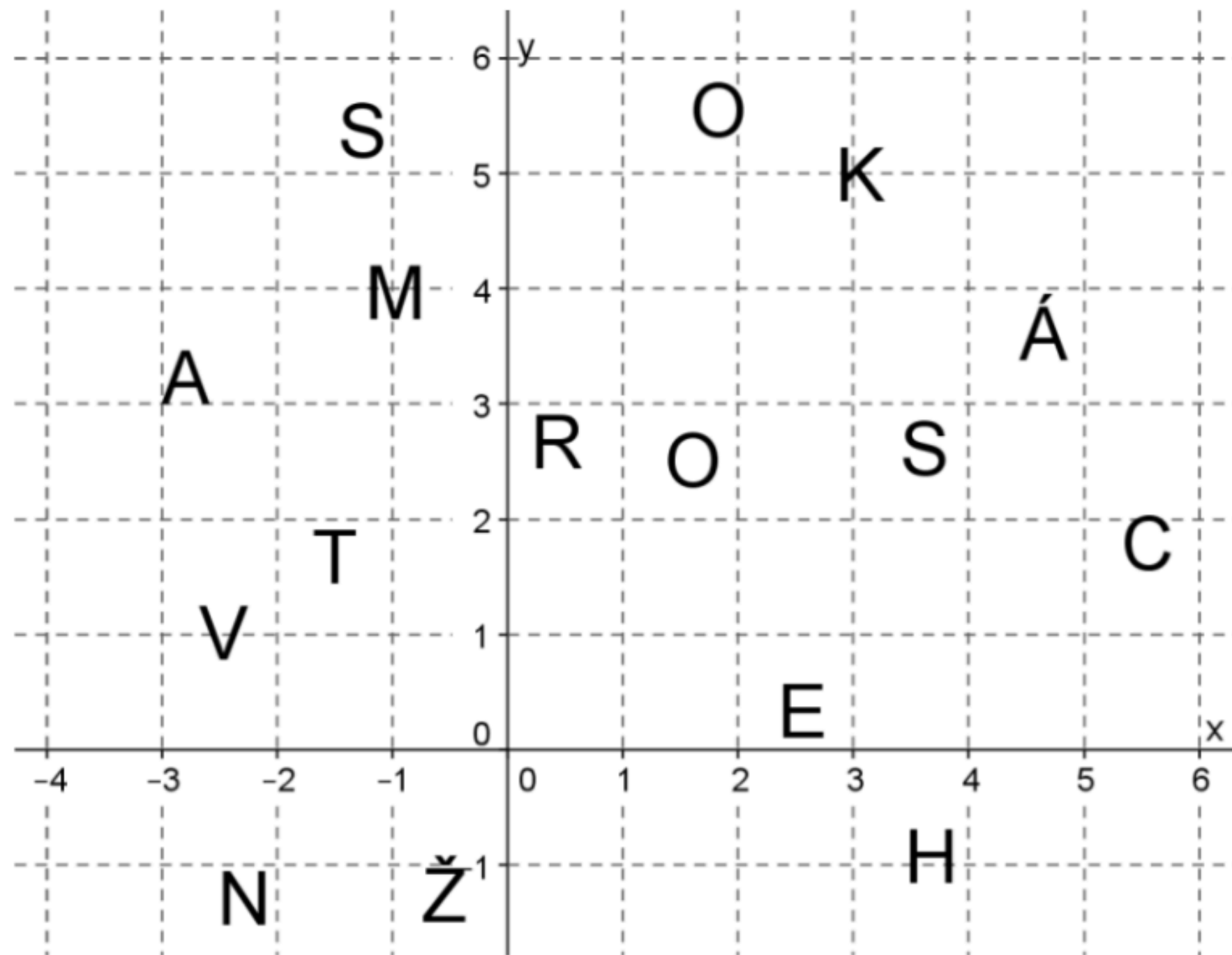


VLNA



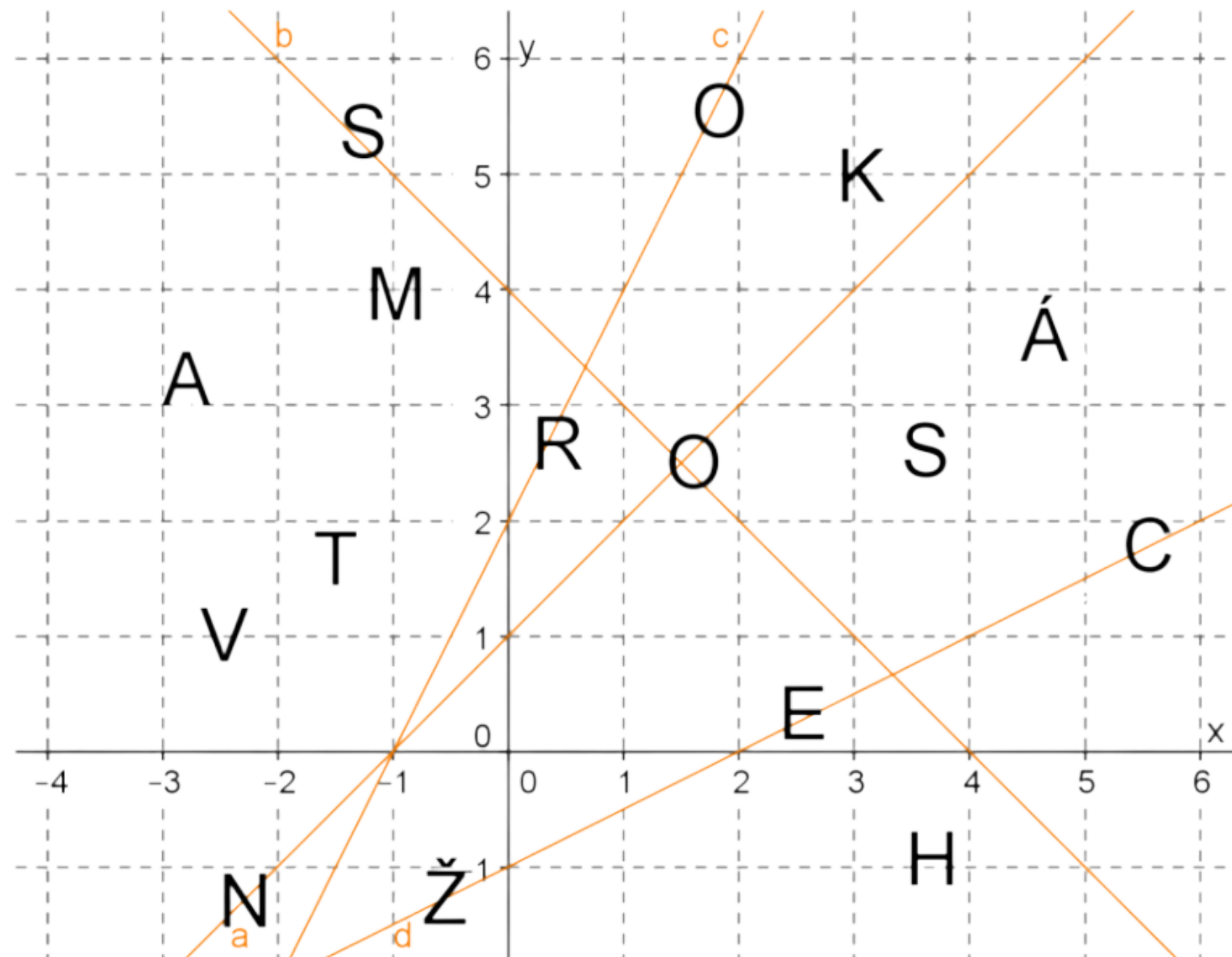
Transpoziční šifra

$$a: y = x + 1, \quad b: y = -x + 4, \quad c: y = 2x + 2, \quad d: y = \frac{1}{2}x - 1$$



Transpoziční šifra

$$a: y = x + 1, \quad b: y = -x + 4, \quad c: y = 2x + 2, \quad d: y = \frac{1}{2}x - 1$$



Šifrování v informatice

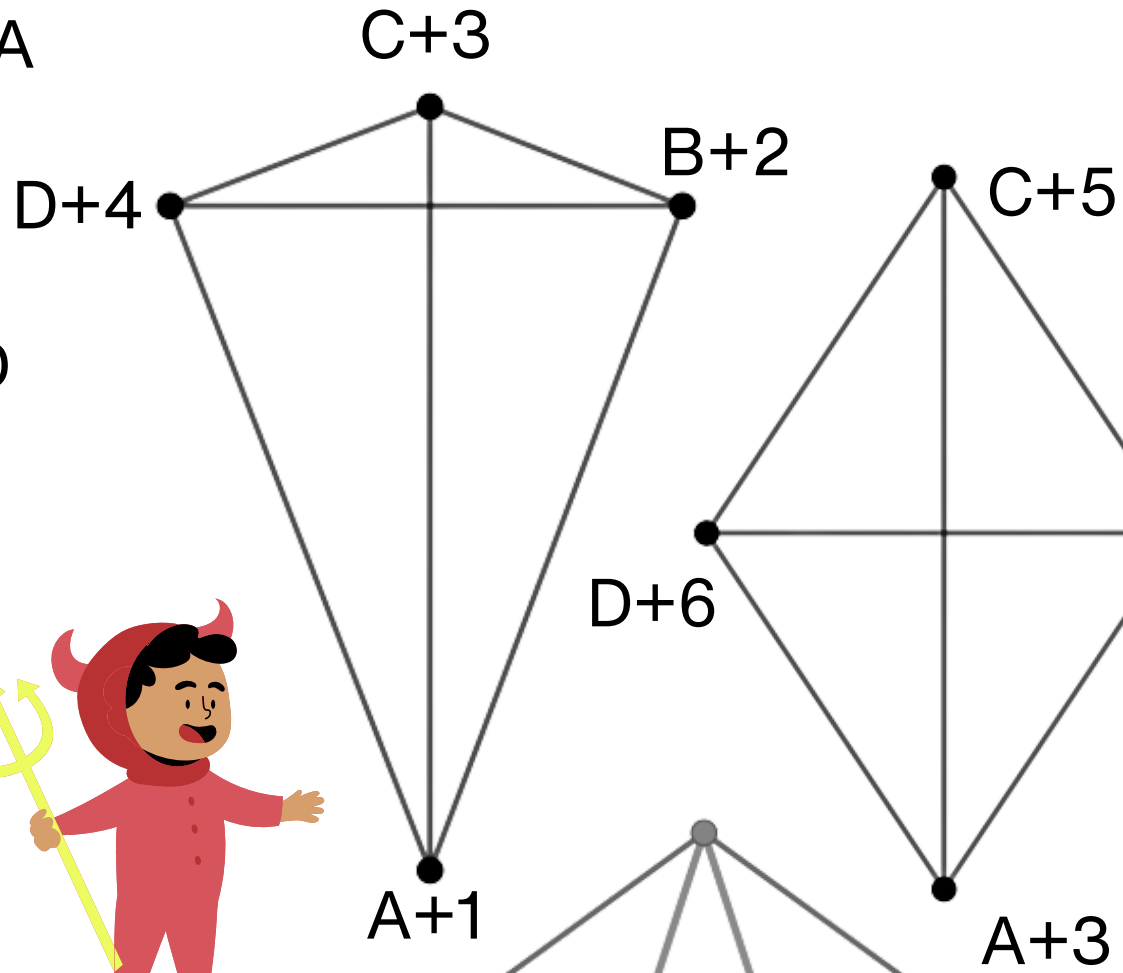
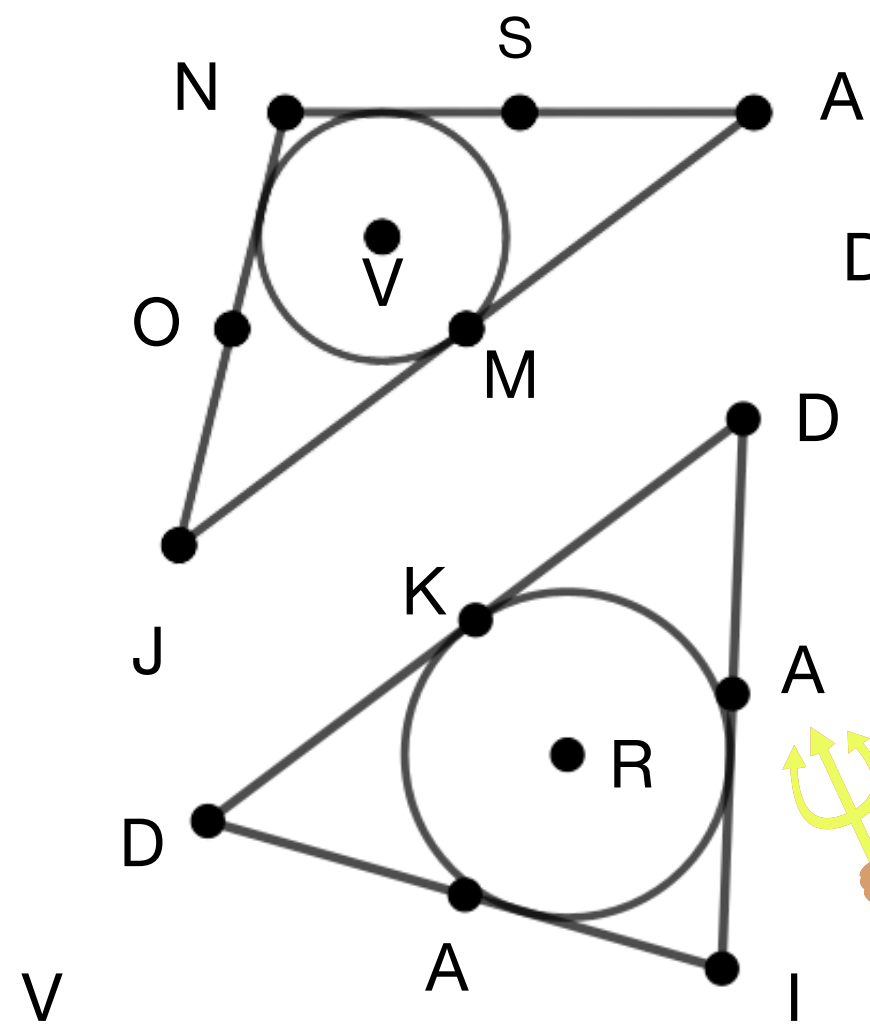
INF-INF-001-ZV9-002

Navrhuje a porovnává různé způsoby kódování dat s cílem jejich uložení a přenosu.

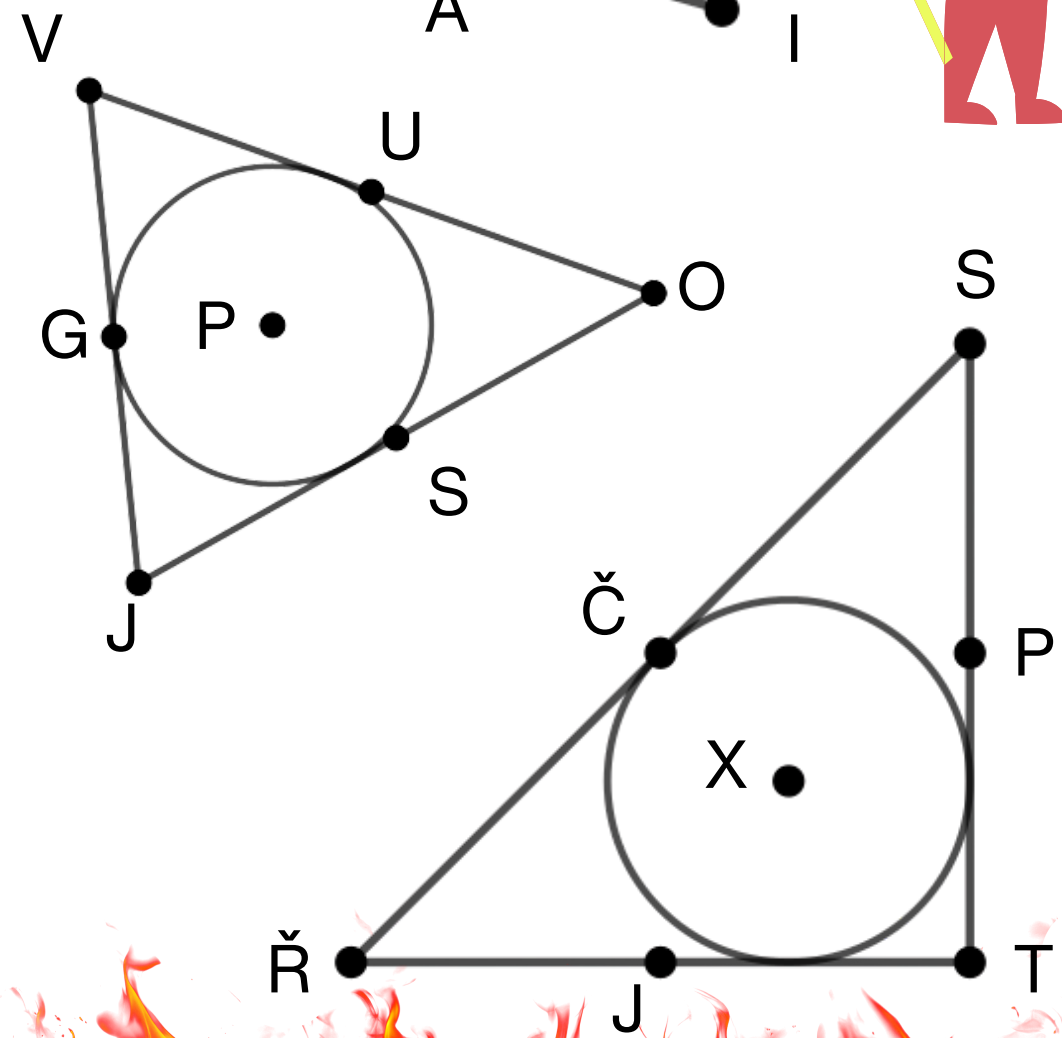
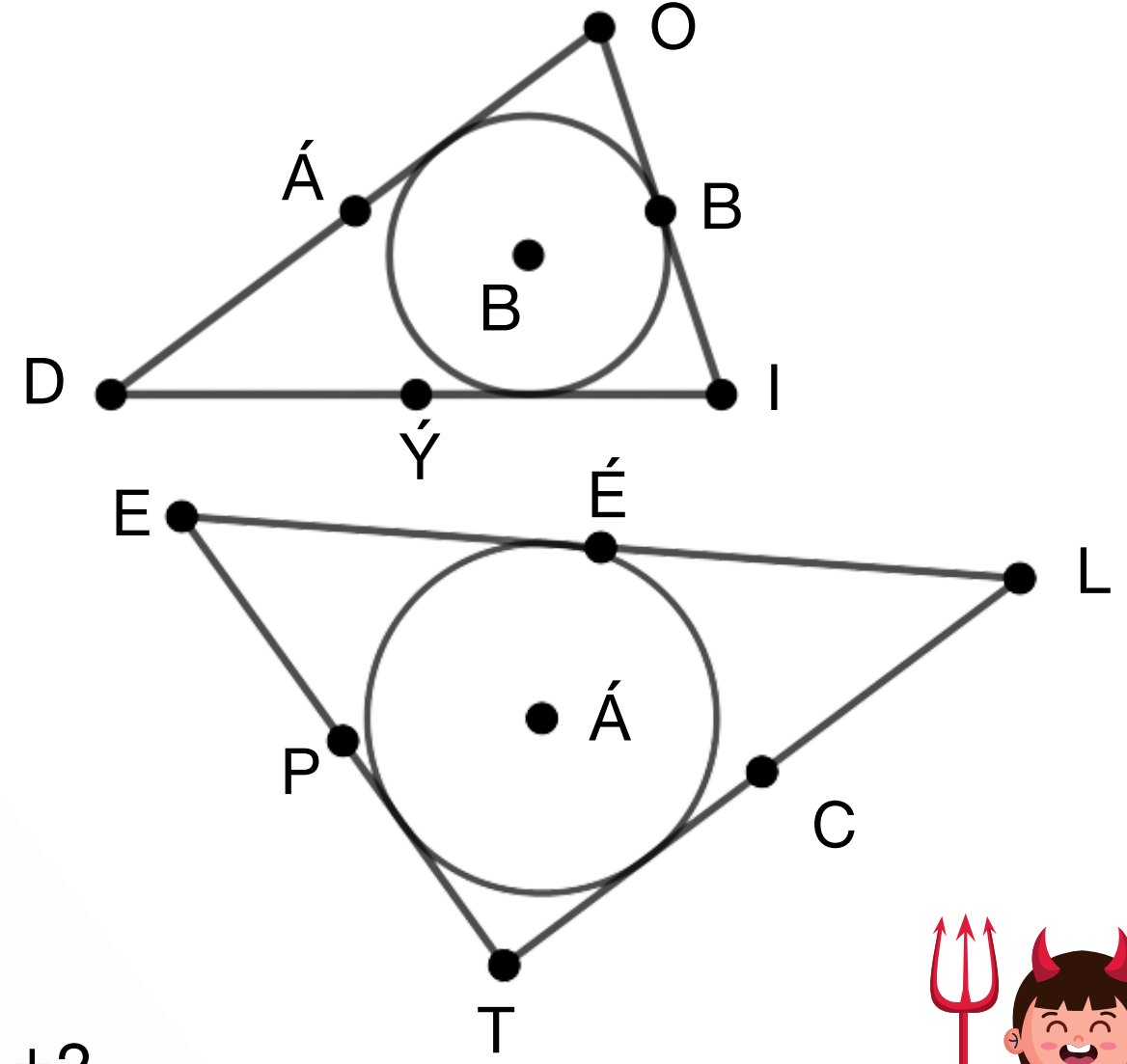
Vyučující postupně vede žáka k tomu, aby:

- měl zkušenost s dalšími způsoby kódování dat (např. římské číslice, Morseova abeceda, Braillovo písmo, notové zápisy)

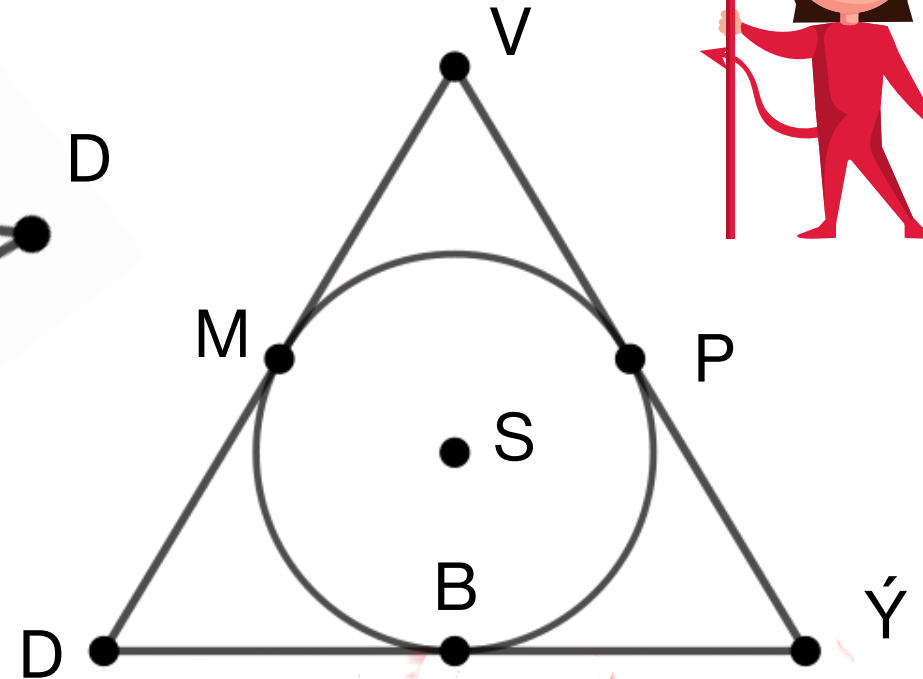
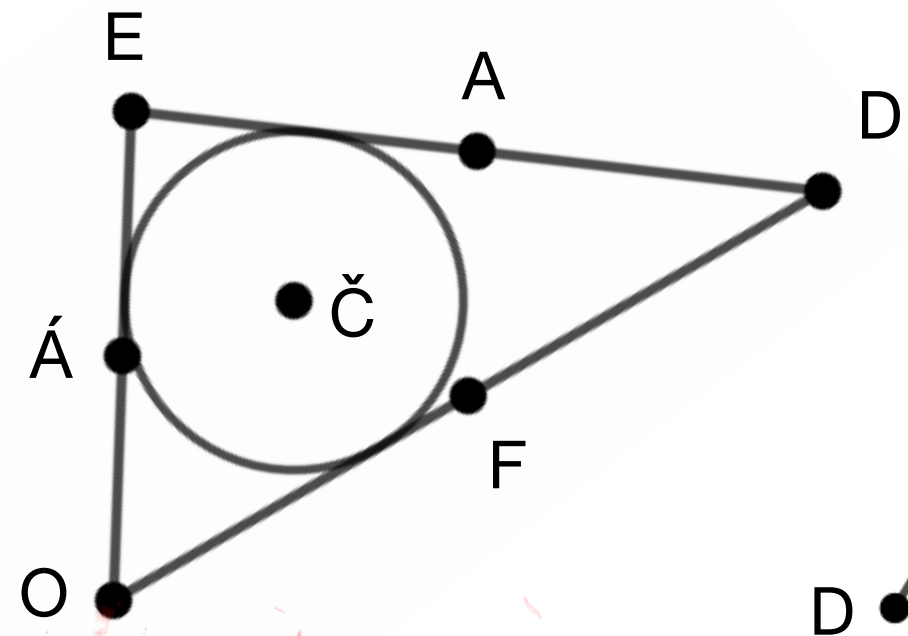




Začni s nejmenším počtem 🍌 🍌

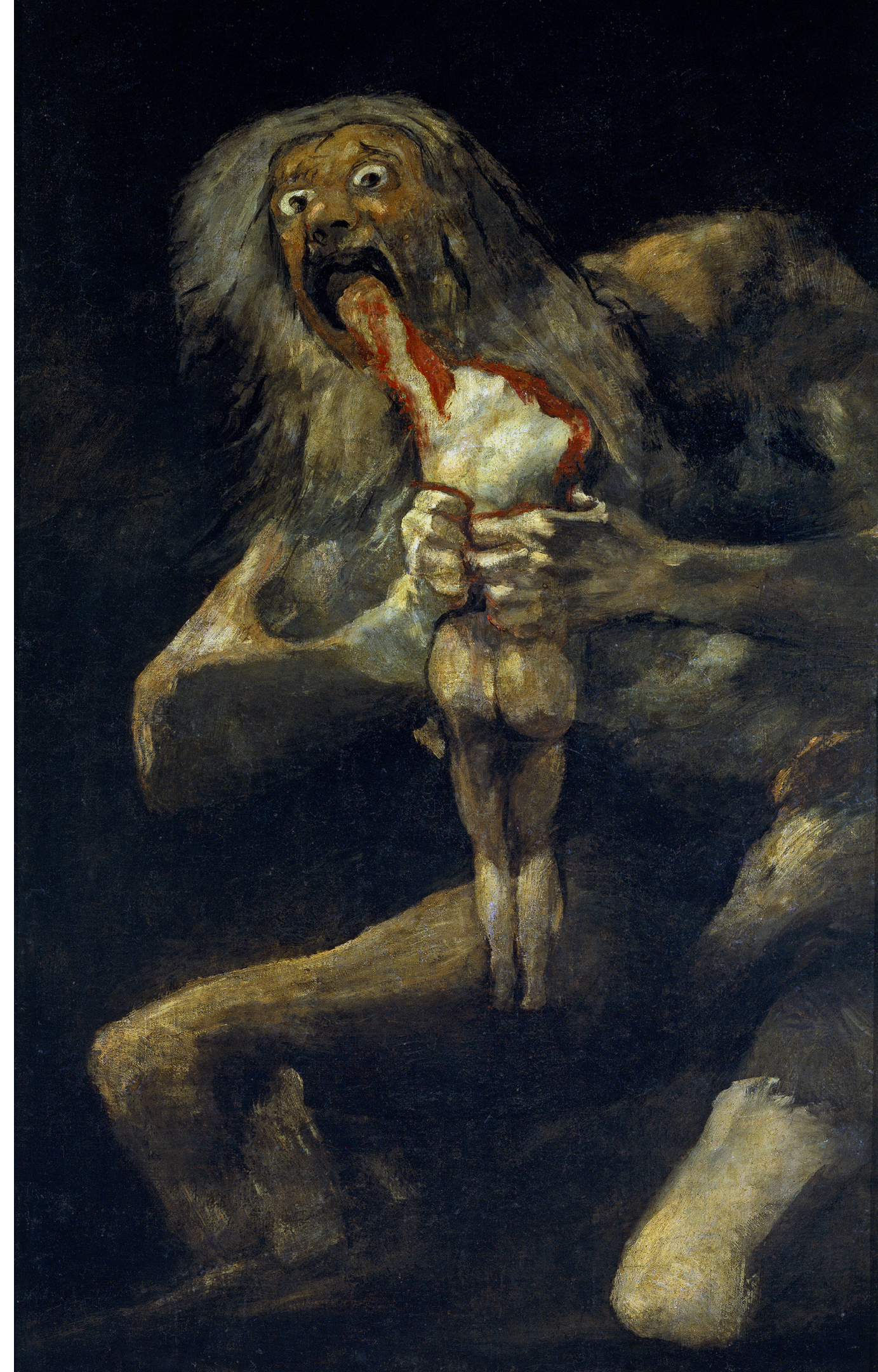


UCIEJMPP
ULFPQLFDN
SEHT



Tudy ne, přátelé!

- Upřednostnění grafiky před obsahem
- Nezvládnuté použití asociační šifry
- Špatný odhad náročnosti
- Problematický výsledek šifer
- Špatně zvolená hesla
- Špatně zadaná aktivita



Šifrované opakování

ŠIFRA 1

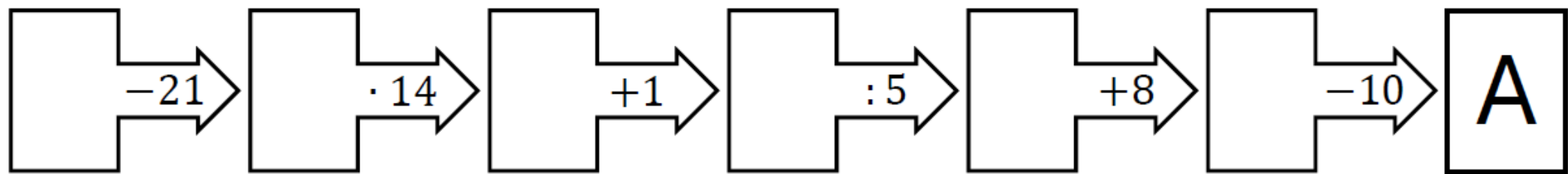
- 3, 6, 9, ...
- 4, 7, 10, ...
- / 5, 8, 11, ...

13, 15, 16, 17, 22, 25, 28, 29, 30, 31, 33, 36, 38, 39, 41, 43, 45, 48, 50, 52

ŠIFRA 2

$13 \cdot 83 \cdot 3761 \cdot 27479 =$

ŠIFRA 3



ŠIFRA 1

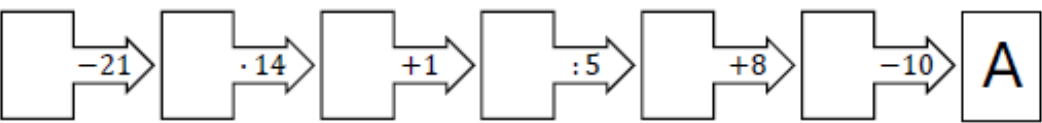
- 3, 6, 9, ...
- 4, 7, 10, ...
- / 5, 8, 11, ...

13, 15, 16, 17, 22, 25, 28, 29, 30, 31, 33, 36, 38, 39, 41, 43, 45, 48, 50, 52

ŠIFRA 2

$13 \cdot 83 \cdot 3761 \cdot 27479 =$

ŠIFRA 3



ŠIFRA 4

(30; 39)

(72; 99)

(21; 105)

(440; 506)

(77; 220)

(120; 495)

(162; 900)

ŠIFRA 5



ŠIFRA 6

0,93 + 1,12	4,09 + 3,02	4,22 + 0,87	0,74 + 0,36	3,57 + 2,46	8,01 + 0,24	0,29 + 3,83	1,53 + 1,66
-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------

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
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Šifrované opakování

ŠIFRA 1

- 3, 6, 9, ...
- 4, 7, 10, ...
- / 5, 8, 11, ...

13, 15, 16, 17, 22, 25, 28, 29, 30, 31, 33, 36, 38, 39, 41, 43, 45, 48, 50, 52

ŠIFRA 4

(30; 39)

(72; 99)

(21; 105)

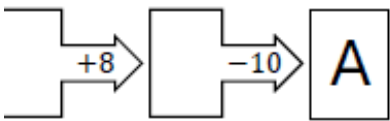
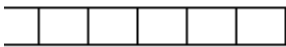
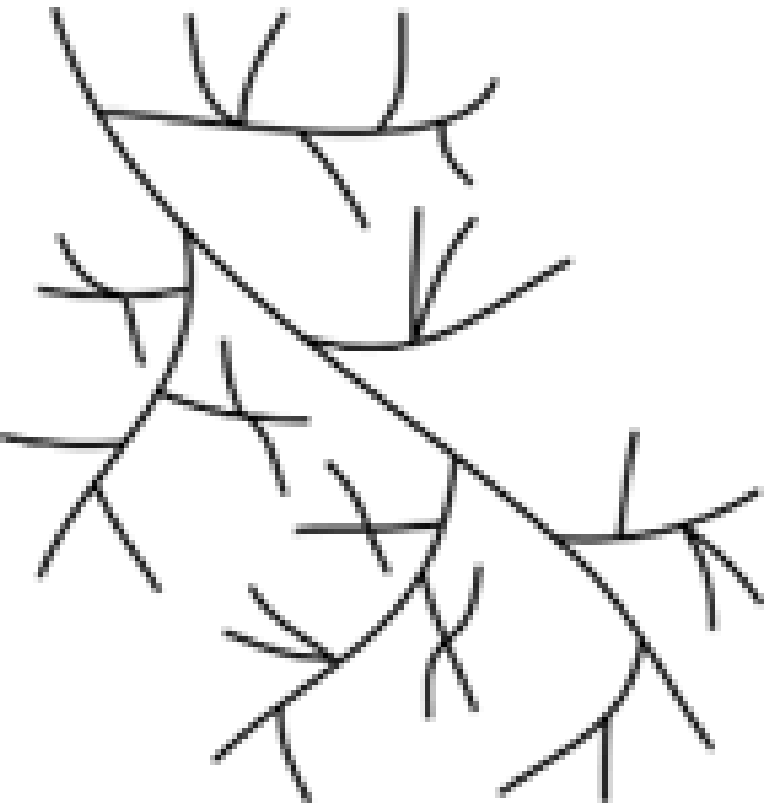
(440; 506)

(77; 220)

(120; 495)

(162; 900)

ŠIFRA 5



ŠIFRA 5



3,57 + 2,46	8,01 + 0,24	0,29 + 3,83	1,53 + 1,66
-------------	-------------	-------------	-------------

ŠIFRA 6

0,93 + 1,12	4,09 + 3,02	4,22 + 0,87	0,74 + 0,36	3,57 + 2,46	8,01 + 0,24	0,29 + 3,83	1,53 + 1,66
-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

Jak šifry použít

- Opakování látky
- Speciální hodiny (vánoční, předprázdninové)
- Badatelská výuka
- Průběžná práce (pro nadané)



Proč šifry použít

- Jiné uchopení matematického obsahu
- Hlubší princip (nejen) matematiky:
 - Hledání řádu, struktury, souvislostí
 - Práce se strukturou
 - Algoritmizace
- Spolupráce žáků v nezvyklé situaci
- Emoce při řešení



Zásady dobrých školních šifer

- Grafika nerozptyluje pozornost
- Náročnost šifer je dobře odhadnuta (nebo kompenzována)
- Správně volená hesla – jasně rozpoznatelná
- Uvědomělé zadání aktivit

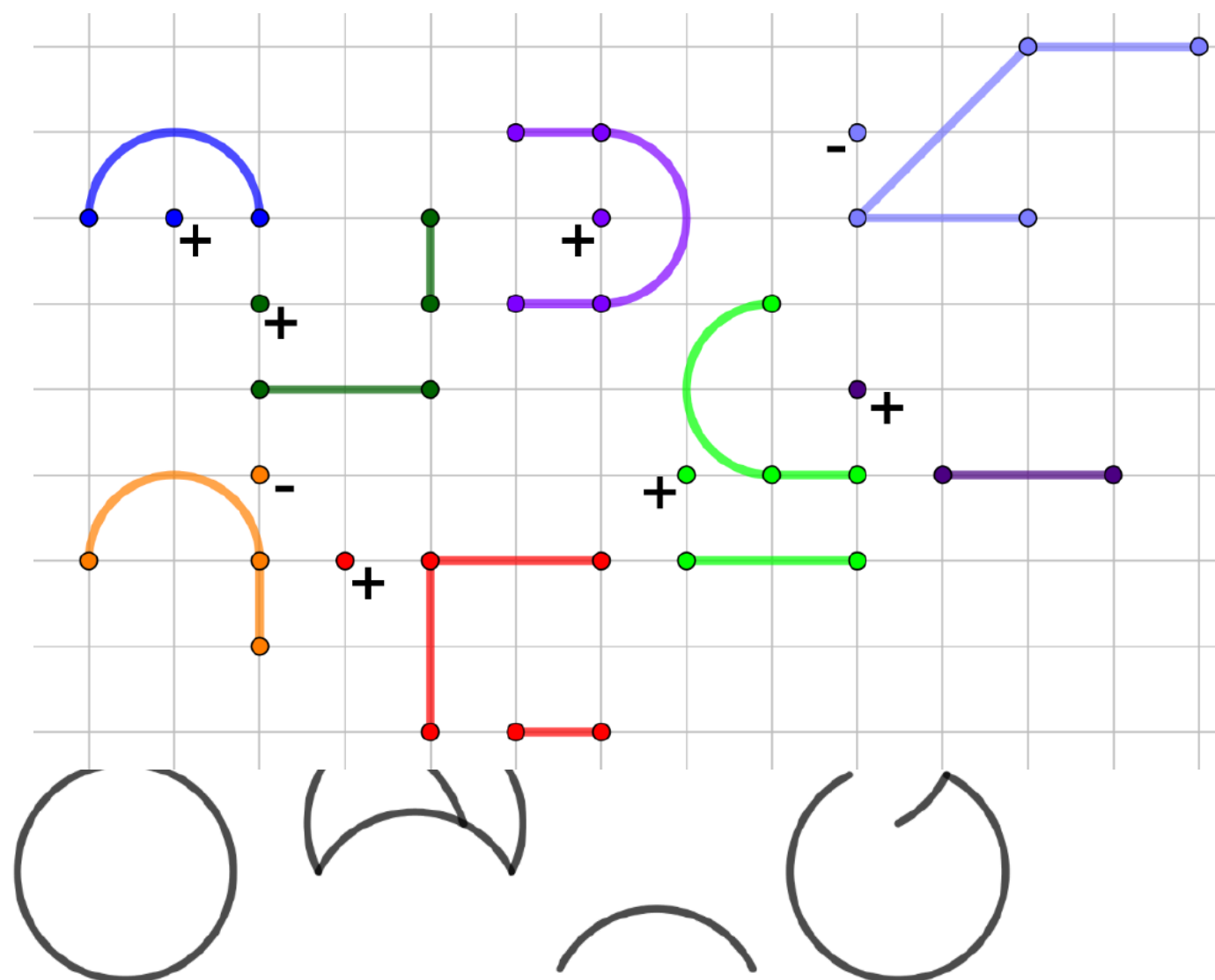
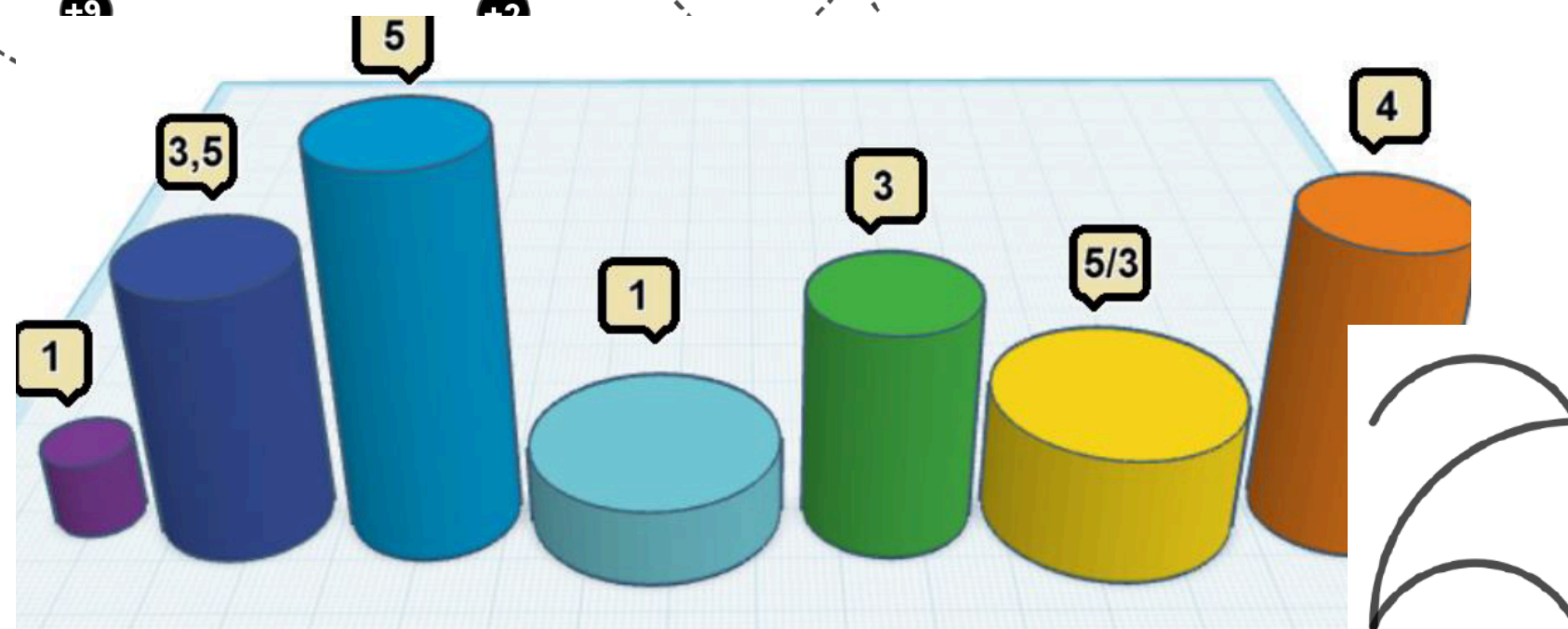
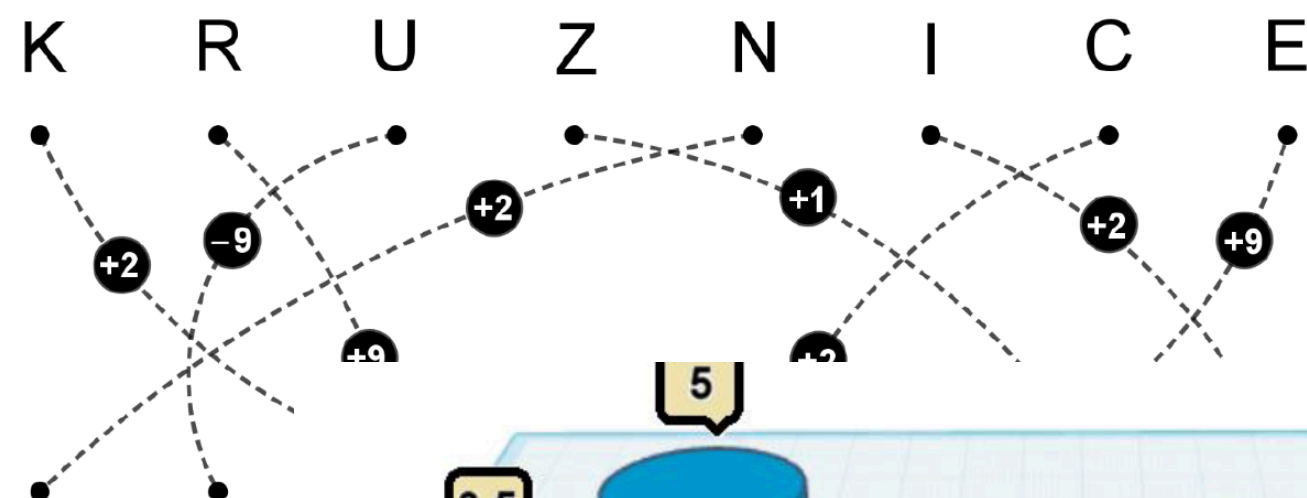


Kde hledat inspiraci



LETNÍ ŠKOLA

GEOMETRIE



Kde hledat inspiraci

