



Rekreační šifrování

Šifry Školní šifrovací soutěže 2013–2014

Karel Pazourek



NOVÉ VÝZVY PRO TŘEBOŇSKO, ČÍSLO PROJEKTU CZ.1.07/1.1.14/02.0050



evropský
sociální
fond v ČR



EVROPSKÁ UNIE



MINISTERSTVO ŠKOLSTVÍ,
MLÁDEŽE A TĚLOVÝCHOVY



OP Vzdělávání
pro konkurenceschopnost

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Karel Pazourek

Rekreační šifrování. Šifry Školní šifrovací soutěže 2013–2014.

Vydalo Gymnázium, Třeboň, Na Sadech 308 v roce 2014 nákladem 100 kusů.

Publikace byla podpořena projektem Nové výzvy pro Třeboňsko, číslo projektu CZ.1.07/1.1.14/02.0050.

Obsah

Úvod	5
<i>O čem je tato příručka</i>	<i>5</i>
1. Rekreační šifrování a šifrovací soutěže	6
<i>Rekreační šifrování – specifika</i>	<i>6</i>
<i>Šifrovací hry a soutěže</i>	<i>6</i>
2. Šifry, kódy a jejich typy	7
<i>Nauky o utajování zprávy</i>	<i>7</i>
<i>Základní pojmy kryptologie</i>	<i>8</i>
<i>Substituční šifry</i>	<i>8</i>
Princip substituční šifry	8
Monoalfabetické substituce	8
Kódování a substituce	11
Kódování a počítače	12
Morseova abeceda	12
Braillovo písmo	14
Binární abeceda	14
<i>Transpoziční šifry</i>	<i>15</i>
<i>Asociační šifry</i>	<i>15</i>
<i>Grafické šifry, prostorové šifry a předměty v šifrování</i>	<i>16</i>
Grafické šifry	16
Předměty v šifrování	16
Šifry v prostoru	17
<i>Šifry využívající schémata</i>	<i>17</i>
<i>Víceúrovňové šifry</i>	<i>19</i>
<i>Šifry se specifickým postavením</i>	<i>20</i>
Úvodní šifry a aktivity	20
Závěrečné šifry a aktivity	21
<i>Určování typu šifry</i>	<i>22</i>
Počítání a šifra	22
3. Vybavení pro šifrovací hru	24
<i>Materiální vybava</i>	<i>24</i>
<i>Psychická vybava</i>	<i>24</i>
4. Školní šifrovací soutěž	25
<i>Cíle soutěže</i>	<i>25</i>

<i>Průběh soutěže</i>	<i>25</i>
5. Šifry ze Školní šifrovací soutěže.....	26
<i>Zadání šifer</i>	<i>26</i>
Substituční šifry	26
Transpoziční a vybírací šifry.....	29
Textové a vyhledávací šifry.....	32
Asociační šifry	34
Grafické šifry.....	37
Šifry využívající schémata	43
Víceúrovňové šifry	47
<i>Řešení šifer.....</i>	<i>49</i>
Substituční šifry	49
Transpoziční a vybírací šifry.....	53
Textové a vyhledávací šifry.....	55
Asociační šifry	57
Grafické šifry.....	59
Šifry využívající schémata	63
Víceúrovňové šifry	67
6. Pracovní listy	69
<i>Pracovní list 1 – Transpoziční šifra a kombinatorika.....</i>	<i>70</i>
<i>Pracovní list 2 – Substituční šifry, kódování a kombinatorika.....</i>	<i>72</i>
<i>Pracovní list 3 – Posuny abecedy a dělitelnost čísel Úlohy.....</i>	<i>74</i>
<i>Pracovní list 3 – Posuny abecedy a dělitelnost čísel Řešení a návod pro učitele.....</i>	<i>76</i>
<i>Pracovní list 4 – Šifrování a grafy funkcí Řešení a návod pro učitele</i>	<i>79</i>
<i>Pracovní list 4 – Šifrování a grafy funkcí Úlohy.....</i>	<i>84</i>
<i>Pracovní list 5 – Graf logaritmické funkce</i>	<i>87</i>
<i>Pracovní list 5 – Graf logaritmické funkce Řešení a návod pro učitele.....</i>	<i>89</i>
<i>Pracovní list 6 – Římské číslice Úlohy.....</i>	<i>92</i>
<i>Pracovní list 6 – Římské číslice Řešení a návod pro učitele</i>	<i>94</i>
Rejstřík.....	97
Bibliografie.....	98

Úvod

O čem je tato příručka

Tato příručka je výstupem projektu Nové výzvy pro Třeboňsko, číslo CZ.1.07/1.1.14/02.0050, podpořeného globálním grantem Operačního programu Vzdělávání pro konkurenceschopnost.

Rekapituluje témata, kterými se zabývala Školní šifrovací soutěž. Zároveň slouží jako návodná příručka pro účastníky v této, ale i dalších šifrovacích soutěžích.

Obsahuje teoretickou část, která se zabývá šifrovacími soutěžemi jako takovými a jednotlivými typy šifer, které se v nich objevují. Šifry jsou rozděleny do několika kategorií, u každé z nich jsou pak diskutována její specifika a možné způsoby prolamování takových šifer. Nechybí ani úvaha o vybavení účastníka šifrovací hry. Závěrem teoretické části je deskripce Školní šifrovací soutěže, jejích cílů a jejího průběhu.

Praktická část příručky je sestavena z šifer, které se vyskytly ve Školní šifrovací soutěži ve školním roce 2013–2014. Je opět rozdělena do skupin podle typů šifer, prezentovaných v teoretické části. Ke každé šifře je uvedeno i její řešení. Jsou rovněž připojeny i pracovní listy pro využití šifer při výuce matematiky. Pracovní listy byly ověřovány v hodinách matematiky na gymnáziu Třeboň.

1. Rekreační šifrování a šifrovací soutěže

Rekreační šifrování – specifika

Rekreační šifrování je specifickou volnočasovou aktivitou. Její podstatou je řešení (luštění) různých úkolů či úloh (šifer), kdy jejich cílem je většinou získat informaci (heslo, popis dalšího stanoviště atp.). Uplatňují se zde různé schopnosti a dovednosti, zejména induktivní myšlení, díky němuž účastník jednotlivé aspekty šifry či úkolu složí v postup vedoucí k vyřešení šifry; dále pak geometrickou představivost, práci s asociacemi, kombinační myšlení, vyhledávání a třídění informací, práce v týmu a jeho vedení ad.

Vedle toho se v rekreačním šifrování užívají specifické znalosti, zejména luštění jednoduchých šifer, převod pomocí základních kódování nebo samotná práce s šifrou. Čím je účastník nebo tým zkušenější, tím více nabývá právě těchto znalostí a dokáže je lépe použít v samotných hrách.

Rovněž se účastník Školní šifrovací soutěže dostává do kontaktu s tradicí šifrování – ať už jednotlivých soutěží, anebo aktivity jako takové. Tím rozumíme znalost šifer, které byly použity v proběhlých soutěžích, ale i znalost komunity, která se utváří právě kolem těchto aktivit.

Šifrovací hry a soutěže

Šifrovací hry a soutěže můžeme dělit podle několika kritérií:¹

Můžeme je rozdělit podle četnosti opakování na soutěže tradiční a jednorázové (popř. začínající). Tradiční soutěže (jako jsou např. Bedna nebo Tmou) využívají zkušeností získaných z předchozích ročníků pro vylepšování a směřování soutěže. Rovněž mohou těžit i z okruhu fanoušků a podporovatelů. Jednorázové soutěže pak bývají dobrodružstvím jak pro účastníky, tak pro organizátory – účastníkům často přinášejí netypické úkoly, (nezkušené) organizátoři pak v průběhu hry poznávají různé mechanismy hry a organizační problémy, na které se mohou pak soustředit i v dalších soutěžích a hrách. Ostatně i zkušeným organizátorům každý ročník soutěže přináší nové poznatky o tom, co by mohli zlepšit.

Šifrovací hry také můžeme rozdělit na kontaktní a korespondenční hry. Kontaktní hry se vyznačují přímým kontaktem mezi účastníky a organizátory. Konají se na určeném místě (resp. v určeném prostoru, v městském či v terénu) v určeném čase (mohou být denní, noční i několikadenní). Jednotlivé úkoly pak nemusí mít podobu textu, ale mohou se skládat z různých fyzických aktivit nebo práce s předměty. Oproti tomu korespondenční soutěže (jako je Sendvič nebo korespondenční část Školní šifrovací soutěže) zapojují účastníky do hry obvykle prostřednictvím internetu. Proto v týmových hrách nemusí členové jednoho týmu být na jednom místě. Dále umožňuje vyžadovat po účastnících připojení k internetu – a pracovat tak s informacemi pomocí internetu dosažitelných (např. encyklopedické znalosti, videa, zvukové nahrávky).

Můžeme snadno rozlišit i hry týmové a pro jednotlivce. Týmových her je naprostá většina. Práce v týmu umožňuje efektivně využívat celé řady metod řešení (brainstorming, rozdělení dílčích úkolů).

¹ Srovnej s Almanachem Tmou [9], s. 24–27, 34–39.

Šifrovací hry můžeme rozdělit i podle náročnosti. Mezi obtížné hry, ve kterých uspějí zejména zkušené týmy, patří již zmiňovaná Bedna nebo Tmou. Jiné soutěže se v alespoň některých kategoriích soustředí i na začínající hráče (Želvování, Dětská šifrovací liga Mensy, Školní korespondenční soutěž).

Rovněž průběh soutěží se může lišit: Lineární soutěže fungují tak, že jsou luštěny postupně jedna šifra za druhou. Oproti tomu nelineární soutěže se mohou větvit (tj. lze postupovat nebo se i musí postupovat po různých řetězcích šifer). Někdy je k lineárnímu řetězci šifer přidán průběžný úkol. Internetové soutěže pak bývají téměř úplně nelineární: Šifry se řeší po sadách či skupinách, nezáleží na pořadí vyluštění šifry ve skupině.

Přehled šifrovacích soutěží pak najdeme v Kalendáři šifrovací her (<http://kalendar.chlyftym.cz/>, citováno 19. 10. 2014). Současné soutěže vhodné i pro začátečníky a děti (popř. v příslušných kategoriích) jsou uvedeny v Tabulka 1.

Název	Termín konání	Webové stránky
Dětská šifrovací liga	celý rok	http://www.mensa.cz/volny-cas/hlavolamy/detska-sifrovaci-liga/
Školní šifrovací soutěž	celý rok	http://www.gymtrebon.cz/a-1097-skolni-sifrovaci-soutez-2013-2014.html http://www.gymtrebon.cz/a-1493-skolni-sifrovaci-soutez-2014-2015.html
Želvování	květen/červen	http://www.sifrovackacb.cz/

Tabulka 1: Šifrovací hry vhodné pro začátečníky a děti

2. Šifry, kódy a jejich typy

V následujícím textu ukážeme základní třídění šifer a kódů v podobě, v jaké byly prezentovány ve Školní šifrovací soutěži. Jedná se o stručný přehled, který je určitým způsobem zaměřený, a tudíž nezahrnuje všechny podoby a typy šifer, které se v šifrovacích hrách vyskytují.

Začněme se samotnými pojmy a principy.

Nauky o utajování zpráv

Rekreační šifrování čerpá z rozsáhlé tradice utajování zprávy. Opírá se především o steganografii a kryptologii.

Steganografie je nauka o utajení existence zprávy. Luštitel tak nemá tušit, že je tu cokoliv k luštění. Známými příklady jsou využití mikroteček nebo ukrytí zprávy v obrázku na internetu.

Kryptologie je nauka o utajení smyslu zprávy. Dělí se na kryptografii, zabývající se tvorbou systémů na utajení smyslu zprávy, a samotnou kryptologii, jejímž cílem je luštění zpráv bez znalosti systému, popř. hesla či klíče. Obě tato odvětví spolu úzce souvisí. V tomto textu se však nebudeme jimi zabývat podrobně, pouze poukážeme na využití jejich výsledků v rekreačním šifrování.

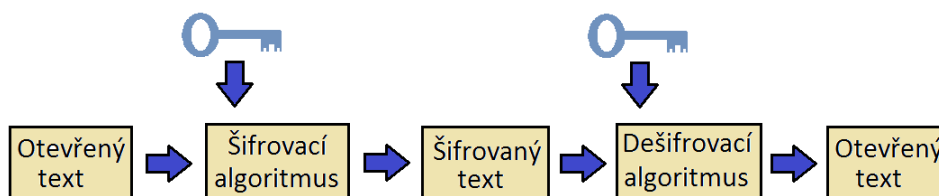
Podstatnou změnou oproti profesionálnímu šifrování je odlišný cíl rekreačního šifrování – šifra má být prolomena po určitém úsilí.

Vedle těchto nauk se v šifrovacích hrách často využívá i různých hádanek, rébusů, křížovek a jim příbuzných schémat, různých stolních her (domino, šachy, logik atd.), logických her (sudoku) nebo i počítačových her (tetris, hra života apod.) a mnoha dalších aktivit.

Základní pojmy kryptologie

Způsob, pomocí něhož byla zpráva zašifrována, se nazývá **šifrovací (šifrový, kryptologický) systém**. Ten určuje samotný **šifrovací algoritmus** (např. přehazování písmen, posun písmen v abecedě atd.). Vedle toho k zašifrování konkrétní zprávy se často využívá ještě tzv. **šifrovací klíč**, který určuje konkrétní průběh šifrovacího algoritmu (např. že písmena slov zprávy se přehazují podle pořadí v abecedě; písmena se v abecedě posunují vždy o 2).

Vedle toho je třeba uvažovat soubory znaků, se kterými pracují šifrovací systémy. Jednak je to **abeceda otevřeného textu** (tj. původní zprávy) a jednak je to **šifrová abeceda** (která obsahuje znaky šifrovaného textu). Typickým příkladem používané abecedy otevřeného textu (ale často i šifrové abecedy) je tzv. **mezinárodní abeceda**, která sestává z 26 písmen bez diakritiky a CH (to se chápe jako dva znaky C a H).



Obrázek 1: Schéma šifrování zprávy

Nejčastěji klasické šifrovací algoritmy dělíme na dva typy: substituční a transpoziční. Ty se dají v jednotlivých šifrovacích systémech různě kombinovat. Oba typy pak budou vysvětleny v následujících odstavcích, spolu s dalšími typy metod a aktivit užívaných v rekreačním šifrování.

Substituční šifry

Princip substituční šifry

Substitute znamená nahrazení. Mohou se nahrazovat jednotlivá písmena zprávy, dvojice písmen (bigramy) nebo větší skupiny písmen, popřípadě celá slova. Nicméně se jedná o univerzální princip (mohou se nahrazovat např. na základě asociací části obrázků apod.).

Monoalfabetické substitute

Nejjednodušším typem substitute je tzv. **jednoduchá monoalfabetická substitute**, při které se nahrazuje každé písmeno otevřeného textu písmenem šifrovaného textu, a to podle neměnného pravidla. Tedy písmenu abecedy otevřeného textu jednoznačně odpovídá písmeno šifrové abecedy.

Jejím základním typem je tzv. **posun**, kam řadíme i **Caesarovu šifru** (někdy se všechny posuny nazývají Caesarova šifra). Při posunu se všechna písmena otevřeného textu nahradí znaky v abecedě posunutými o pevně daný počet pozic, při Caesarově šifře se posouvá o 3 pozice. Abeceda se využívá cyklicky, tj. když dojdeme na konec abecedy, začneme znovu od začátku a obráceně.

D	K	R	M
↑	↑	↑	↑
C	J	Q	L
↑	↑	↑	↑
B	I	P	K
↑	↑	↑	↑
A	H	O	J
↓	↓	↓	↓
Z	G	N	I
↓	↓	↓	↓
Y	F	M	H
↓	↓	↓	↓
X	E	L	G

Tabulka 2: Zašifrování slova AHOJ pomocí posunu

Můžeme též využít **posunu pomocí klíče**. Stačí první písmena abecedy nahradit písmeny klíče a ostatní písmena abecedy příslušně posunout. Klíč musí mít všechna písmena různá (popřípadě opakovaná písmena se musí vynechat). Například pokud klíčem je slovo TAJNE, pak posun abecedy bude následující:

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

Tabulka 3: Posun pomocí klíče

Zpráva TREBON JE LAZENSKE MĚSTO se pak zašifruje jako SQEAML GE ITZELRHE KERSM.

Písmena abecedy se někdy **nahrazují zlomky**. Rozdělíme písmena abecedy do pětic (jako v následující tabulce; písmeno W je vynecháno, aby bylo pouze 25 písmen, lze vynechat i Q nebo považovat I a J za jedno písmeno):

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	X	Y	Z
1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5
1					2					3					4					5				

Tabulka 4: Substituce zlomky

Číslo v druhém řádku představuje čitatel a číslo ve třetím řádku jmenovatel zlomku. Slovo SIFROVANI se pak nahradí zlomky

$$\frac{4}{4} \frac{4}{2} \frac{1}{2} \frac{3}{4} \frac{5}{3} \frac{2}{5} \frac{1}{1} \frac{4}{3} \frac{4}{2}$$

Polybiův čtverec je dalším typem substituční šifry využívající tabulku. Písmena se uspořádají do následující tabulky (písmeno J je nahrazováno I; v jiných variantách se obdobně píše U místo V nebo V místo W):

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Tabulka 5: Polybiův čtverec

Písmenům pak odpovídá vždy dvojice čísel řádku a sloupce. Slovo SIFROVANI pak se zašifruje jako 43 24 21 42 34 51 11 33 24. Zde tedy jedno písmeno je nahrazováno dvojicí čísel.

Jednoduchá monoalfabetická substitute je snadno prolomitelná. Zvláště posun – šifrovacími klíči pro zašifrování i dešifrování je shodně počet pozic, o který se písmena posunují. Možných posunů je přitom pouze 25.

Pokud zvolíme jiný způsob přiřazení písmen abecedy otevřeného textu a šifrové abecedy, zvýšíme obtížnost. Nicméně pak bude existovat pouze $403\,291\,461\,126\,605\,635\,583\,999\,999 \div 4 \cdot 10^{26}$ možných substitucí, což je při použití počítače snadný úkol pro luštitel. Ostatně monoalfabetické substitute byly prolamovány o mnoho dříve, než spatřily světlo světa počítače. Už z 9. století se nám zachoval spis Rukopis o dešifrování kryptografických zpráv od al-Kindiho, ve kterém je popsána metoda zvaná **frekvenční analýza**. Její podstatou je, že v daném jazyce se v průměrném textu vyskytuje od každého písmene určitý podíl písmen (např. v češtině jsou nejčastějšími písmeny e a o). Pokud tedy nahradíme nejčastější znaky šifrovaného textu nejčastějšími znaky, budeme moci následně s trochou trpělivosti doplnit i další znaky a zprávu doložit. Uvádí se, že tato metoda bývá jednoznačná pro zprávy o délce alespoň 50 znaků.

Aby se luštění ztížilo, můžeme využít **klamačů**. Jsou to znaky, které nenesou žádnou informaci, ale ztěžují rozluštění zprávy. Jsou vkládány do textu a mění tak frekvenci znaků. Například můžeme využít toho, že se písmena Q, W a X v českém textu vyskytují velmi málo, takže pokud je přidáme do zprávy, mohou v něm mít klamače jinou frekvenci než je obvyklé:

TREXBON JEXQW LAZENSKEW MĚSTQO

Příjemce, který zná šifrovací algoritmus a dešifrovací klíč tato písmena snadno ze zprávy odstraní a otevřený text přečte. „Nepřítel“, který chce šifru prolomit bez znalosti klíče, má tak ztíženou pozici.

Klamače se však v rekreačním šifrování vyskytují i v jiných typech šifer než substitučních, jsou to jakékoliv části šifry, které se při luštění nevyužijí, například písmena v tabulce, která se vynechají a přečtou se jen ostatní apod. Některé části šifry nemusí být využity přímo pro rozluštění, ale odkazují na způsob zašifrování, nejjednodušším příkladem je nápověda u šifry.

Další metodou je **použití kódů** pro často se opakující slova nebo slabiky. Pokud se například v textu často objevuje slovo MĚSTO, můžeme jej nahradit znaky QQW:

TREBON JE LAZENSKE **QQW**

Z historie známe příklady využití jednoduché substituce spolu s kódy a klamači. Je jím případ Marie Stuartovny, kdy prolomení šifry, kterou používala se spiklenci, posloužilo jako klíčový důkaz pro její obžalobu a následnou popravu. Více informací o tomto procesu lze nalézt například v knize S. Singha [1].

Složitější formou substituce je **polyalfabetická substituce**. Využívá několik různých substitucí, například lichá písmena posuneme o 5 znaků a sudá posuneme pomocí hesla TAJEMNO (využívám tak 2 substituce).

Známým příkladem polyafabetické substituce je **přičítání klíče**. K písmenům otevřeného textu se přičtou písmena klíče, a to tak, že se sečtou pozice písmen otevřeného textu a klíče:

Například pokud klíčem je slovo TAJNE, pak písmena klíče převedeme na jejich pořadí v abecedě (19; 0; 9; 13; 4), o ně pak posuneme prvních pět písmen zprávy, pak další pětici atd. Je-li zprávou TREBON JE LAZENSKE MĚSTO, rozdělíme ji do pětic (poslední pětici popřípadě doplníme klamači):

TREBO NJELA ZENSK EMEST OXXXX

Pak posunujeme jednotlivá písmena pětic o udaný počet pozic:

MRNOS GJNYE SEWFO XMNFX HXGKB

Jedná se v podstatě o slavnou a v novověku hojně využívanou **Vinegèrovu šifru**.

Pokud je heslo kratší, přičítá se opakovaně k textu. Tento způsob není příliš bezpečný. Lepší je využít heslo, které je stejně dlouhé jako text, který potřebujeme zašifrovat. Pokud však použijeme smysluplné heslo, zpráva bude snadno rozluštitelná. Příkladem je použití textu předem určené knihy, čehož se skutečně v historii využívalo zejména pro zprávy s krátkodobou potřebou utajení. Pokud by se však používalo pro přičtení heslo beze smyslu, které je náhodným souhrnem znaků abecedy, zpráva by byla téměř neluštitelná. Pokud navíc se dané heslo použije pro zašifrování pouze jediné zprávy, pak dostáváme dokonalou šifru – zašifrovaný text nelze prolomit. Tohoto bylo využíváno v druhé polovině 20. století pro komunikaci mezi prezidenty USA a Sovětského svazu, viz knihu [1].

Na principu substituce funguje i proslulý šifrovací stroj Enigma, používaný zejména německou armádou za 2. světové války. Historie jeho dešifrování je vynikající ukázkou práce špiónážních služeb, konstruktérů a matematiků. Mezi nejznámější matematiky spojené s dešifrováním Enigmy patří Polák Marian Rejewski a Brit Alan Turing. Podrobnější informace lze nalézt v knize [1] nebo na stránkách [2] či [3].

Kódování a substituce

Možná bude pro čtenáře překvapením, že např. Morseova abeceda není substituční šifrou. Není totiž šifrou vůbec. Proč? Protože je „pouze“ kódováním.

Kódování je přepis znaků (nebo jejich skupin) otevřeného textu pomocí nových symbolů. Přepis je striktně dán, například pomocí tabulky. Způsob převedení bývá veřejný, neutahuje se. Tedy kódování neslouží k utajení zprávy. Většinou je tomu naopak.

Kódování se používá pro přenos informace pomocí zvoleného kanálu. Například Morseova abeceda byla vymyšlena pro přenos zpráv pomocí telegrafu, Braillovo písmo slouží slepým, atd. Jako kódování můžeme chápat i zapsání textu jiným písmem jako je azbuka, klínové písmo, japonská či čínská písma. Jiná známá kódování jsou uzlové písmo, semaforová abeceda, vlajková abeceda nebo binární abeceda.

Kódování tedy šifrou samo o sobě není, může však být v šifrování rozmanitě využito. Následují podrobnější informace o některých kódováních.

Kódování a počítače

S příchodem počítačů se pojem kódování rozšířil i do tohoto odvětví. **Kódování znaků v počítači** je založeno na některém ze standardů (například ASCII nebo Unicode).



Obrázek 2: Čárový kód odpovídající textu **Šifrování v Třeboni** ve standardu Code 128 (generováno pomocí [4])

Dalším moderním kódem jsou **čárové kódy**, které jsou opět různě standardizovány. Nejpoužívanějšími jsou EAN, Code 128 nebo dvourozměrný QR kód.



Obrázek 3: QR kód odpovídající textu **Školní šifrovací soutěž v Třeboni** (generováno pomocí [5])

I **barvy** se kódují v počítačích. Nejznámějšími standardy jsou RGB a CMYK.

Morseova abeceda

Morseova abeceda, krátce morseovka, je jedním z nejznámějších příkladů kódování. Byla vymyšlena Samuelem F. B. Morsem pro zakódování znaků abecedy do signálů, které by bylo možné přenášet pomocí telegrafu. Podobných kódovacích systémů se používalo několik, samotná morseovka byla několikrát upravována (naposledy v roce 2003 byl přidán kód pro zavináč). Dnes je spravována Mezinárodní telekomunikační unií (ITU), což je orgán OSN.

Morseovka kóduje písmena mezinárodní abecedy pomocí kódů o 1 až 4 znacích, čísla 0 až 9 pomocí pětimístných kódů, interpunkční znaky a další pak pomocí šestimístných kódů. Kódy pro písmena (viz Tabulka 6) nebyly zvoleny náhodně. Délka kódu odpovídá četnosti výskytu písmene v anglicky psaném textu (nejčastěji se vyskytují E a T atd.). Morse tak chtěl zefektivnit přenos zpráv.

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

Tabulka 6: Znaky Morseovy abecedy pro písmena anglické abecedy

Často jsou používána tzv. **pomocná slova**, odkazující na kódy písmene pomocí délek slabik. Nejsou nijak jednoznačně stanovena (na stránkách Wikipedie [6] lze najít odkazy na několik verzí), nicméně nejpoužívanější verze jsou shrnuty v Tabulka 7.

A	.-	Akát	N	-.	Nástup
B	-...	Blýskavice	O	---	Ó náš pán
C	-.-. .	Cílovníci	P	.--.	Papírníci
D	-..	Dálava	Q	--.-	Kvílí orkán
E	.	Erb	R	.-.	Rarášek
F	..-. .	Filipíny	S	...	Sobota, sekera
G	--.	Grónská zem	T	-	Trám
H		Hrachoviny	U	..-	Uličník, učený
I	..	Ibis	V	...-	Vyučený
J	.---	Jasmín bílý	W	.-.	Vagón klád
K	-.-	Krákorá	X	-..-	Xénokratés
L	.-..	Lupíneček	Y	-.--	Ýgar mává
M	--	Mává	Z	--..	Znamá žena

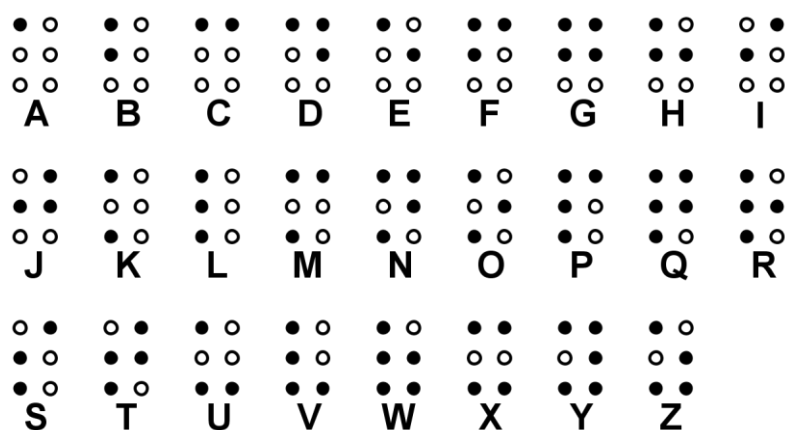
Tabulka 7: Pomocná slova Morseovy abecedy

Další specifickým aspektem morseovky je komunikační kanál, pomocí kterého je předávána. Nejčastěji ji vidíme předávanou písemně pomocí vodorovných čárek, teček a lomítek coby oddělovačů (jedno lomítko odděluje písmena, dvě lomítka slova, tři lomítka věty). Rovněž lze morseovku přenášet světelně např. pomocí pulsů světla (krátké pulsy znamenají tečku, dlouhé čárku) nebo tzv. semaforem (vzpřímený člověk upažuje jednu ruku jako tečku, obě ruce jako čárku). V různých táborových hrách, ale i v hrách šifrovacích, se může morseovka předávat zvukově, např. pomocí píšťalky.

Braillovo písmo

Slepecké Braillovo písmo vymyslel v 18. století Louis Braille, francouzský učitel, sám od dětství slepý. Umožňuje zapsat běžný text, ale i matematické zápisy nebo noty. Jednotlivé národní varianty Braillova písma se liší, vycházíme tak z české normy.

Každé písmeno abecedy je reprezentováno mřížkou 2×3 tvořenou šesti body. V praxi je každý bod buď vyvýšený, anebo ne. V „plošném“, obrázkové podobě je bod černý, anebo bílý. V šifrování se pak binární charakter bodů znázorňuje různě.



Obrázek 4: Znak Braillova písma pro písmena mezinárodní abecedy

V šifrování pak závisí na způsobu přenosu. V grafických šifrách (ale i šifrách jiných typů) lze většinou identifikovat šestiprvkové skupiny, někdy navíc dělené do dvojic či trojic. Dalším poznávacím znamením je binárnost kódu – v šifrovaném textu jsou dva skupiny znaků (ano – ne, má – nemá danou vlastnost atd).

Binární abeceda

Binární abeceda je kód, který přepisuje písmena mezinárodní abecedy pomocí pětice nul a jedniček, a to tak, že tato pětice je zápisem pořadí písmene ve dvojkové soustavě.

A	00001	H	01000	O	01111	V	10110
B	00010	I	01001	P	10000	W	10111
C	00011	J	01010	Q	10001	X	11000
D	00100	K	01011	R	10010	Y	11001
E	00101	L	01100	S	10011	Z	11010
F	00110	M	01101	T	10100		
G	00111	N	01110	U	10101		

Tabulka 8: Binární abeceda

Jedná se opět o binární kód, tedy rozpoznávacím znakem v šifře jsou pětičlenné skupiny s dvěma druhy znaků.

Transpoziční šifry

Transpoziční šifry nemění smysl znaků, jen jejich pořadí – tvoří jejich transpozici. Uvedme pro ilustraci několik jednoduchých transpozic slova SIFROVANI:

- psaní pozpátku: INAVORFIS
- nejdřív souhlásky, pak samohlásky: SFRVNIOAI
- střídavě od začátku a od konce: SIINFARVO
- nejprve písmena na lichých pozicích, pak na sudých: SFOAIIRVN
- transpozice slabik: FRONISIVA

Transponovat můžeme kromě písmen a slabik i slova ve větách nebo v textu, části obrázků (puzzle není vlastně nic jiného než transpozice obrázku), části tabulky apod.

K transpozicím existuje celá řada pomůcek.

Velice jednoduchým příkladem je **plot**. Písmena se napíší do tabulky například o dvou řádcích následovně:

S		F		O		A		I
	I		R		V		N	

Pak se čtou písmena po řádcích a dostaneme šifrovaný text SFOAIIRVN. Vzali jsme tedy nejprve písmena na lichých pozicích a pak písmena na sudých pozicích. Plot můžeme nakreslit i s více řádky, pro tři bychom dostali šifrovaný text SOIIRVNFA:

S				O				I
	I		R		V		N	
		F				A		

Jedná se v podstatě o postupné vybírání písmen podle čísla pozice v textu a její dělitelnosti: Nejprve se berou písmena z pozic, které dělí čtyřka se zbytkem 1, pak ty, co dělí čtyřka se zbytkem 2 nebo 0, a nakonec ty, co dělí čtyřka se zbytkem 3.

Jinou možností je vepsat text do tabulky určitým způsobem a pak jej znovu zapsat jiným způsobem – tomu se pak věnuje kapitola o schématech v šifrování (viz str. 17).

Asociační šifry

Asociační šifry, jak napovídá název, pracují s asociacemi a podobnostmi – slovními, textovými, grafickými či významovými.

Podle toho je můžeme i rozdělit:

- Textové asociace: Text šifry, často poměrně rozsáhlý, může vyvolávat asociace několika způsoby. Jednak to může být stylem textu, odkazujícím se na konkrétní literární text nebo slohový útvar, jednak to může být použitím konkrétních výrazů či slovních spojení, která v kontextu celého textu šifry poukazují na řešení. Mezi tyto šifry můžeme zařadit i práci s texty písní.
- Slovní asociace: V zadání šifry se objevují slova (ne nutně ve větných celcích), která spolu souvisí při správné spojitosti. Nejčastějšími vztahy jsou synonyma, antonyma, ustálená spojení (fráze, přísloví, přirovnání), popřípadě části názvů uměleckých děl, měst, států, organizací a jejich zkratk atp.
- Obrázkové asociace: Různé asociační šifry pracují s obrázky odlišně. Někdy je třeba se soustředit na celé zadání jako celek, jindy na jeho dílčí části. Objevují se tak šifry nakládající všemožně s fotografiemi, logy a grafickými symboly, částmi map atd.

Grafické šifry, prostorové šifry a předměty v šifrování

Grafické šifry

Jak název napovídá, jedná se o šifry na bázi obrázku. Může je tvořit i víc obrázků nebo jejich částí. Často se využívají různá loga, piktogramy a další charakterizující atributy. Patří sem i šifry pracující s mapami.

Principů grafických šifer je velké množství, uvedeme zde některé:

- Je třeba poznat a pojmenovat, co je na obrázku nebo jaké části obrázek tvoří.
- Části obrázku je třeba přeskládat nebo jinak přetvořit.
- Je třeba si všimnout, co je na obrázku neobvyklého či co obrázek narušuje. Tato zvláštnost se pak použije pro řešení šifry.
- Do obrázku je třeba doplnit chybějící část. Je možné i dorýsovat úsečky, vybarvit plochy apod.

Jistým zobecněním grafických šifer jsou pak šifry pracující s prostorovými útvary a předměty, popřípadě se vztahy v prostoru.

Předměty v šifrování

Využití předmětů v šifrování lze rozličnými způsoby. Některé předměty hráč očekává, protože se staly tradičními. Příkladem jsou Bednářské listy ve hře Bedna, kdy organizátoři před hrou vydali „noviny“, které pak mimo jiné sloužily jako návod k šifráům ve hře.

V šifrovacích hrách pak najdeme různé hlavolamy, hry s kostkou, puzzle a skládačky, stolní hry (pexeso), kazety či CD.

S předměty lze pracovat různě:

- Předmět na povrchu obsahuje šifru.

- Předmět obsahuje šifru uvnitř. To může být jasné z kontextu, nebo naopak může být součástí úkolu šifru objevit (např. lísteček schovaný uvnitř diskety, takže samotná disketa je nepoužitelná).
- Předmět je třeba přestavovat (například puzzle).
- Předmět je třeba zničit. Toto bývá riskantní krok, neboť tím jiný předmět znovu nedostane, tudíž se zničení odkládá až na poslední místo.
- Předmět je třeba zkoumat jinými smysly než zrakem a hmatem, speciálně chutí. Ve hrách najdeme využití různých pokrmů (např. bonbónů s různými příchutěmi ve hře Tmou 2006 nebo zákusků s různými kulatými kousky ve hře Želvodání 2014).
- Předmět funguje jako černá skříňka. Je třeba zjistit, co dělá a jak se chová. Skvělým příkladem je Bednička, ze hry Bedna 2009, kde týmy dostaly Bedničku, elektronický hlavolam tvaru krychlové krabice, která se pak různým způsobem používala v průběhu celé hry.

Šifry v prostoru

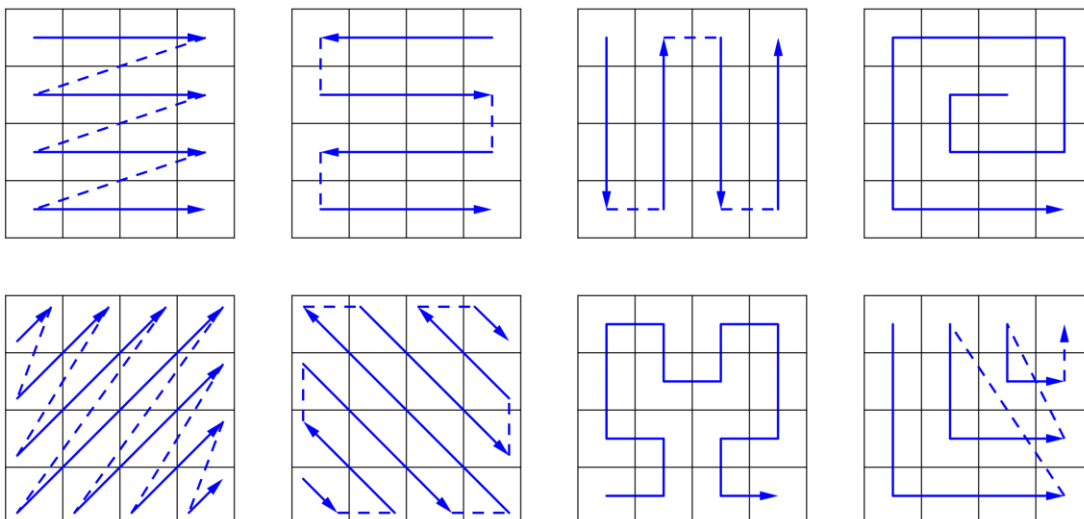
Dále najdeme šifry přímo umístěné ve veřejném prostoru. Příkladem může být morseovka vysílaná z okna domu nebo zprávy v oknech žižkovského vysílače při hře Bedna. Rovněž startovní hry mají často podobu jakési šifry pracující s prostorem, kde jsou do ní někdy zapojeni i hráči sami.

Šifry využívající schémata

Jedná se často o šifry s transpozičním prvkem. Mohou využívat například:

- tabulky různých tvarů;
- mřížku, zvláště pak otočnou mřížku;
- (polský) kříž;
- křížovku, osmisměrku, sudoku nebo podobné rébusy;
- kalendář;
- klávesnici počítače nebo telefonu;
- bludiště nebo labyrint;
- šachovnici.

Začneme **procházením tabulky**. Pokud procházíme všechna pole tabulky (což se ne vždy dělá), jedná se o transpoziční šifru. Procházet tabulku můžeme celou řadou způsobů, viz Obrázek 5: Procházení tabulky. Jinou možností je využít skákání šachového jezdce, tzv. **jezdcovy procházky**.



Obrázek 5: Procházení tabulky

Rovněž je možné z tabulky vybírat pouze některá pole. Specificky využívá tabulky **Playfairova šifra**, která ji používá jako klíč pro substituci dvojic písmen.

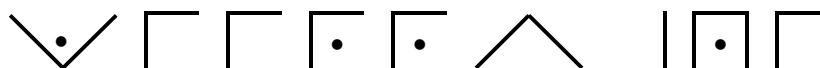
Otočná mřížka je klasickou šifrovací pomůckou, která umožňuje pomocí prázdných polí mřížky vybírat pole z tabulky o stejných rozměrech.

Podívejme se na využití křížů. **Polský kříž** se obvykle používá ve dvou formách. **Malý polský kříž** rozděluje písmena do následujícího schématu:

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

Tabulka 9: Malý polský kříž

Zprávu pak zašifrujeme pomocí ohraničení políčka v kříži a případné tečky, například slovo SIFROVANI se přepíše takto:



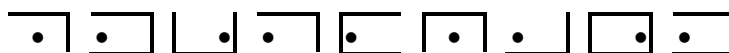
Obrázek 6: Příklad užití malého polského kříže

Velký polský kříž tvoří jediná tabulka obsahující 27 znaků včetně Ch (alespoň nejčastěji používaná verze):

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

Tabulka 10: Velký polský kříž

Písmeno je pak určeno ohraničením políčka a polohou tečky (vlevo, uprostřed, nebo vpravo). Zpráva SIFROVANI se přepíše takto:



Obrázek 7: Příklad užití velkého polského kříže

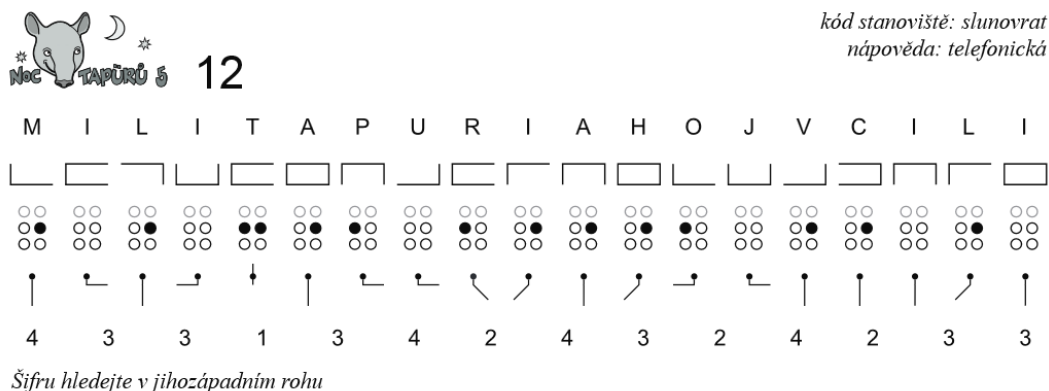
Existuje pak celá řada dalších křížů a jejich využití. jako je hebrejšťina neboli trojitý kříž.

Víceúrovňové šifry

Šifru často nelze přiřadit k některému z výše uvedených typů, ale kombinuje několik postupů. Setkáme se tak např. s šiframi, které luštíte pomocí morseovky a asociací nebo třeba pracujete s tabulkou obsahující obrázky nebo znaky Braillova písma. Takovým šifrářem se říká víceúrovňové, vícestupňové, mnohastupňové apod.

Někdy je třeba používat tyto postupy najednou, jindy je používáme postupně (například nejprve pomocí asociací dostaneme pomocná slova k písmenům morseovky a následně ve druhém kroku rozkódováním morseovky dostaneme řešení šifry).

Příkladem víceúrovňové šifry s více postupy je šifra 12 z ročníku 2011 hry Noc Tapürů:



Obrázek 8: Šifra 12 ze hry Noc tapürů 2011, část [7]

Řešení pak organizátoři popsali následovně: „Písmena v prvním řádku přepíšeme do polského kříže, jak napovídá druhý řádek, vezmeme polohu tečky v nich a tu vložíme do připraveného okénka. Výsledný znak převedeme zpět na písmeno. Toto písmeno přeložíme do Braillova písma, z něj použijeme první řádek a přidáme ho k připraveným dvěma řádkům teček na třetím řádku. Výsledek opět přepíšeme zpět na písmena. Získáme písmena A až G. Ta, převedená do semaforové abecedy, mají všechna jeden praporek směrem dolů. Tento praporek ignorujeme a zbylý sloučíme s připravenou druhou polovinou písmene. Převedeme zpět na písmena a získáme pouze písmena ze slova MORSEOVKA. Tato písmena převedeme do morseovky, odstraníme oddělovače a rozdělíme řadu čárek a teček do skupin podle čísel na posledním řádku. Převedením zpět na písmena získáme tajenku POSTUPICKAPARK.

Mnohastupňová šifra 12 se vyvinula z posledního kroku výsledné šifry, ke kterému jsme postupně přidávali další a další patra. Největší problém byl zvolit v každé úrovni co možná nejintuitivnější postup slučování částí kódování. Šifra 12 je navíc nejčastěji opravovanou šifrou ve hře. Naposledy se měnila ještě po vytištění ostatních zadání a bylo ji třeba vytisknout znovu. I přesto v ní zůstala jedna chyba až do hry. Na Dvanáctou šifru bylo vybráno 9 nápověd a 5 řešení.“ [8]

Jiným častým principem je opakování stejné procedury tak dlouhou, až dostaneme řešení šifry. Příkladem je přepisování textu do tabulky, která se mění podle zadaných pravidel, tak dlouho, až dostaneme heslo.

Šifry se specifickým postavením

Šifrovací hra může obsahovat specifickou část, která se liší od ostatního průběhu hry. Typicky se toto uplatňuje na začátku hry, kdy je třeba zařídit, aby všechny týmy nepostupovaly mezi stanovišti ve stejný okamžik, což by způsobilo logistický kolaps (čekání ve frontě na zadání šifry, málo prostoru pro lušticí týmy apod.). Stejně tak na závěr bývají často dány šifry, které využívají předmětů, znalostí a dovedností získaných během hry.

Mezi tyto šifry můžeme zařadit i jakési mezníky ve hře: Například pokud tým byl rozdělen na dvě části a luštil šifry ve dvou oddělených trasách hry, může dojít u určité šifry k opětovnému spojení týmu nad šifrou, kde se využívají informace z obou tras.

Úvodní šifry a aktivity

Úvodní šifry a aktivity se u her s větším počtem účastníků zaměřují na rozptýlení týmů. Mohou to být šifry vyžadující po týmech jistou logistiku (např. části šifry jsou rozmístěny na několika stanovištích v dostatečné vzdálenosti, takže týmům trvá delší čas jejich shromáždění a vyřešení) nebo se jedná o netypickou šifru či aktivitu, kdy týmy mají poznat, co se po nich ve skutečnosti chce. Další variantou je uspořádání jakéhosi turnaje v nějaké hře mezi týmy, kdy je třeba zvítězit v určitém množství zápasů, aby mohl tým postoupit k další šifře. Často není toto rozptýlení organizováno organizátory, postarají se o ně samotné týmy a náhoda.

Příkladem mohou být úvodní aktivity ve hře Bedna:

- 2003 – Organizátoři ukázali obrázek jakéhosi mimozemšťana s velkými parabolickými anténami. Vzhledem k tomu, že na Kavčích Horách, kde byl začátek soutěže, je sídlo České televize s podobnými anténami, bylo třeba hledat zadání první šifry zde – i ta byla těžší, aby týmy rozdělila.
- 2004 – Obíhání lamp veřejného osvětlení a dávání částí šifry dohromady.
- 2005 – Vyškrtávání písmen z řetězce podle daného pravidla – tedy jde spíše o pracovní postup než o myšlenkově náročnou šifru.
- 2006 – Turnaj ve hře HuPo, jejíž plán byl zakreslen na dlažbě a hráči představovali figurky. Tým musel získat dvě vítězství, aby byl odeslán na jednu ze šesti variant další šifry.
- 2007 – Týmy dostaly kostičky a musely je mezi sebou vyměňovat, dokud neměly sedm různých.
- 2008 – Živé scrabble.
- 2009 – Slovní bingo.²
- 2010 – Týmy dostaly písmenko šifry a pak si je vyměňovaly mezi sebou.

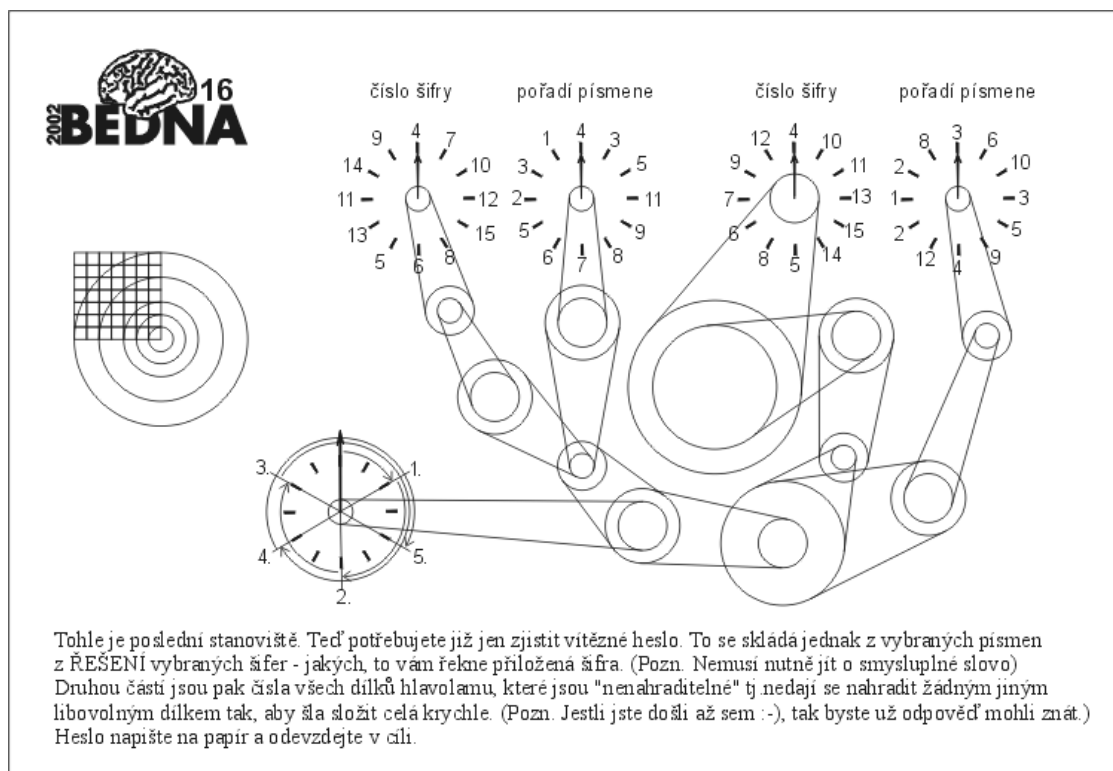
² Více informací na <http://bedna.org/2009/bingo/> (cit. 19. 10. 2014).

- 2011 – Luštění sedmnácti drobných šifer v mapě. Poté byly týmy rozděleny na druhé šifře pomocí tří stanovišť.
- 2012 – Každý tým dostal kostku, na kterou nalepil tečky a pak se utkal ve hře s ostatními týmy.
- 2013 – Týmy si musely vyměňovat písmenka Bednářské abecedy.
- 2014 – Jakýsi AZ-kvíz mezi týmy.

Závěrečné šifry a aktivity

Závěrečné šifry a aktivity mají často specifickou podobu a liší se od ostatních aktivit ve hře. Zde uvedeme několik příkladů:

- Semílací šifra – jedná se o šifru, která využívá hesel šifer luštěných v předchozí hře. Typickým představitelem je šifra 16 ze hry Bedna 2002, viz **Chyba! Nenalezen zdroj odkazů..**
- Využití předmětu získaného ve hře. Příkladem může být hraní pexesa získaného během Želvování 2013 nebo přehrání Ódy na radost na Bedničce při Bedně 2009.
- Jiný typ aktivity nenavazující na předchozí hru. Nemusí jít vůbec o činnost náročnou na přemýšlení nebo luštění, nebo se jich dotýká částečně. Ukázkou tohoto přístupu by pak mohlo být přehrabování se míčky a hledání částí písmen na nich napsaných při hře Želvování 2014. Jiným příkladem bylo rozdělení týmu na dvě části, které si měly předávat šifrované zprávy přes organizátory při hře Krtčí norou 2010.



Obrázek 9: Šifra 16 ze hry Bedna 2009 (<http://www.bedna.org//content/codes/tasks/2002/16.png>, cit. 28. 10. 2014)

Určování typu šifry

Nic jako přesný nástroj na určení typu šifry neexistuje. Přesto můžeme najít pár úvah, které mohou pomoci. Tyto úvahy se nejčastěji provádějí na začátku luštění v průběhu brainstormingu, pokud je luštění prováděno ve skupině. Pokud luštíme samostatně, je dobré provést analýzu šifry.

Při analýze šifry se zaměřujeme na jednotlivé aspekty šifry. Můžeme si pokládat následující otázky:

- Jaký typ šifry připomíná? Jaký první dojem vyvolává?
- Z čeho se šifra skládá? Jsou její části podobné? Které části se nejspíš využijí nejdříve, které později?
- Co se v šifře opakuje? Obsahuje nějakou pravidelnost?
- Jak spolu jednotlivé části šifry souvisí? Navazují na sebe, tvoří určitou posloupnost?
- Jak můžeme aplikovat na šifru pomůcky rozdávané organizátory?
- Kde jsme už něco podobného viděli, ať už v šifrovacích hrách, anebo jinde?
- Souvisí šifra s dobou či místem jejího předání/nalezení? (Tato otázka se vztahuje zejména k terénním šifrovacím hrám.)

Podobné otázky mohou přijít v průběhu luštění šifry, zvláště když zdoláme její dílčí část.

Počítání a šifra

Při analýze šifry můžeme využít jednoduché výpočty, které pomohou určit, zda je v šifře užito určité kódování nebo určitá šifra. Pokud jsou znaky užité v šifře rozděleny do skupin se stálým nebo nepřiliš proměnlivým počtem členů, právě tyto počty ukazují na konkrétní kódování či šifru, viz Tabulka 11: Velikosti skupin a kandidát na šifru. Jedna skupina může být realizována jako uspořádaná n -tice, tabulka či podobné schéma.

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	Přepis skupiny do tabulky (zvláště když počet je roven druhé mocnině)

Tabulka 11: Velikosti skupin a kandidát na šifru

3. Vybavení pro šifrovací hru

Jako na každou rekreační aktivitu i na šifrovací soutěž je třeba se připravit. Vybava a další přípravy pak závisejí na konkrétní šifrovací hře.

Materiální vybava

Vhodná výstroj je velmi důležitá pro úspěšnou účast v šifrovací hře. Některé pomůcky jsou nutné, jiné ulehčují práci.

Zaměříme se nejprve na pomůcky pro Školní šifrovací soutěž. Jsou to především psací a rýsovací pomůcky: Obyčejná tužka či mikrotužka, guma, pastelky, fixy, propisovací tužka, pravítka (dobrá jsou dlouhá i s ryskou), kružítko, nůžky, lepidlo a lepicí páska. Dále pak se hodí kalkulačka, případně rozdané či doporučené šifrovací pomůcky (v průběhu Školní šifrovací soutěže byly rozdány šifrovací pomůcky Chlýftýmu³ a dál se i využívaly).

Každá soutěž má specifické požadavky, jednotlivé ročníky her vyžadují jiný materiál. Proto je vhodné si dobře prostudovat pravidla a pokyny pro soutěžící s dostatečným předstihem.

Psychická vybava

Důležitý je i okamžitý fyzický a psychický stav hráče. Hráč by měl být odpočínutý a vyspaný, aby se mu dobře přemýšlelo. Měl by být i trpělivý, aby neodbočoval od luštění šifry při první překážce (která by mohla jít obejít) nebo prvním neúspěšným pokusu o prolomení šifry.

Žádanou schopností hráče je podílet se na brainstormingu – určování strategie pro luštění šifry v týmu. Vedle znalostí a zkušeností hráče o šifrování se zde projevuje jeho schopnost komunikovat v týmu. A hráči úspěšných týmů musí mezi sebou dobře komunikovat. Podstatou brainstormingu je nahlas vyslovit, co šifra připomíná, kde něco podobného už bylo použito nebo odkud něco známe, z čeho se samotná šifra skládá atd. Právě tato část bývá klíčová pro vyluštění šifry. Hráč by se neměl bát říci nahlas své myšlenky, za neúspěchem často stojí myšlenka „ale to je nesmysl“, „to nejspíš nepůjde“, „to už tam bylo použito“ apod.

Výhodou je i schopnost pobavit ostatní, humor je výborný lék na krizi týmu.

³ Viz <http://chlyftym.cz/web/pomucky> (cit. 28. 10.2014)

4. Školní šifrovací soutěž

Cíle soutěže

Školní šifrovací soutěž probíhá na třeboňském gymnáziu od školního roku 2012–2013.

Cílem soutěže je především představit typy šifer a jejich metody luštění.

Dalším cílem je pak umožnit setkání se šifrovací soutěží, s jejím systémem a průběhem, i se specifiky jednotlivých šifrovacích her.

V neposlední řadě se jedná o aktivitu rozvíjející induktivní a logické myšlení, všeobecný přehled, geometrickou představivost. Rovněž se rozvíjejí i další vlastnosti, jako jsou péle, vytrvalost nebo sebekritika. Přispívá tak k budování lidských postojů soutěžících.

Průběh soutěže

Školní šifrovací soutěž od roku 2013 probíhá ve dvou částech, kontaktní a korespondenční.

Kontaktní část se skládá ze setkání konaných jednou měsíčně. Slouží především k představení jednotlivých typů šifer. Setkání je uvozeno přednáškou, která nejprve představí teoretické a historické zázemí kryptologického tématu, následně poukáže na konkrétní uplatnění v šifrách z různých šifrovacích her. Účastníci si pak mohou vyzkoušet luštění šifer ze zvoleného okruhu.

V korespondenční části je každý měsíc připravována sada pěti šifer. Soutěžící je řeší samostatně. Šifry jsou obtížnější než při setkáních, protože je na ně více času a soutěžící mohou použít i další prostředky (internet). To ostatně umožňuje zadávat více šifer postavených na asociacích či jiných vědomostech.

Na konci školního roku pak se koná setkání s vyhodnocením soutěže.

5. Šifry ze Školní šifrovací soutěže

V této kapitole najdete šifry a jejich řešení z druhého ročníku Školní šifrovací soutěže. Jsou rozděleny podle jednotlivých typů. To je umožněno jejich relativní lehkostí, přesněji jejich obvyklým zaměřením na určitý typ. Ne vždy je však zařazení úplně jednoznačné a závisí na volbě autora. U šifer je vždy poznamenáno původní bodování, které by mělo odrážet obtížnost šifry.

Zadání šifer

Substituční šifry

Šifra 1	Podivuhodná věta	2 body
	Zápisník projasní siláckými pistáciemi chvilku.	
Šifra 2	Přímo morseovka	2 body
	-. / ... / ..- / - / - . / .	
Šifra 3	NKBOANF	2 body
	NKBOANF	
Šifra 4	Caesarův následník	2 body
	ERXSRMYW	
Šifra 5	Webdings	2 body
	 Nepoužívejte diakritiku.	
Šifra 6	Dvojnásobek	3 body
	NJBJBFI	

Šifra 7	Předchůdci a následníci	3 body
----------------	--------------------------------	---------------

LNNAJMBBF

Šifra 8	Závorky	2 body
----------------	----------------	---------------

(ROZ(D(ÚČINEK))UJ)I(TVR((SPOR)DAT)KÁŇ)

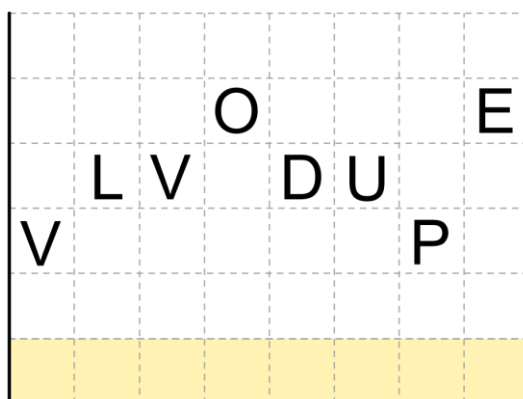
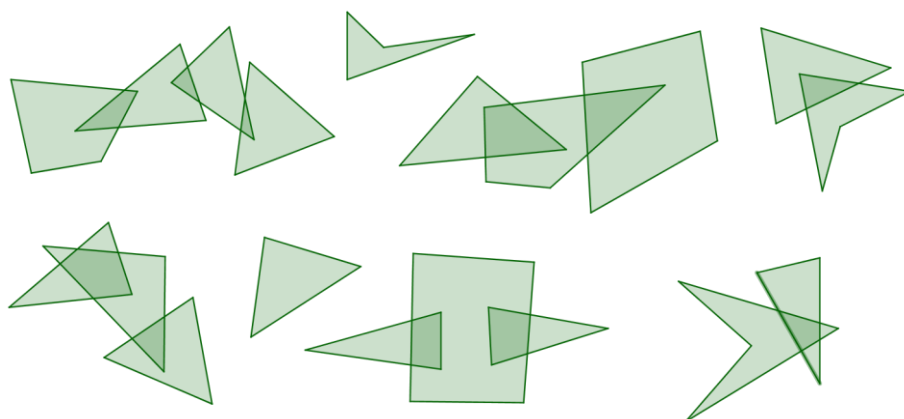
Šifra 9	Úsměv nade vše	2 body
----------------	-----------------------	---------------

Šifra 10	Neznámý posun	3 body
-----------------	----------------------	---------------

JHIPKCXHIXOCDHI

Šifra 11	ČATELO	3 body
-----------------	---------------	---------------

TETETELOTETELOTEČATETELOČATELOČAČAČALOTEČAČATELOTEČATELOČAČ
AČALOTEČAČALOČATETE

Šifra 12 Padající písmena
3 body

Šifra 13 Obrazce
2 body

Šifra 14 Vyplňte test
3 body

Která z čísel jsou lichá?

1 2 3

Jaká nejhorší známka je za chování?

☐ ☐ ☐

Kolik mužů bylo ve člunu podle Jeromeho?

☐ ☐ ☐

Kolik lidí tvoří kapelu Roxette?

☐ ☐ ☐

Kolik bylo Panských válek?

☐ ☐ ☐

Kolik rybníků v ČR je větších než rybník Dvořiště

☐ ☐ ☐
Šifra 15 Podivná chemie
2 body
 N_3 C_2S_1 F_2 H_7N_1 S_4O_1

Šifra 16	Vánoční Playfair	3 body
-----------------	-------------------------	---------------

Následující šifra je tzv. Playfairova. Použito je 25 písmen abecedy bez Q. Náповědou je, že první slovo šifrovaného textu je JEZISEK. Luštění šifry je například popsáno v detektivce Mrtvola nutná Dorothy Sayersové. Její přesný popis najdete třeba na internetu.

EZ JN VJ OK ZP JD CB BR JV UB MZ AJ RM VY SV TV JX IO KM ZM JV UB TF WL
IK GM OI MI TV RI ZJ TD BJ WS BZ GO UJ TP LU EZ GB JC EH BG JV JB DT RB JV
NC YL BZ JV UB

Šifra 17	Jednoduchá substituce	2 body
-----------------	------------------------------	---------------

FQERTVEZ GFLQZMREV GIF EVAJKRIJZ KZJKVER UZCR GFTYRQVAZTZ Q
VMIFGP Q TRJFMVYF FSUFSZ DVQZ MPERCVQVD BEZYKZJBL R BFETVD
GRKERTKVYF JKFCVKZ

Šifra 18	Dopis	2 body
-----------------	--------------	---------------

Vážená kolegyně/vážený kolego, zdravím tě jménem všech – tedy všech kolegyň/kolegů, kteří tento dopis také čtou. Jistě i tvým kolegyním/kolegům připadá divný – a naprosto oprávněně. Je to šifra připravená pro Vaši/jejich potěchu. Jejím cílem je roztočit veškeré mozkové závity na plné obrátky. Tato šifra Vám/vám jistě přinese mnoho zábavy a snad i nějaké poučení. To ostatně bylo cílem při jejím sepisování. Jistě stojí za povšimnutí. Přejeme hodně štěstí, drahá kolegyně/drahý kolego!

Šifra 19	Kolem kuchyně	3 body
-----------------	----------------------	---------------

Polotovár voda prokladano dost tvaroh dort zaprodano

Transpoziční a vybírací šifry

Šifra 1	Přeházená písmena	2 body
----------------	--------------------------	---------------

32145
ÉMJNOKERYJÍJEŽPTÍŘOKJMEEVATLVA

Šifra 2 Vybírání písmen 2 body

OHENSALAPROCJENJETVUJCAJTAKSNADNOSTARY

Nápověda:



☐ ☐ ☐ ☒ ☒ ☒ ☒ ☒

☐ ☐ ☒ ☒

☐ ☐ ☐ ☒ ☒ ☒

Šifra 3 Vyplňte slova bez diakritiky 3 body

MESTO

☐ ☐ ☐ ☐ ☐ ☐ ^C

☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ^{*}

☐ ☐ ☐ ⁺

OSOBA

⁺ ☐ ☐ ☐ ☐ ☐

☐ ☐ ☐ ☐ ☐ ☐ ☐ ^{*}

☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ^C

Šifra 4 Mnohobarevná písmena 3 body

HESLOMASEDMPISMEN

POČÁTKY MĚSTA TŘEBOŇ SAHAJÍ ZHRUBA DO POLOVINY 12 STOLETÍ KDY
NA JEDNÉ Z POHRANIČNÍCH STEZEK VZNIKLA MALÁ TRHOVÁ OSADA S
PANSKÝM DVORCEM

Šifra 5 Čtverce s písmeny 2 body

N	A	J	D	I	H	E	S	L	O
B	T	K	H	S	J	A	X	Y	O

Šifra 6 Prorocství 2 body

MLEEIASVJJAHTVAIMDAPSTASLETOPKVL EEJNTDIPYKATMDZRJEEADTCOEARS
RDEANEARHOUNZEERDEZYT VTHSE

Šifra 7 Sestavte kukátko 3 body

U	S	K	T	H	I	U	Z	E	K	B	O	V	R	Y	H
I	L	R	A	B	C	P	E	H	O	V	C	L	N	E	R
L	S	U	M	V	T	B	S	U	I	A	P	U	R	N	I
V	H	O	P	L	M	N	H	J	T	M	B	S	B	S	O
A	Y	B	V	E	I	H	E	P	O	R	E	A	D	Z	V
1.															

Šifra 8 Divná věta 2 body

Řeholnice mele stvol noční cibuli.

Šifra 9 Přeměna slov 3 body

? + ismus = sloh (3)
 ? + ec = pták (2)
 ? + en = měsíc (2)
 ? + at = šlehat pomlázkou (1)
 ? + íc = číslo (1)
 ? + ě = šlechtic (2)

Nápověda: LÍPA +rna = PALÍRNA

Šifra 10	Prvních pět písmen abecedy	2 body
-----------------	-----------------------------------	---------------

ahakmpftjsejeezrmp
 yjpsivbygyeetfeohr
 agratbobluenmyeytk
 rztpobbbbdpeoicepjc
 anaswbkbtijvkocghc
 hrmrrhfdndeoiceyzk
 auhiaszygtilstfrcv
 poztytdodldzrcsuzc
 aiatnrjziysqicfzic
 zvfshdzmklzdsiljky

Šifra 11	Ryby	2 body
-----------------	-------------	---------------

pstruh lín jeseter štika ostroretka mníkovec paokoun hlavatka

Textové a vyhledávací šifry

Šifra 1	Verše	2 body
----------------	--------------	---------------

Štěstí! Co je štěstí? Muška jenom zlatá, která za večera kol tvé hlavy chvátá; oblétá ti skráně, v kadeři se kryje, v dlaně hlavu skládáš, ruka utlačí je.	Štěstí jako rosa na květech se skvěje, ale bludná noha náhle zašlápne je; zašlápnuto vzdechne,
---	--

Šifra 2	Čtvrtá žena	2 body
----------------	--------------------	---------------

Luisa	3. 4. 1812	11. 10. 1850
Marie	23. 8. 1836	19. 9. 1902
Alžběta	2. 10. 1900	23. 11. 1965
???	17. 11. 1905	29. 8. 1935

Šifra 3	Text klasika	3 body
----------------	---------------------	---------------

Zdalo se mu, že letí přinejmenším rychlostí světla; nějak se mu svíralo srdce, ale to dělá jen Fitzgerald-Lorentzovo zploštění, řekl si; musím být placatý jako lívanec. A najednou se proti němu vyježí nesmírné skleněné hranoly; ne, jsou to jenom nekonečné hladce vybroušené roviny, jež se protínají a

prostupují v břitkých úhlech jako krystalografické modely; a proti jedné hraně je hnán úžasnou rychlostí. “Pozor,” zařval sám na sebe, neboť v tisícíně vteřiny se musí roztříštit; ale tu již bleskově odletěl zpět a rovnou proti hrotu jehlanu; odrazil se jako paprsek a byl na skleněně hladkou stěnu, smeká se podle ní, sviští do ostrého úhlu, kmitá šíleně mezi jeho stěnami, je hozen pozpátku nevěda proti čemu, zas odmrštěn dopadá bradou na ostrou hranu, v poslední chvíli ho to odhodí vzhůru; nyní si roztřískne hlavu o euklidovskou rovinu nekonečna, ale již se řítí střemhlav dolů, dolů do tmy; prudký náraz, bolestné cuknutí v celém těle, ale hned zas se zvedl a dal se na útěk. Uhání labyrintickou chodbou a za sebou slyší dupot pronásledovatelů; chodba se úží, svírá se, její stěny se přirážejí k sobě děsným a neodvratným pohybem; i dělá se tenký jako šídlo, zatajuje dech a upaluje v bláznivé hrůze, aby tudy proběhl, než ho ty stěny. Zavřelo se to za ním s kamenným, zatímco sám svistí do propasti podle ledově čišící zdi. Strašný úder, a ztrácí vědomí; když procitl, vidí, že je v černé tmě; hmatá po slizkých kamenných stěnách a křičí o pomoc, ale z jeho úst nevychází zvuku; taková je tu tma. Jektaje hrůzou klopýtá po dně propasti; nahmatá postranní chodbu, i vrhá se do ní; jsou to vlastně schody, a nahoře, nekonečně daleko svítá malinký otvor jako v šachtě; běží tedy nahoru po nesčíslných a strašně příkrých stupních; nahoře není než plošinka, lehoučká plechová platforma drnčící a chvějící se nad závratnou hlubinou, a dolů se šroubem točí jen nekonečné schůdky ze železných plátů. A tu již za sebou slyšel supění pronásledovatelů. Bez sebe hrůzou se řítí a točil po schůdkách dolů, a za ním železně řinčí a rachotí dupající zástup nepřátel. A najednou vinuté schody se končí ostře v prázdnu.

Šifra 4 Kontakt

2 body

...ná?iu...
 ...Na S?de...
 ...ře?oň...
 ...ís?o ú...
 ...dr?sa...
 ...si?te...
 ...tel?a š...

Šifra 5 Čeští pěvci

2 body

vblastrnmargitpeckovaaadchutosykopenkralicdestinokosvaekiceralietuhbeh
 akennackovaykra

Šifra 6	Zaklínání čarodějnic	2 body
	do kotle vhod listi vlahe svar je s jedem v pachy nahe prihod to co vteklo v ceslo co se v tlame mloka neslo zdibec slizu hranostaje ocas stira co hlen saje z obesence jedno stehno prst starce co ztratil leno ze zraloka bile maso z vlasu polednice laso proved varem v kлокot skoro jen se zvedni ze dna paro prihod v ohen smolny prazec at vyvstane tlustokožec	

Asociační šifry

Šifra 1	Vyber písmena ze slov	2 body
	NAJIT OBJEVIT ODHALIT UKRAST VYNALEZT LOUCE LUCERNA MAJAK SVETLUSKA ZAROVKA KALHOTY KILT KRATASY NAHRDELNIK PLAVKY FRANK LIBRA TOLAR TOPAS YEN KONGO NIL PANDA SAHARA SURIKATA BERLIN DECIN CHEB PLZEN TREBON	

Šifra 2	Věty...	3 body
	Samý řev, ten černej pták neztichne... Je třeba vymýtit tu invazivní dřevinu, listí nekompostujte! Vyskakuje si, jak čertík ze škatulky. Zkontrolujte stav střechy – a nejen tašek! Ve stříbrném štítě s modrou vlnkovitou patou snížené modré vlnkovité břevno. Malá vstupenka do kina.	

Šifra 3	Prostředník	2 body
	rybí – 2 – dlouhé přivřu – 1 – na punčoše houby – 3 – židle průvodu – 4 – postele rodiny – 4 – v písku černá – 3 – zákona tahá za – 3 – dlouhé	

Šifra 4 Kroužky a čtverečky 2 body

Dukát	●	Terč	Rotunda
Pyramida	●		
Křída	●	Srnčí hřbet	
Válec	●	Tisícikoruna	Fix
Bábovka	●	Globus	
Brána	●	Hranol	Krabice
Atlas	●		
Sud	●		

Šifra 5 Doprava třikrát jinak 3 body

Kanoe, člun, koráb, tank, balón, auto, koloběžka, kolo, dvouplošník, surf, tramvaj, letadlová loď, parník, tryskáč, trajekt, autobus, helikoptéra, skateboard, kajak, rogalo, moped

Šifra 6 Skládačka 3 body

pravý	zábavný	sváteční	chlapeč	tichý	černý	zelený	škodlivý	nudný
lhostejný	originální	zralý	červín	užitečný	nízký	vágní	nový	horký
vysoký	vřelý	zdravý	dlouhý	starý	přesný	opsaný	drobný	včasný
velký	hlasitý	falešný						

Střed je žlutý.

Šifra 7	Povedená dcerunka	2 body
----------------	--------------------------	---------------

Paní doktorko, já nevím, co mám s tou holkou dělat. Pořád někde lítá, jen se otočím, už je pryč a běhá kdovíkyde. Tuhle si předcházela tomu mladýmu astronomovi, chodila celá v černém, on jí chtěl prý tajemnou a temnou. A ten románek s chemikem – ten byl hodně výbušný. Chlapíka ze železářství si přitáhla jak magnetem. Všichni elektrikáři z okolí se o ní perou.

A jak ta je na sladké! Jakmile jen vytáhnu čokoládu a kousnu do ní, hned je v pokoji a vyčítá mi, že jí všechno sním. Ale kdybych uvařila něco dietního, k obědu ji nedostanu.

Šifra 8	Poslouchej	2 body
----------------	-------------------	---------------

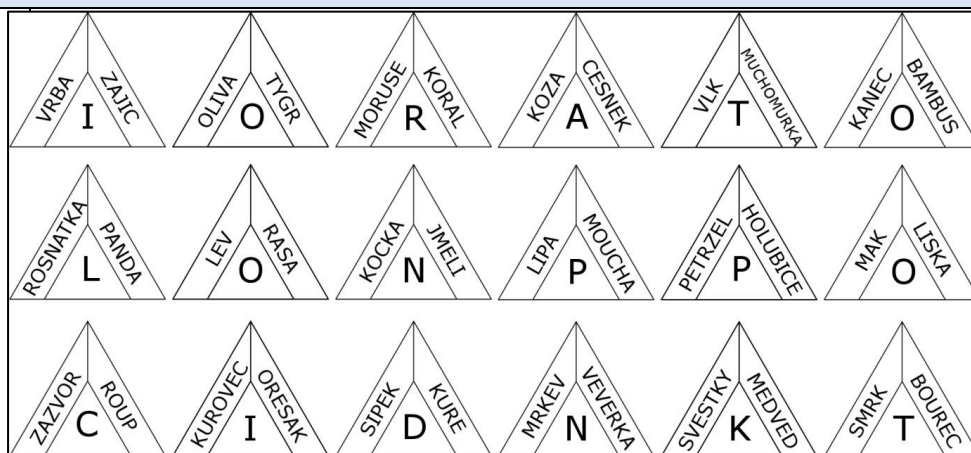
<http://youtu.be/U3kP-KbFafQ> 1:23
<http://youtu.be/AfRikVOCFqA> 0:43
<http://youtu.be/MajhxpqDMEg> 2:01

→ první odkaz 1:31

Šifra 9	Pro rádia	2 body
----------------	------------------	---------------

Včelka 1
 Vlk 3
 Štolverk 2
 Bota 3
 Dlaždič 4
 Žádost na byt 7
 Řípa 4

Šifra 10	Skládačka 2	3 body
-----------------	--------------------	---------------



Šifra 11	Skrumáž	2 body
-----------------	----------------	---------------

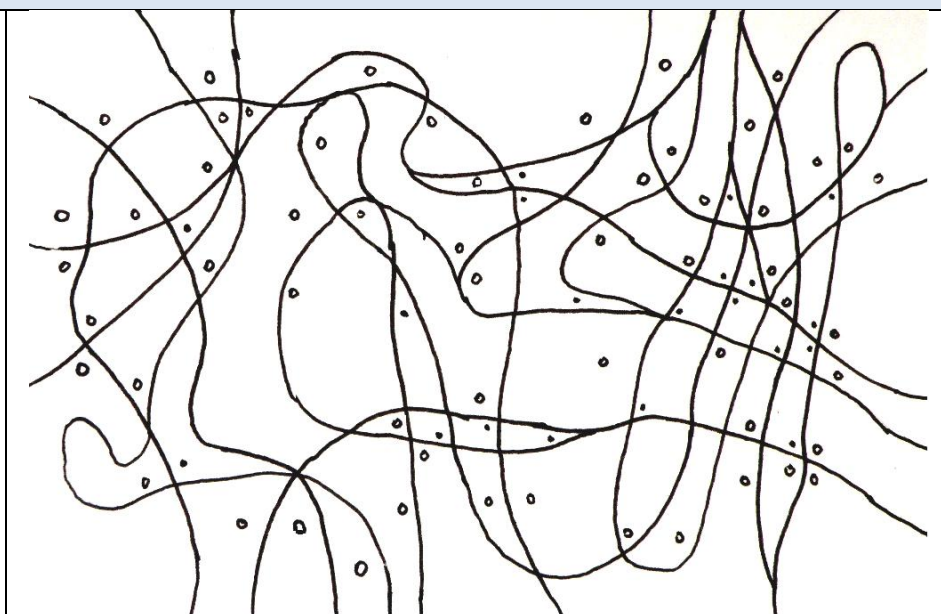
lezata osmicka – nekonečna stanice – biorytmy / magneticke pole – rubikon
 – inzerat / jestrab – má prava láska – vzdalene ostrovy / nebudeme –
 rytmus – vyskrabu ti oči / ulice – brejle – zelva / usi – rybi tuk – hollywood /
 jeste jednou – slavná vec – kolektivní vina

Šifra 12	Předmět zájmu	3 body
-----------------	----------------------	---------------

alsinula 4
 lumen 6
 meridianus 3
 oppugnator 5
 trianguli 2

Grafické šifry

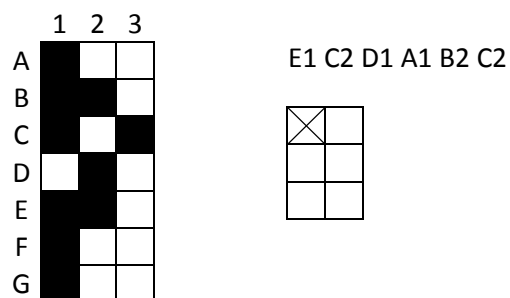
Šifra 1	Čáry máry	3 body
----------------	------------------	---------------



Šifra 2	Dva křížky a heslo	3 body
----------------	---------------------------	---------------

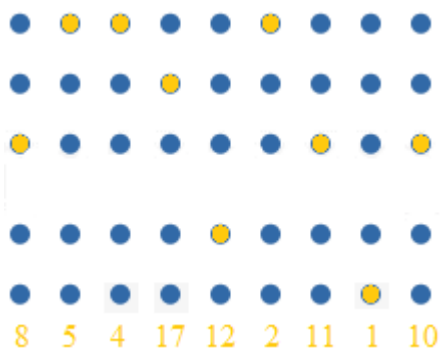


Šifra 3	Souřadnice černobíle	3 body
----------------	-----------------------------	---------------

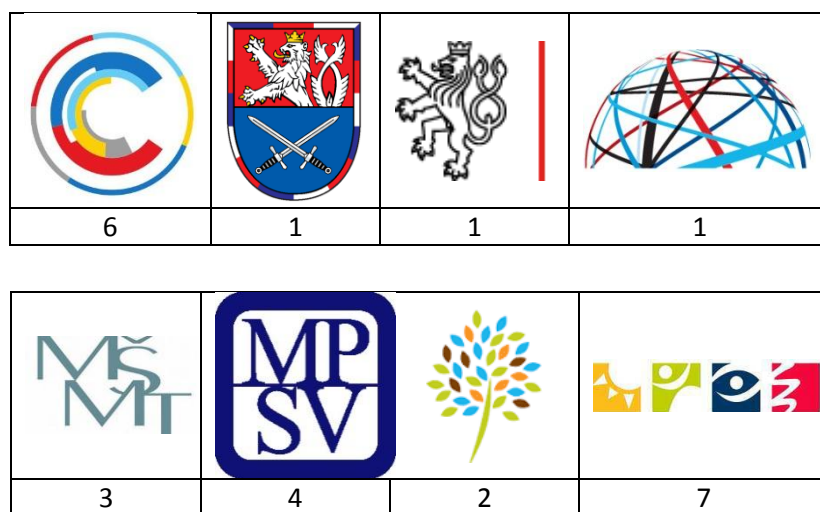


Šifra 4	Pět bodů	3 body
----------------	-----------------	---------------

Školní šifrovací soutěž 2013-2014



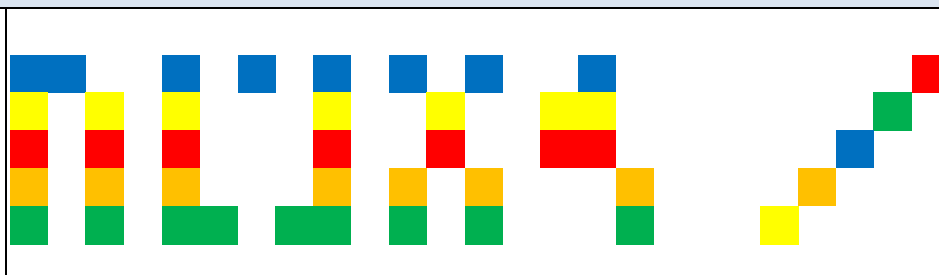
Šifra 5	Logo - číslo - písmeno	2 body
----------------	-------------------------------	---------------



Šifra 6	Kočka na louce	2 body
---------	----------------	--------

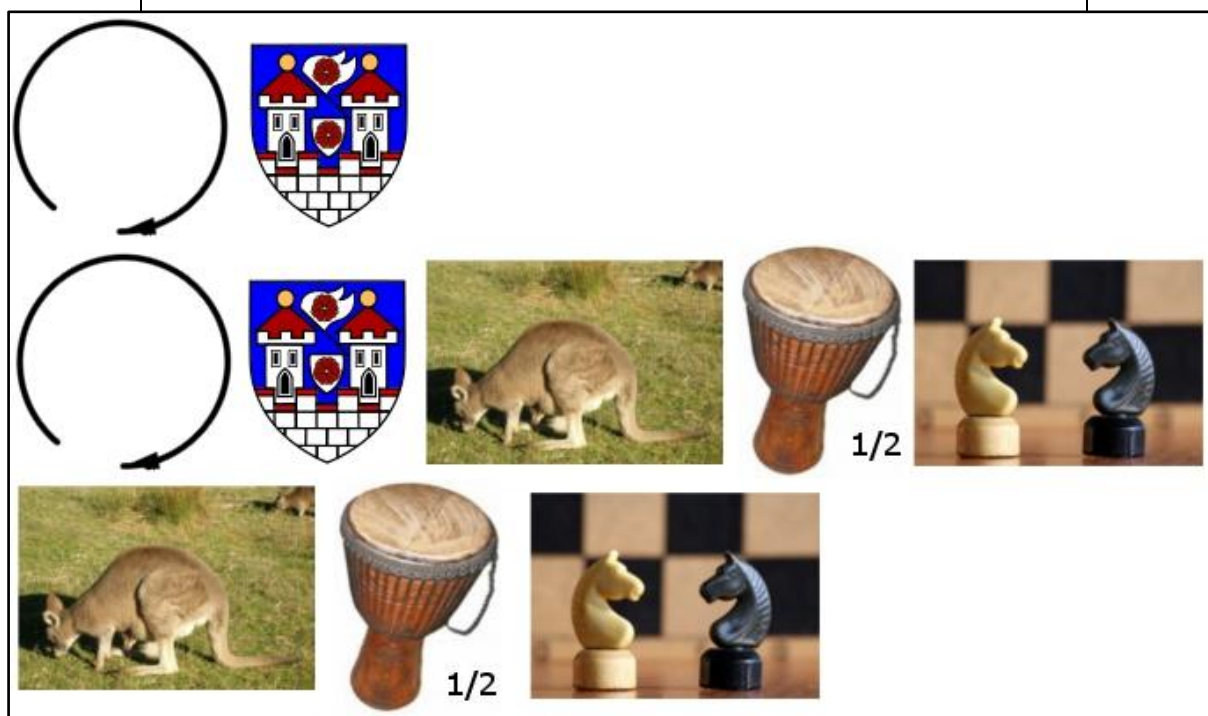


Šifra 7	Chybí nárys	2 body
---------	-------------	--------



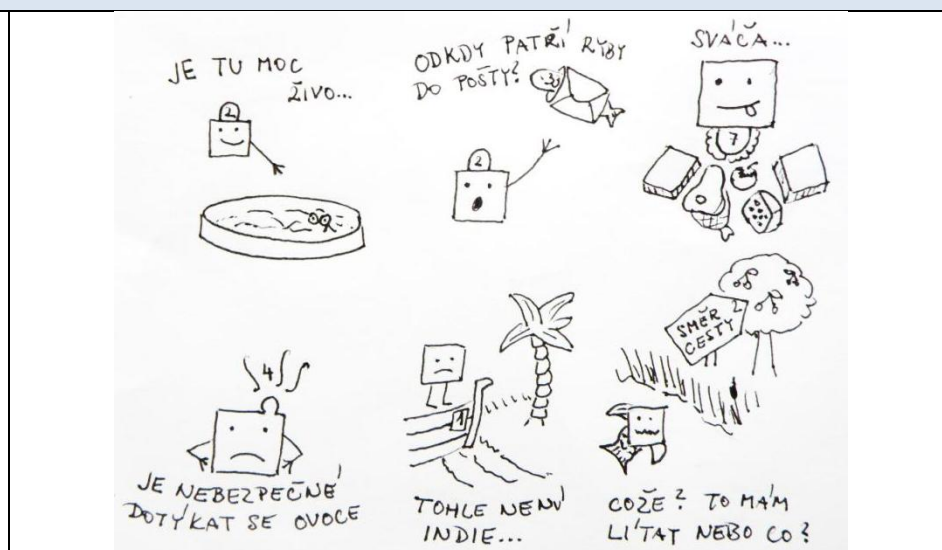
Šifra 10 Najdi obilí

3 body



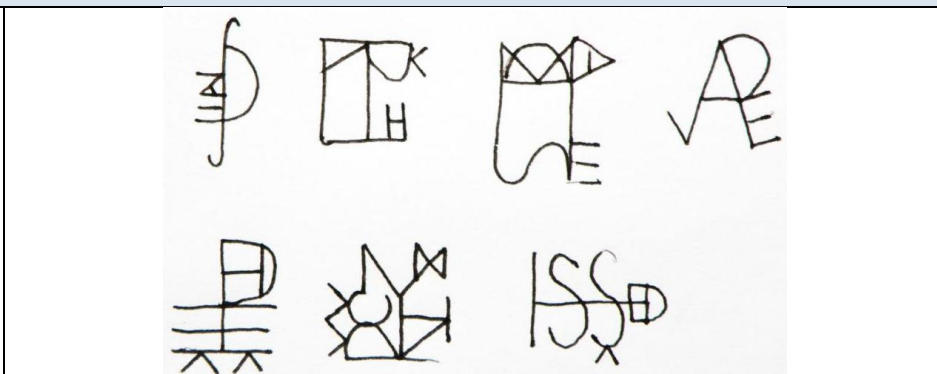
Šifra 11 Osobnostní komiks

3 body



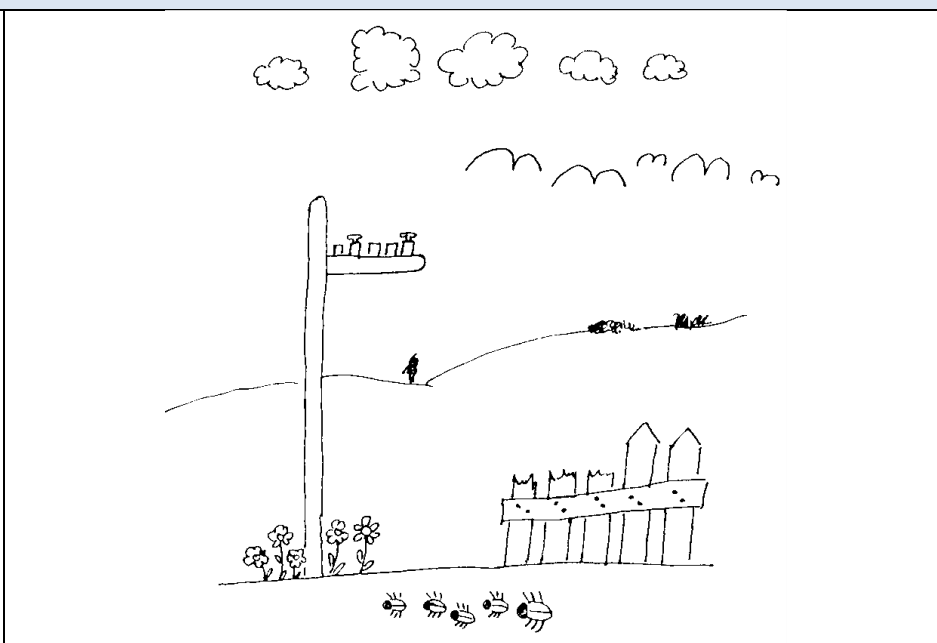
Šifra 12 Cizokrajné znaky

2 body



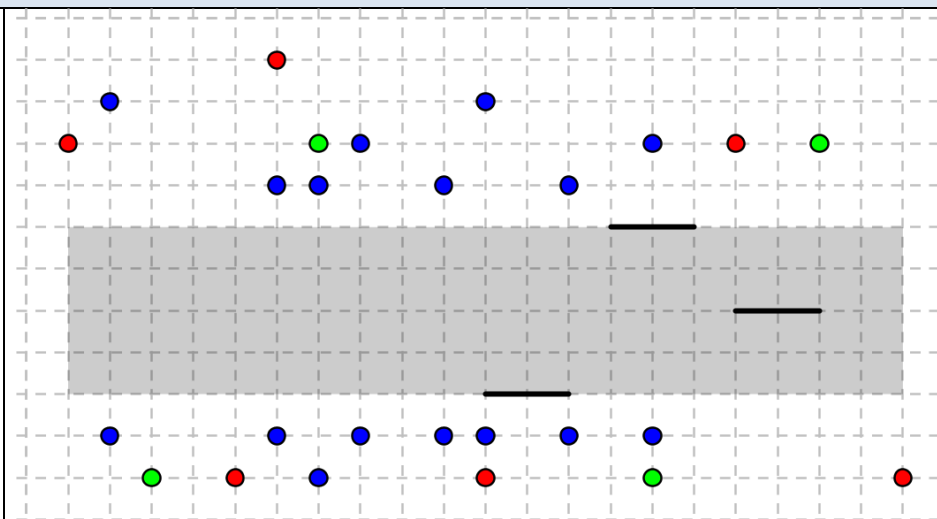
Šifra 13 Obrázek z venkova

2 body



Šifra 14 Barvy - body - úsečky

3 body



Šifry využívající schémata

Šifra 1

Ve čtverci

3 body

	a		3				w
			l			k	
j		t	i		k		5
					v		
1		r		o			2
			n	a			m
	e		4		q	r	
	z		l				

Šifra 2

Osmisměrka

3 body

B	R	R	K
Z	O	O	A
I	S	L	P
L	Y	Z	U
F	N	R	M
A	S	Y	A

ARY, FY, MY, PUMA, ROSY, SOK, ZOO

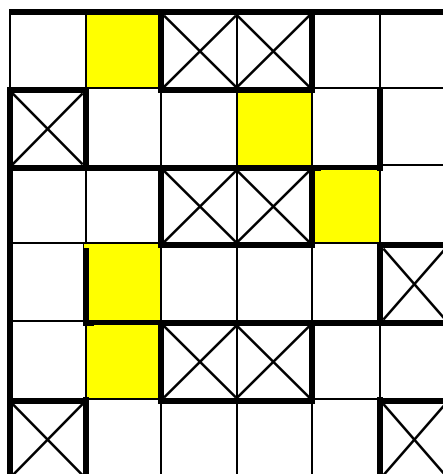
Šifra 3

Mříž – rozděl a překryj

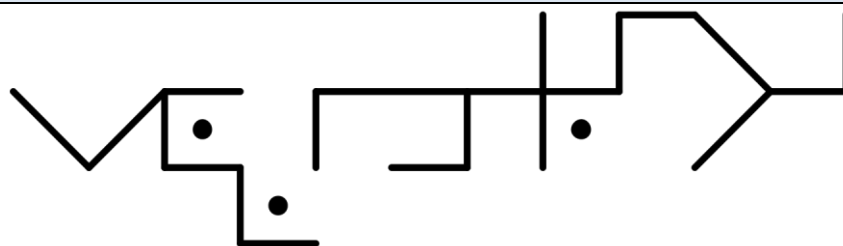
2 body

[illegible]

Šifra 4	Labyrint	2 body
----------------	-----------------	---------------



Šifra 5	Graffiti	3 body
----------------	-----------------	---------------



Šifra 6	Astromřížka	3 body
----------------	--------------------	---------------

Otáčíme po směru hodinových ručiček



Šifra 7

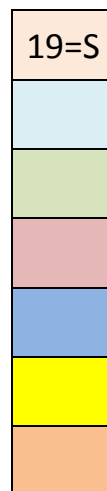
Sudoku

3 body

				7	5	4	3	
9					4			
		8		9	6			2
				6		5	2	1
		7		8		6		
1	6	4		5				
8			5	1		7		
			7					4
	2	1	6	4				

Heslo:

19=S



Šifra 8

Křížovka s obrázky

3 body



1



2



3



4



5



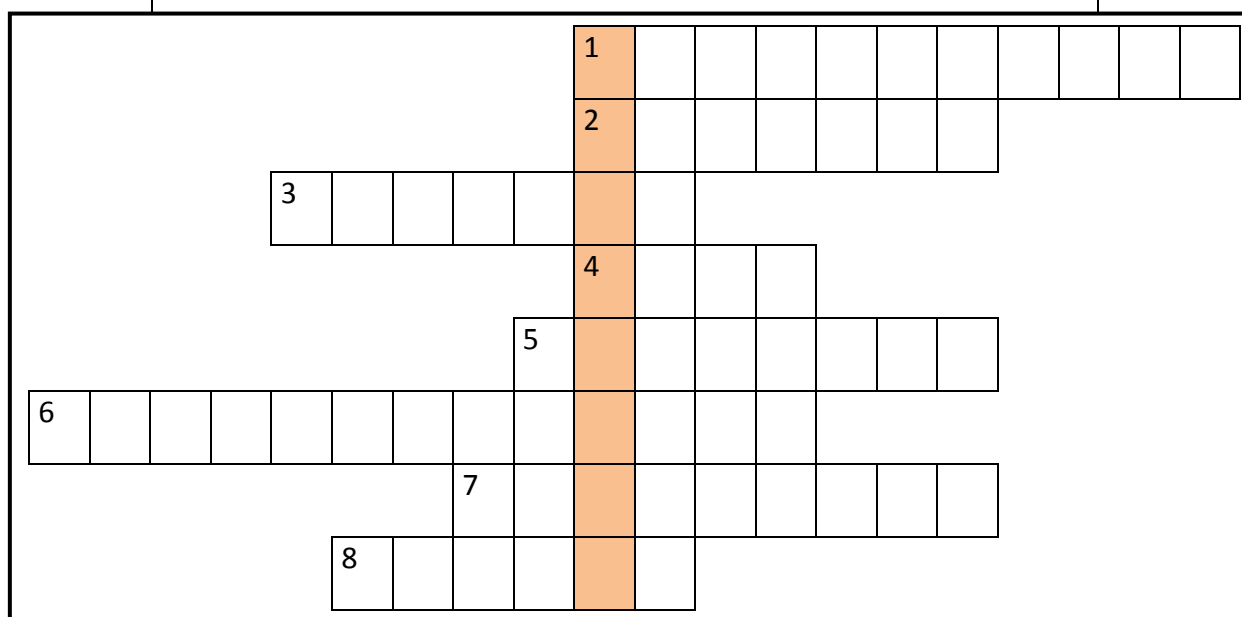
6



7



8



Šifra 12 Šachová smršť 3 body

on tahnul na b4 ona na e7 on nato c2 a pak jeste f5
proste konec ona tahla na h4 mat

Šifra 13 Transpozice čtverce 2 body

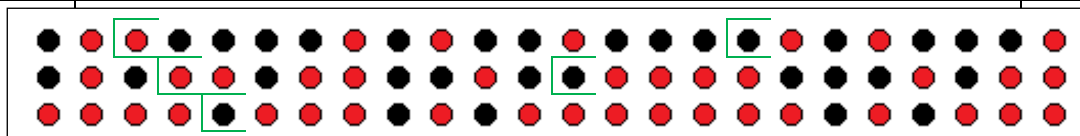
J	V	H	H	L	A
U	P	I	M	Ě	S
E	T	E	E	M	Ě
O	R	O	V	N	Í
C	O	D	T	O	Z
I	D	E	S	N	E

Víceúrovňové šifry

Šifra 1 Brail a pak morseovka 2 body

EFIEBISU

Šifra 2 Ber šest a pak pět 3 body



Šifra 3 Obrazová galerie 2 body



Šifra 4	Vlajky a kříž	2 body
---------	---------------	--------

				
		Ch J O	Q X Y	
•	•	•	•	•
•	•	•	•	•
•	•			

Substituční šifry

Šifra 1

Podivuhodná věta

2 body

Pokud přečteme čárky a tečky nad písmeny, dostaneme -./-./---./-./., což je KAPLE.

Šifra 2

Přímo morseovka

2 body

Třetí znak nic neznamená, je třeba morseovku přepsat. Hledaná změna je záměna teček a čárek, dostaneme tak ROZERT, což je pozpátku TREZOR.

Šifra 3

NKBOANF

3 body

Přepíšeme text do morseovky: -./-./---./-./...
Pozpátku dostaneme -../-./-./---/...-./-./., což je LANOVKA.

Šifra 4

Caesarův následník

2 body

Jedná se o posun o 4 písmena. Pokud provedeme zpětný posun, dostaneme ANTONIUS.

Šifra 5

Webdings

2 body

Symbody představují medaile – talir – fotoaparát – radio. První dvě písmena (první slabiky) dávají METAFORA.

Šifra 6

Dvojnásobek

3 body

Vypišme si tabulku pořadí písmen. Pak pořadí zdvojnásobme (popřípadě odečtěme 26):

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
2	4	6	8	10	12	14	16	18	20	22	24	26	2	4	6	8	10	12	14	16	18	20	22	24	26
B	D	F	H	J	L	N	P	R	T	V	X	Z	B	D	F	H	J	L	N	P	R	T	V	X	Z

Vypišme si, která písmena, se mohou zobrazit na písmena šifrovaného textu:

$N \leftarrow G, T$
 $J \leftarrow E, R$
 $B \leftarrow A, N$
 $J \leftarrow E, R$
 $J \leftarrow E, R$
 $B \leftarrow A, N$
 $F \leftarrow C, P$
 $J \leftarrow E, R$

Nyní z možných písmen vybereme písmena hesla. Heslo je GENERACE.

Šifra 7 Předchůdci a následníci

3 body

Napišme si předcházející a následující písmena:

K	M	M	Z	I	L	A	A	E
L	N	N	A	J	M	B	B	F
M	O	O	B	K	N	C	C	G

Střídavě vybíráme předchozí a následující písmena a dostaneme heslo KOMBINACE.

Šifra 8 Závorky

2 body

Postupně nahrazujeme výrazy v závorkách za synonyma a odstraňujeme závorky:

(ROZ(DEFEKT)UJ)I(TVR(PŘEDAT)KÁŇ)

(ROZKAZUJ)I(TVRDÁTKÁŇ)

VELIKOST

Heslem je VELIKOST.

Šifra 9 Úsměv nade vše

2 body

Jedná se o binární abecedu, černé smajlíky značí 1, bílé 0. Dostaneme tak heslo HROBNIK.

Šifra 10 Úsměv nade vše

2 body

Stačí písmena šifry posunout o 11 písmen a dostaneme heslo USTAVNI STIZNOST. Velikost posunu snadno určíme například pomocí stránek Michala Musíla (<http://www.musilek.eu/michal/sifry-jz-heslo.html?menu=cc&item=d&lang=cz>) nebo jakýchkoli jiných obdobných...

Šifra 11 ČATELO 3 body

Jedná se o morseovku. ČA znamená čárku, TE tečku a LO lomítko čili oddělovač:

.../../-./-./---/.../../-./---/../-/..
Heslem je SILNOPROUD.

Šifra 12 Padající písmena 3 body

Jak písmena padají, mění se, zmenšuje se jejich pořadí v abecedě. Např. protože V v prvním sloupci padá o 2 čtverce, změní se na T (T-U-V). Heslo vyjde TISKARNA.

Šifra 13 Obrazce 2 body

Máme zde skupiny dvou typů mnohoúhelníků, trojúhelníků a čtyřúhelníků. Jedná se o morseovku, trojúhelníky představují čárku, čtyřúhelníky tečku. Znaky čteme po řádcích. Vyjde slovo JEDNOTKA.

Šifra 14 Vyplňte test 3 body

Po vyplnění testu dostaneme bílá a černá kolečka. Pokud je rozdělíme do tří šestic, dostaneme znaky Braillova písma, které znamenají MEC.

1	2	3
●	○	●
○	○	●
○	○	●
○	●	○
○	○	●
○	○	●

Šifra 15 Podivná chemie 2 body

Pokud písmena „posuneme dozadu“ o udaný počet písmen (tedy bereme písmena, která jsou o udaný počet míst před nimi v abecedě), dostaneme heslo KARDAMON.

Šifra 16 Vánoční Playfair 3 body

Jak se přijde na řešení? Různě. Do začátku máte informaci, že
JE<->EZ, ZI<->JN, SE<->VJ, K?<->OK

Zbytek je na vás. Nakonec vyjde říkanka:

JEZISEK TU NECHAL HESLO

NEJSPIS SE MU SPATNE NESLO

KDYZ NAD PAPIREM PRELETAL
 VYKLOUZLO MU Z JEHO SAL
 DO HESLA TEHLE SIFRY KLESLO
 Heslem (šifry i Playfairovy) je slovo JEZULATKO. Použitá tabulka pro převod písmen je následující:

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

Šifra 17 Jednoduchá substituce

2 body

Jedná se o posun písmen o -9 (nebo o +17):

OZNACENI POUZIVANE PRO NEJSTARSI TISTENA DILA POCHAZEJICI Z EVROPY
 Z CASOVEHO OBDOBI MEZI VYNALEZEM KNIHTISKU A KONCEM
 PATNACTEHO STOLETI

Jde o úryvek z Wikipedie vysvětlující pojem INKUNÁBULE čili PRVOTISK (za řešení se uznává kterékoliv z obou slov).

Šifra 18 Dopis

2 body

V textu je výrazná interpunkce. Stačí vzít lomítka, pomlčky a tečky a dostaneme /-./-./-./.../, což je TENIS.

Šifra 19 Kolem kuchyně

3 body

Jedná se o morseovku: Souhlásky vynecháme, o kódují tečky, a čárky. Heslo je VAPENEC.

Transpoziční a výběrací šifry

Šifra 1 Přeházená písmena

2 body

Písmena jsou přeházená podle pořadí 32145. Tedy rozdělíme řetězec znaků do pětic a přerovnáme písmena podle návodu:

ÉMJNO KEŘYJ ÍJEŽP TÍŘOK JMEEV ATLVA

JMÉNO ŘEKYJ EJÍŽP ŘÍTOK EMJEV LTAVA

Heslem je jméno řeky, do které se vlévá Vltava – to je LABE.

Šifra 2 Vybírání písmen

2 body

Nápovědou je slovo prvočísla (prvosenska Čína slámák). Vybereme tedy z textu písmena na prvočíselných místech (druhé, třetí, páté, sedmé, jedenácté...) Vyjde HESLO JE VANDR.

Šifra 3 Vybírání písmen

3 body

Písmeno C připomíná půlměsíc, + kříž, * šesticípou hvězdu – jedná se o symboly islámu, křesťanství a judaismu. Stačí tak vyplnit důležité město a osobnost spojenou s náboženstvími do políček, označené písmeno vybereme do hesla. Heslo je KAMERA.

MESTO	C M E K K A	* J E R U Z A L E M	+ R I M
OSOBA	+ J E Z I S	* A B R A H A M	C M O H A M E D

Šifra 4 Mnohobarevná písmena

3 body

Vybíráme postupně sedm písmen, a to podle barvy – jsou srovnány podle barev duhy, od fialové po červenou (barev je sedm!, každá odpovídá jednomu písmenu hesla). Nejprve najdeme první fialové písmeno (R), pak hledáme dál první tmavě modré písmeno (A) atd. Vyjde heslo RADNICE.

HESLO M A S E D M P Í S M E N

POČÁTKY MĚSTA TŘEBOŇ SAHAJÍ ZHRUBA DO POLOVINY 12 STOLETÍ KDY
NA JEDNÉ Z POHRANIČNÍCH STEZEK VZNIKLA MALÁ TRHOVÁ OSADA S
PANSKÝM DVORCEM

Šifra 5	Čtverce s písmeny	2 body
	Pokud čtverce přerovnáme tak, aby horní písmena byla srovnána v abecedním pořadí, dolní písmena dají heslo THAJSKYBOX.	
Šifra 6	Proroctví	2 body
	MLEEIASVJJAHTVAIMDAPSTASLETOPKVL EEJNTDIPYKATMDZRJEEADTCOEARS RDEANEARHOUNZEERDEZYT VTHSE	
Šifra 7	Sestavte kukátko	3 body
	Pokud přehneme tabulku podle vodorovné čárkované čáry a pak podle svislých čárkovaných čar, poté prostříhneme vyznačená políčka, dostaneme jakési kukátko, jehož otvory (pokud jej otáčíme podle návodných čísel) uvidíme písmena hesla JAK SE VAM LIBI.	
Šifra 8	Divná věta	2 body
	První a poslední písmena slov dávají ŘEMESLNÍCI.	
Šifra 9	Přeměna slov	3 body
	Je třeba najít jména stromů, která doplní jednotlivé přeměny: BUK, VRBA, DUB, SMRK, TIS, HABR Z nich pak vybereme označená písmena a dostaneme heslo KRUSTA.	

Šifra 10 Prvních pět písmen abecedy 2 body

Je třeba si vyznačit výskyt písmen a, b, c, d, e v textu. Rozmístění každého písmene vykresluje jedno písmeno hesla BANAN.

a	h	a	k	m	p	f	t	j	s	e	j	e	e	z	r	m	p
y	j	p	s	i	v	b	y	g	y	e	e	t	f	e	o	h	r
a	g	r	a	t	b	o	b	l	u	e	n	m	y	e	y	t	k
r	z	t	p	o	b	b	b	d	p	e	o	i	c	e	p	j	c
a	n	a	s	w	b	k	b	t	i	j	v	k	o	c	g	h	c
h	r	m	r	r	h	f	d	n	d	e	o	i	c	e	y	z	k
a	u	h	i	a	s	z	y	g	t	i	l	s	t	f	r	c	v
p	o	z	t	y	t	d	o	d	l	d	z	r	c	s	u	z	c
a	i	a	t	n	r	j	z	i	y	s	q	i	c	f	z	i	c
z	v	f	s	h	d	z	m	k	z	l	d	s	i	l	j	k	y

Šifra 11 Ryby 2 body

Vybereme z prvního slova první písmeno, ze druhého druhé písmeno atd.
 pstruh lín jeseter štika ostroretka mníkovec paokoun hlavatka
 Dostaneme heslo PÍSKOVNA.

Textové a vyhledávací šifry

Šifra 1 Verše 2 body

Zadáním je báseň Adolfa Heyduka Štěstí! Co je štěstí? V ní jsou některá písmena vyznačena kurzívou a jiným typem písma – tvoří heslo ZRADCE.

Šifra 2 Čtvrtá žena 2 body

Jedná se o první čtyři belgické královny, tou čtvrtou byla Astrid Švédská.
 Heslo je ASTRID.

Šifra 3 Text klasika 3 body

Zdroj textu snadno zjistíme zadáním např. první věty do vyhledávače.
 V ukázce z románu Krakatit Karla Čapka chybí některá slova. Stačí zjistit která a vzít jejich první písmena, dostaneme heslo TOVARNA. (Krakatit lze volně stáhnout např. na stránkách Městské knihovny v Praze
<http://www.mlp.cz/cz/projekty/on-line-projekty/karel-capek/>).

Zdalo se mu, že letí přinejmenším rychlostí světla; nějak se mu svíralo srdce, ale to dělá jen Fitzgerald-Lorentzovo zploštění, řekl si; musím být placatý jako lívanec. A najednou se proti němu vyježí nesmírné skleněné hranoly; ne, jsou to jenom nekonečné hladce vybroušené roviny, jež se protínají a prostupují v břitkých úhlech jako krystalografické modely; a proti jedné **takové** hraně je hnán úžasnou rychlostí. "Pozor," zařval sám na sebe, neboť v tisícíně vteřiny se musí roztříštit; ale tu již bleskově odletěl zpět a rovnou proti hrotu **obrovského** jehlanu; odrazil se jako paprsek a byl **vržen** na skleněnou hladkou stěnu, smeká se podle ní, sviští do ostrého úhlu, kmitá šíleně mezi jeho stěnami, je hozen pozpátku nevěda proti čemu, zas odmrštěn dopadá bradou na ostrou hranu, **ale** v poslední chvíli ho to odhodí vzhůru; nyní si roztřískne hlavu o euklidovskou rovinu nekonečna, ale již se řítí střemhlav dolů, dolů do tmy; prudký náraz, bolestné cuknutí v celém těle, ale hned zas se zvedl a dal se na útěk. Uhání labyrintickou chodbou a za sebou slyší dupot pronásledovatelů; chodba se úží, svírá se, její stěny se přirážejí k sobě děsným a neodvratným pohybem; i dělá se tenký jako šídlo, zatajuje dech a upaluje v bláznivé hrůze, aby tudy proběhl, než ho ty stěny **rozdrtí**. Zavřelo se to za ním s kamenným **nárazem**, zatímco sám svistí do propasti podle ledově čišící zdi. Strašný úder, a ztrácí vědomí; když procitl, vidí, že je v černé tmě; hmatá po slizkých kamenných stěnách a křičí o pomoc, ale z jeho úst nevychází zvuku; taková je tu tma. Jektaje hrůzou klopýtá po dně propasti; nahmatá postranní chodbu, i vrhá se do ní; jsou to vlastně schody, a nahoře, nekonečně daleko svítá malinký otvor jako v šachtě; běží tedy nahoru po nesčíslných a strašně příkrých stupních; **ale** nahoře není než plošina, lehoučká plechová platforma drnčící a chvějící se nad závratnou hlubinou, a dolů se šroubem točí jen nekonečné schůdky ze železných plátů. A tu již za sebou slyšel supění pronásledovatelů. Bez sebe hrůzou se řtil a točil po schůdkách dolů, a za ním železně řinčí a rachotí dupající zástup nepřátel. A najednou vinuté schody se končí ostře v prázdnu.

Šifra 4	Kontakt	2 body
----------------	----------------	---------------

Jedná se o části slov ze stránky kontaktů gymnázia
<http://www.gymtrebon.cz/c-6-kontakt.html>:
 Gymnázium, Na **Sadech**, Tře**boň**, číslo účtu, ad**re**sa, asistentka, ředitel**ka**
 školy. Řešením je ZABLESK.

Šifra 5	Čeští pěvci	2 body
----------------	--------------------	---------------

Je třeba postupně vyškrtávat jména operních pěvců a pěvků a jména pěvců – ptáků:
 peckova, margita, kos, haken, destinova, strnad, blachut, kralicek,
 benackova, penice, sykora, tuhyk
 Nakonec zbyde slovo VOLIERA.

Šifra 6	Zaklínání čarodějnic	2 body
----------------	-----------------------------	---------------

Vzývání volně inspirované macbethovskými čarodějnicemi. Stačí vzít rýmy: he-slo-je-no-so-ro-zec. Tedy heslo je NOSOROŽEC.

Asociační šifry

Šifra 1	Vyber písmena ze slov	2 body
----------------	------------------------------	---------------

V každém z řádků jedno ze slov nepatří mezi ostatní (ukrást, světluška, náhrdelník, topas, panda, Berlín). Z něj vybereme tučné písmeno a dostaneme heslo KANAPE.

Šifra 2	Věty...	3 body
----------------	----------------	---------------

Věty popisují pomocná slova: krákorá, akát, rarášek, trám, erb (znak Chlumu u Třeboně), lupíneček. Heslem je tak KARTEL.

Šifra 3	Prostředník	2 body
----------------	--------------------	---------------

Je třeba doplnit vždy slovo, které je s oběma výrazy na řádku spojeno. Ukáže se, že se vždy o část těla (prsty, oko, noha, čelo, hlava, ruka, vlasy). Vybereme-li pak označená písmena, dostaneme heslo ROHOVKA..

Šifra 4	Kroužky a čtverečky	2 body
----------------	----------------------------	---------------

Stačí dát k sobě slova, která k sobě patří – představují vždy jeden „hranatý“ a jeden „kulatý“ předmět stejného typu: Dukát – tisícikoruna, pyramida – rotunda, křída – fix, válec – hranol, bábovka – srnčí hřbet, brána – terč, atlas – globus, sud – krabice. Dostaneme tak znaky Braillova písma, které dávají heslo PASTELKA.

Šifra 5	Doprava třikrát jinak	3 body
----------------	------------------------------	---------------

Dopravní prostředky rozdělíme podle toho, zda jezdí po zemi, po vodě nebo létají vzduchem:

Kanoe, člun, koráb, tank, balón, auto, koloběžka, kolo, dvouplošník, surf, tramvaj, letadlová loď, parník, tryskáč, trajekt, autobus, helikoptéra, skateboard, kajak, rogalo, moped

Dostáváme tři skupiny, které odpovídají symbolům Morseovy abecedy,

	vodní dopravní prostředky jsou tečky, pozemní čárky a vzdušné oddělovače. Heslo je VOLANT.	
Šifra 6	Skládačka	3 body
	Pokud seskládáme kartičky k sobě do čtverce tak, že slova při sousedících stranách jsou opačná, dostaneme obrázek loď. Heslo je LOĎ.	
Šifra 7	Povedená dcerunka	2 body
	Je třeba najít to, co představuje dcerunka z textu. Asociace vedou na ENERGII: temná energie, chemická energie, magnetická energie, elektrická energie a energie v jídle.	
Šifra 8	Poslouchej	2 body
	Tři odkazy jsou písničky (Pavčina Jíšová a Jarek Nohavica – Žába, Anna K. - Spojeny kralovství smutku a radosti, Zrní + Radůza – Autobus), z jejich textů je třeba vybrat slova zpívaná v uvedených časech (Třeboň spojený ruce) a ta zadat do vyhledávání na Youtube – první odkaz je JaksiTaksi – Ruce spojený. V uvedeném čase zazní slovo NÁZORY.	
Šifra 9	Pro rádia	2 body
	Jedná se o části přirovnání, stačí doplnit příslušné písmeno přídavného jména: P pilný jak včelka A hladový jak vlk T tvrdý jako štolverk R černý jak bota O sprostý jak dlaždič N vyřízený jak žádost o byt A zdravý jako řípa Heslem je PATRONA.	
Šifra 10	Skládačka 2	3 body
	Na každém trojúhelníku je jednak jméno zvířete, jednak jméno rostliny nebo její části či houby. Je třeba najít asociace mezi nimi: veverka – ořešák,	

kůrovec – smrk, bourec – moruše, korál – řasa, lev – lípa (české národní symboly), moucha – rosnatka, panda – bambus, kanec – šípek (kančí se šípkovou omáčkou), kuře – švestky (Kuře na švestkách, komiks M. Satrapiové), medvěd – česnek (česnek medvědů), koza – petržel (překlad „vzná se v tom jak koza v petrželi“), holubice – oliva (symboly míru), tygr – muchomůrka (muchomůrka tygrovaná), vlk – mák (vlčí mák), liška – zázvor („Běží liška k Táboru, nese pytel zázvoru...“), roup – jmelí (parazité), kočka – vrba (květy kočičky), zajíc – mrkev
Pokud trojúhelníkové kartičky poskládáme podle nich, můžeme číst heslo NITROPLODKA POTOČNI, což je druh lišejníku.

Šifra 11 Skrumáž

2 body

Každá trojice je trojicí názvů alb českých kapel: Tata boys, Kryštof, Asonance, Laura a její tygři, Olympic, Už jsme doma, Neřež. První písmena názvů kapel dávají heslo TKALOUN.

Šifra 12 Předmět zájmu

3 body

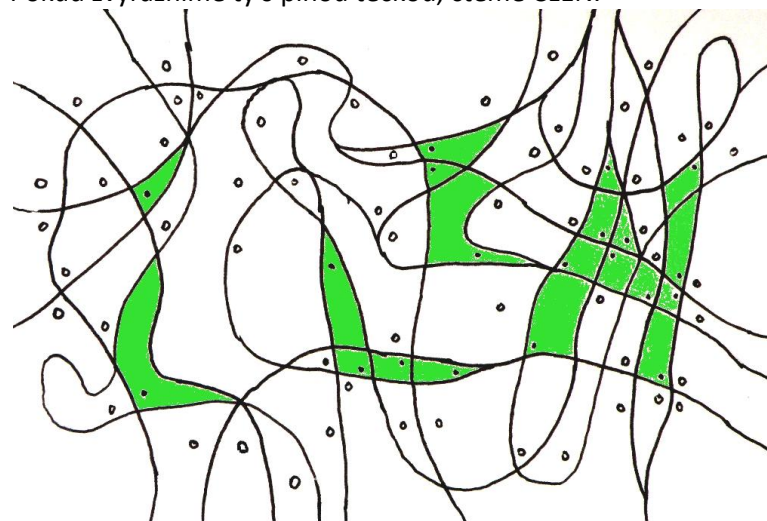
Jedná se o slova v latině (žabinec, světlo, poledník, dobyvatel, trojúhelník). Každému z nich jde přiřadit jeden školní předmět (biologie, fyzika, zeměpis, dějepis, matematika). Z nich pak bereme požadovaná písmena, dostaneme heslo LAMPA.

Grafické šifry

Šifra 1 Čáry máry

3 body

Jednotlivé části jsou označeny vždy buď plnou, nebo prázdnou tečkou. Pokud zvýrazníme ty s plnou tečkou, čteme ČLEN.



Šifra 2	Dva křížky a heslo	3 body
----------------	---------------------------	---------------

Pokud spojíme vyznačené křížky úsečkou a zvýrazníme její průnik s písmeny, dostaneme morseovku.



Pak stačí přečíst heslo KAROLINKA.

Šifra 3	Souřadnice černobíle	3 body
----------------	-----------------------------	---------------

Souřadnice ukazují umístění levého horního rohu obdélníku 3x2 do sítě, které dává příslušnou značku Braillova písma. Heslem je PSTROS.

Šifra 4	Pět bodů	3 body
----------------	-----------------	---------------

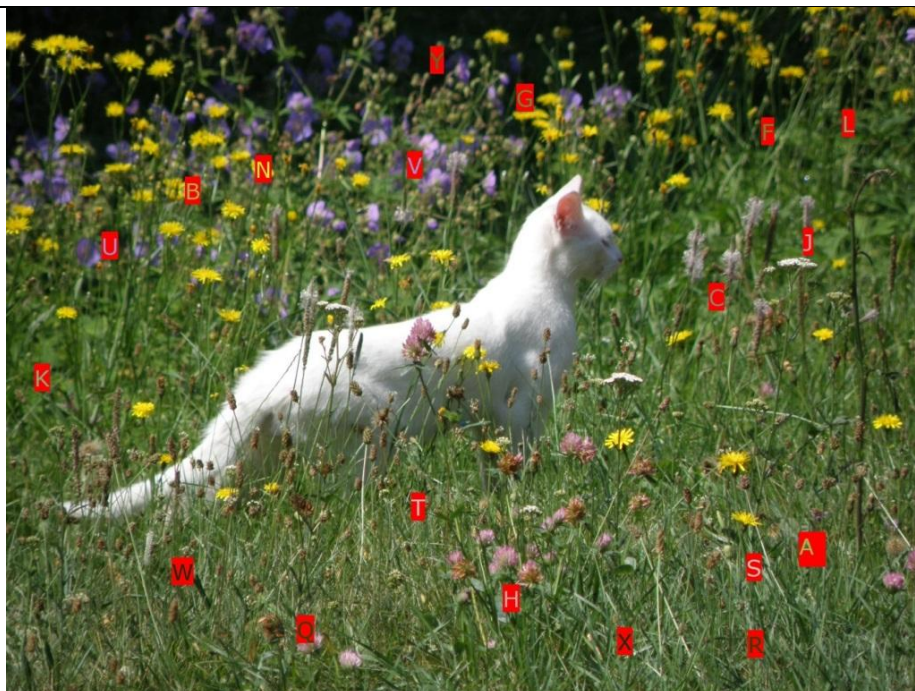
Prohlédneme-li si stránky školní šifrovací soutěže (<http://www.gymtrebon.cz/a-1097-skolni-sifrovaci-soutez-2013-2014.html>, text v šifře stylem kopíruje styl nadpisu stránek), najdeme zde seznam s pěti body (stejně velikosti, barvy i rozmístění) jako v jednom sloupci. Pokud vybíráme písmeno (pořadí určuje číslo pod sloupcem) z oranžově vyznačeného bodu seznamu, dostaneme heslo SYROVINKA.

Šifra 5	Logo – číslo – písmeno	2 body
----------------	-------------------------------	---------------

Jedná se o loga (nebo jejich části) ministerstev ČR. Z jejich názvů vybíráme příslušná písmena:
 kultury – R, obrany – O, zahraničních věcí – Z, průmyslu a obchodu – P, školství, mládeže a tělovýchovy – O, práce a sociálních věcí – C, zemědělství – E, zdravotnictví – T. Heslem je ROZPOCET.

Šifra 6	Kočka na louce	2 body
----------------	-----------------------	---------------

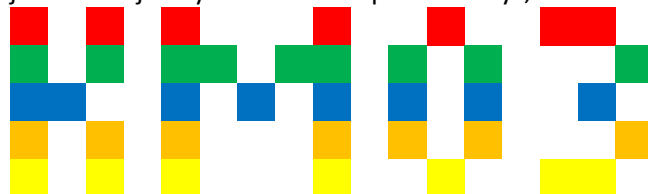
Na obrázku jsou schovaná písmena abecedy, nejsou však všechna, chybí DEIMOPZ. Po přerovnání písmen dostaneme heslo PODZEMI.



Šifra 7 Chybí nárys

2 body

Představme si, že na obrázku je půdorys a bokorys, kostky o stejné barvě jsou ve stejné výšce. Pokud doplníme nárys, dostaneme

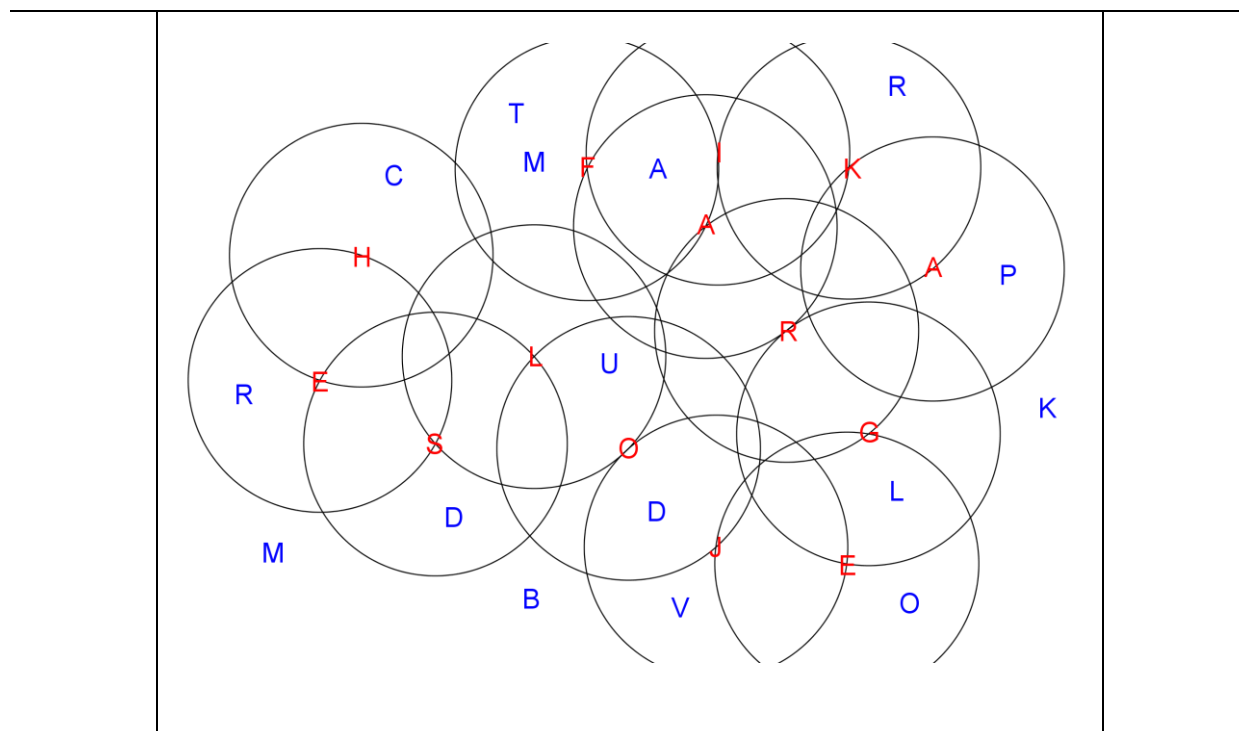


Čteme KMO3, čili KMOTŘI.

Šifra 8 Písmena a kružnice

3 body

Na kružnici se středem v H leží E, na kružnici se středem v E a stejným poloměrem leží S atd. Postupně děláme kružnice o stejném poloměru, až dostaneme text HESLO JE GRAFIKA.



Šifra 9 Učitelský stůl

2 body

Rozházené korálky tvoří znaky Braillova písma. Přečteme-li je, dostaneme VLAK.

Šifra 10 Najdi obilí

3 body

Jedná se o převedení do obrázků prvních tří veršů z textu písničky Okolo Třeboně. V textu písničky se pak zpívá o OVSU.

Šifra 11 Osobnostní komiks

3 body

Jednotlivé obrázky se vztahují k různým objevům (penicilin, zavináč v emailové adrese, sendvič, gravitace, Amerika, evoluce), u kterých je třeba určit osobu vynálezce či objevitele (Fleming, Tomlinson, Montague, Newton, Kolumbus, Darwin). Vyjde heslo LOUTKA.

Šifra 12 Cizokrajné znaky

2 body

Symbody lze rozložit na písmena, která tvoří číslovku, přičemž jedno písmeno vždy přebývá:

JEDNA(J), TŘI(H), SEDM(A), DVA(E), PĚT(Ě), ČTYŘI(N), ŠEST(D)

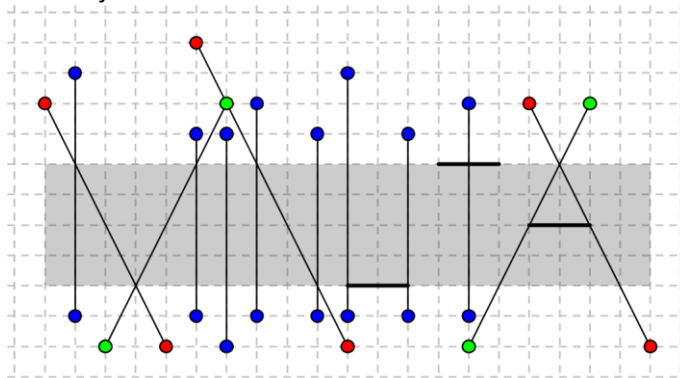
Přebývajcí písmena pak (po srovnání čísel od 1 do 7) dávají heslo JEHNĚDA.

Šifra 13 Obrázek z venkova**2 body**

Na obrázku jsou pětice (mraků, ptáků, izolátorů na sloupu, prken plotu, kytěk, brouků). Ty vždy určují kód jednoho písmene v binární abecedě. Heslo čteme odshora, je to LZICKA.

Šifra 14 Obrázek z venkova**2 body**

Spojíme modré body svisle, červené pak šikmo dolů, zelené šikmo nahoru. V obdélníku se objeví heslo MINUTA.

**Šifry využívající schémata****Šifra 1 Ve čtverci****3 body**

Pokud spojíme čísla od 1 do 5 čarami a čteme písmena, která postupně na těchto čarách leží, dostaneme slovo ROKLINA.

	a		3			w
			l			k
j		t	i		k	5
					v	
1		r		o		2
			n	a		m
	e		4		q	r
	z		l			

Šifra 2 Osmisměrka**3 body**

Pokud vyškrtneme slova, dostaneme:

B	R	R	K
Z	O	O	A
I	S	L	P
L	Y	Z	U
F	N	R	M
A	S	Y	A

Zbývá políčka dávají BRAILLZNAS, pokud tedy osmisměrku čteme jako dva a dva znaky Braillova písma, které tvoří heslo KOZA.

Šifra 6 Astromřížka 3 body

Mezi 25 obrázky se čtyřikrát opakuje černá díra – pokud je odstraníme, dostaneme šifrovací mřížku. Třemi jejími otočeními můžeme na pozicích po odstraněných černých dírách číst BILYTRPASLIK.

Šifra 7 Sudoku 3 body

Vyplníme sudoku.

6	1	2	8	7	5	4	3	9
9	3	5	1	2	4	8	6	7
4	7	8	3	9	6	1	5	2
3	8	9	4	6	7	5	2	1
2	5	7	9	8	1	6	4	3
1	6	4	2	5	3	9	7	8
8	4	3	5	1	2	7	9	6
5	9	6	7	3	8	2	1	4
7	2	1	6	4	9	3	8	5

V barevně označených polích vždy sečteme čísla a dostaneme písmena hesla STRECHA.

Šifra 8 Křížovka s obrázky 3 body

Osm obrázků jsou loga (nebo jejich části) hokejových mužstev, které se účastnili hokejové extraligy. Do křížovky doplníme města, ve kterých působí: Karlovy Vary, Liberec, Olomouc, Zlín, Litvínov, Mladá Boleslav, Vítkovice, Třinec. Vyjde heslo KLUZISTE.

Šifra 9 Tabulka morseovky 2 body

Symbody morseovky je třeba číst „po spirále“, začne se v levém horním rohu čtením prvního řádku. Dostáváme .--./-./...-/..-/..-/..-/..-, což je PANVICKA.

Šifra 10 Čtverce s písmeny**2 body**

Čtverce představují trojice kláves na klávesnici (české rozložení QWERTZ). Stačí vždy najít chybějící písmeno. Heslo je STRIZLIVOST.

Šifra 11 Tabulka morseovky 2**3 body**

Pod každým jménem je 12 políček, což odpovídá počtu měsíců v roce. Pokud vybarvíme políčko odpovídající měsíci, v němž slaví svátek daná jména, dostaneme:

Čtírad	Ludmila	Alexandr	Čestmír	Doubravka	Adriána	Vít	Patrik	Ester	Julie	Jeroným	Alois	Medard	Vanda	Robin	Ilona	Kryštof	Matouš	Zora	Leoš	Bruno	Vlasta	
																						1
																						2
																						3
																						4
																						5
																						6
																						7
																						8
																						9
																						10
																						11
																						12

Morseovka po řádcích dává heslo PSOUN.

Šifra 12 Šachová smršť**3 body**

Jedná se o podivný text s šachovou tematikou – takže k řešení bude potřeba právě šachů: Všech znaků je 64, což je počet písmen v šachovnici. Vepíšeme tedy text do šachovnice:

8	o	n	t	a	h	n	u	l
7	n	a	b	4	o	n	a	n
6	a	e	7	o	n	n	a	t
5	o	c	2	a	p	a	k	j
4	e	s	t	e	f	5	p	r
3	o	s	t	e	k	o	n	e
2	c	o	n	a	t	a	h	l
1	a	n	a	h	4	m	a	t
	a	b	c	d	e	f	g	h

Na označených polích pak čteme heslo SONAR.

Šifra 13 Transpozice čtverce**2 body**

Pokud rozdělíme tabulku na čtyři čtverce 3×3 a „pootočíme“ je kolem středu tabulku o 90 stupňů proti směru hodinových ručiček, dostaneme:

J	V	H	H	L	A
U	P	I	M	Ě	S
E	T	E	E	M	Ě
O	R	O	V	N	Í
C	O	D	T	O	Z
I	D	E	S	N	E

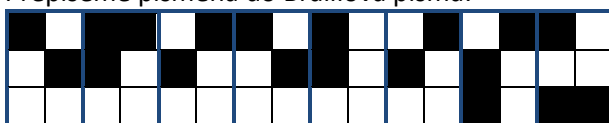
→

H	L	A	V	N	Í
M	Ě	S	T	O	Z
E	M	Ě	S	N	E
J	V	H	O	R	O
U	P	I	C	O	D
E	T	E	I	D	E

Hledaným hlavním městem země s nejvyšší horou Pico de Teide (Španělska) je MADRID.

Víceúrovňové šifry**Šifra 1 Braill a pak morseovka****2 body**

Přepíšeme písmena do Braillova písma:



Černé značky pak dávají po řádcích morseovkou PANDA.

Šifra 2 Ber šest a pak pět**3 body**

Pokud si přečteme Braillovo písmo z černých teček, dostaneme nápovědu BINARNICERNA. Vezmeme tedy pětice teček počínající vždy u vyznačených teček, černá znamená 1, červená 0. Dostaneme písmena O, U, D, P, R, která dávají po přesmyčce slovo PROUD.

Šifra 3 Obrazová galerie**2 body**

V obou řadách je pět obrazů, lze vždy vybrat po jednom obraze z obou řad, které jsou od stejného autora (da Vinci, Gogh, Mucha, Gauguin, Aleš). Ty pak určují znak Braillova písma. Dostaneme dohromady heslo TUREK.

Šifra 4 Vlajky a kříž**2 body**

Vlajky náleží následujícím státům: Irsko (IRL), Kuvajt (KWT), Maledivy (MDV), Singapur (SGP), Česká republika (CZE), Burkina Faso (BFA), Maďarsko (HUN).

Z jejich zkratek pak dáme dohromady polský kříž:

IRL	KWT	MDV
SGP	CZE	BFA
HUN	ChJO	QXY

Z něj pak přečteme heslo SYNChRONIZACE.

6. Pracovní listy

Následující část shrnuje vzniklé pracovní listy, které mají sloužit pro zpestření hodin matematiky a zopakování různých témat netradičním způsobem. Témata a jejich zařazení do výuky na osmiletém gymnáziu jsou uvedena v následující tabulce:

Název pracovního listu	Téma	Zařazení do výuky
Pracovní list 1 – Transpoziční šifra a kombinatorika	Využití kombinatorických pravidel v šifrování	Oktáva
Pracovní list 2 – Substituční šifry, kódování a kombinatorika	Využití kombinatorických pravidel v šifrování	Oktáva
Pracovní list 3 – Posuny abecedy a dělitelnost čísel	Posunování písmen zprávy v závislosti na jednoduchých vlastnostech dělitelnosti přirozených čísel	Sekunda a vyšší ročníky
Pracovní list 4 – Šifrování a grafy funkcí	Práce s grafy lineárních funkcí, nepřímých úměrností a jednoduchých kvadratických funkcí	Kvarta a vyšší ročníky
Pracovní list 5 – Graf logaritmické funkce	Práce s grafy logaritmických funkcí	Sexta a vyšší ročníky
Pracovní list 6 – Římské číslice	Zápis čísel pomocí římských číslic	Prima a vyšší ročníky

Tabulka 12: Pracovní listy

Pracovní list 1 – Transpoziční šifra a kombinatorika

Základní pojmy a úmluvy

Transpoziční šifra je šifrovací metoda, při níž se znaky zprávy (otevřeného textu) přehází daným způsobem a vznikne tak zašifrovaný text.

Budeme používat mezinárodní abecedu s 26 písmeny (tj. bez háček, čárek a CH).

Příklad 1

Kolika způsoby můžeme zašifrovat slovo HESLO?

Řešení: Máme 5 písmen na 5 pozic. Na první pozici můžeme dát 5 písmen, na druhou pozici už jen 4 písmena, na třetí pozici jen 3 písmena, na čtvrtou pozici pouze 2 písmena a na poslední už zbývá jediné písmeno. Celkem tedy máme $5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 5! = 120$ možností:

--	--	--	--	--

$$5 \cdot 4 \cdot 3 \cdot 2 \cdot 1$$

Jedno z možných přerovnání však představuje otevřený text - šifrovaných textů je tak jen 119.

Příklad 2

Kolika způsoby můžeme zašifrovat slovo TRANSPOZICE?

Řešení: Žádné z 11 písmen se neopakuje, tudíž postupujeme stejně jako u předchozího příkladu.

Počet možných přerovnání je $11! = 11 \cdot 10 \cdot 9 \cdot \dots \cdot 2 \cdot 1 = 39\,916\,800$, počet šifrovaných textů je o jeden menší. Slovo TRANSPOZICE můžeme zašifrovat 39 916 799 způsoby.

Příklad 3

Kolika způsoby můžeme zašifrovat slovo PONORKA?

Řešení: Ve slově se opakuje dvakrát písmeno O. Nejprve si obě O rozlišíme jako O_1 a O_2 . Pak máme 7 různých znaků, které umísťujeme na 7 pozic. Máme celkem $7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 7! = 5040$ možných uspořádání. Protože však uspořádání stejná až na pořadí O_1 a O_2 považujeme za totožná, musíme jejich počet dělit dvěma, máme tak $5040 : 2 = 2520$ různých přerovnání písmen. Slovo PONORKA tak můžeme zašifrovat celkem $2520 - 1 = 2519$ způsoby.

Příklad 4

Kolika způsoby můžeme zašifrovat jméno radaru TAMARA?

Řešení: Postupujeme stejně jako u předešlého příkladu. Rozlišme si tři písmena A na A_1, A_2, A_3 . Pak máme šest různých znaků umístit na šest pozic. Máme tak $6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 6! = 720$ různých umístění.

Kolik takových umístění považujeme za totožná? Za totožná považujeme ta umístění, která se liší pořadím výskytu A_1, A_2, A_3 . Kolik je takových pořadí?

Jako první A můžeme zvolit kterékoliv ze tří znaků. Za druhé A pak můžeme dát pouze jedno ze zbylých dvou znaků. Na třetí A zbude poslední z trojice A_1, A_2, A_3 . Celkem máme tak $3 \cdot 2 \cdot 1 = 6$ různých pořadí znaků A_1, A_2, A_3 .

Počet uspořádání písmen slova TAMARA je $720 : 6 = 120$. Šifrovaných textů tak získáme $120 - 1 = 119$.

Pracovní list 2 – Substituční šifry, kódování a kombinatorika

Substituční šifry vznikají záměnou znaků otevřeného textu za znaky jiné podle daného algoritmu.

Jednoduchá monoalfabetická substituce nahrazuje každý znak otevřeného textu znakem jiným, pevně daným.

V úlohách budeme používat mezinárodní abecedu s 26 písmeny jako abecedu otevřeného i šifrovaného textu.

Příklad 1

Nejjednodušší substituční šifrou je posun písmen abecedy o dohodnutý počet míst. Například Julius Caesar posouval abecedu o tři písmena ($A \rightarrow D, B \rightarrow E, C \rightarrow F, \dots W \rightarrow Z, X \rightarrow A, Y \rightarrow B, Z \rightarrow C$). Slovo BABKA se zašifruje jako EDEND.

Proto se této metodě říká Caesarova šifra. Kolik různých Caesarových šifer existuje?

Řešení: Je jich tolik, na kolik písmen je možné posunout například písmeno A, tedy 25.

Příklad 2

Kolik existuje všech jednoduchých monoalfabetických substitucí? Za jak dlouho by počítač s jistotou rozluštil tuto šifru, jestliže dokáže za vteřinu ověřit 100 miliard možností?

Řešení: Vypišme si abecedu. První písmeno A můžeme nahradit 26 písmeny, písmeno B už jen 25 písmeny atd. Jedná se tedy o počet permutací z 26 prvků:

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							
26	·	25	·	24	·	...							...							...							·	3	·	2	·	1

Celkem tedy existuje $26! - 1 = 403\,291\,461\,126\,605\,635\,583\,999\,999 \doteq 4,03 \cdot 10^{26}$ jednoduchých monoalfabetických substitucí. (Jedna substituce nahrazuje písmena totožnými písmeny, šifrovaný text by tak byl totožný s otevřeným. Proto se odečítá 1.)

Počítač by zprávu rozluštil za $(4,03 \cdot 10^{26} : 10^{11}) = 4,03 \cdot 10^{15}$ vteřin, což je zhruba $6,7 \cdot 10^{13}$ minut, tedy $1,3 \cdot 10^8$ let.

Poznámka

Ve skutečnosti není třeba všechny možnosti procházet. Existuje metoda zvaná **frekvenční analýza**, která umí rozluštit jednoduché substituce s podstatně menší kapacitou. Je založena na četnosti výskytu písmen v textu psaném určitým jazykem. Pro texty s více jak 50 písmeny bývá spolehlivá.

Tato metoda byla známa už muslimským učencům v 9. století. První známý popis metody je sepsán ve spisu Rukopis o dešifrování kryptografických zpráv od al-Kindího.

Příklad 3

Kolik existuje substitucí, které nahrazují dvojice písmen?

Řešení: Všechno uspořádaných dvojic písmen je $26 \cdot 25 = 650$. Tedy počet všech uvažovaných substitučních šifer je $650! - 1$.

Příklad 4

Kolik existuje substitucí, ve kterých jsou znaky samohlásek nahrazovány opět znaky samohlásek a znaky souhlásek opět znaky souhlásek?

Řešení: Znaků samohlásek je 6 (A, E, I, O, U, Y), znaků souhlásek je tedy 20. Dostáváme tak

$$6! \cdot 20! = 1\,751\,689\,445\,887\,180\,800\,000 = 1,7 \cdot 10^{21} \text{ možností.}$$

Příklad 5

Kolik existuje tzv. polyalfabetických substitucí, ve kterých se používají dvě abecedy šifrovaného textu, a to tak, že lichá písmena jsou převedena na znaky první abecedy a sudá písmena na znaky druhé abecedy?

Řešení: Lichá písmena můžeme zašifrovat pomocí $26!$ různých substitucí, stejně tak i sudá písmena. Dohromady dostáváme $(26!)^2 - 1 = 1,63 \cdot 10^{53}$ různých substitucí.

Kódováním budeme rozumět převedení písmen otevřeného textu na jiné znaky. Na rozdíl od šifrování ale hlavním účelem převodu není utajení smyslu textu, ale jeho přenesení, předání. Příklady kódů jsou Morseova abeceda nebo Braillovo písmo.

Příklad 6

Braillovo písmo je sestaveno ze znaků, které jsou tvořeny šesti tečkami, bílými, anebo černými. Kolik takových znaků existuje?

Řešení: Máme šest uspořádaných teček, každá je buď bílá, anebo černá. Máme tedy $2^6 = 32$ možných znaků Braillova písma.

Příklad 7

Nejvýše kolikačlenné skupiny by bylo třeba používat při kódování písmen morseovkou, jestliže bychom kromě teček a čárek používali i +?

Řešení: Pracujeme se třemi symboly, které mohou tvořit jeden znak. Jednočlenné znaky máme 3, dvoučlenných znaků je $3 \cdot 3 = 9$, tříčlenných pak $3 \cdot 3 \cdot 3 = 27$. Postačily by tedy nejvýše tříčlenné znaky. (Z výpočtu plyne, že by stačily i právě tříčlenné znaky.)

Pracovní list 3 – Posuny abecedy a dělitelnost čísel

Úlohy

Úloha 1

Zašifrujte slovo PROVAZY posunutím písmen o +2 a +5.

Úloha 2

Zjistěte slovo, které po posunutí o -3 se změní na YBGHOLW.

Úloha 3

Určete slovo, které bylo zašifrováno na KLSPALS posunutím o $+p$, kde p je neznámé prvočíslo.

Úloha 4

Zašifrujte skupinu znaků DPXPJMMZVDTG, a to tak, že první znak posunete o +1, druhý znak o +2, třetí znak o +3 atd.

Úloha 5

Dešifrujte skupinu znaků UROQQCCCPK, a to tak, že znaky na prvočíselných pozicích posuňte o +1, znaky na pozicích označenými složenými čísly posuňte o -2 .

Úloha 6

Posuňte každé z písmen skupiny RMRDDJKORR o tolik, kolik je zbytek čísla jeho pozice po dělení čtyřmi.

Úloha 7

Posuňte ve skupině DJGBSOVPLVZFK ta písmena, jejichž pozice jsou označeny děliteli čísla 30, o -1 , ostatní písmena o +3.

Úloha 8

Máme rozluštit skupinu znaků

MHGUC LYBLW HWDNW LMABG KHIDY UFWBG XWDAN WFWLJ CKNSS KNGXN SUYL.

Písmena na pozicích, které jsou násobky 2 nebo 3, posuňte o +8, ostatní o +6. Najděte požadované číslo v šifře.

Úloha 9

Máme rozluštit skupinu znaků

SLOTL SZNZW TSJJU DUFZV GLPVZ RKJZH YHUEK JZFAZ JZY

Písmena na pozicích s lichým zbytkem po dělení pěti posuňte o -4 , ostatní o -7 .

Pracovní list 3 – Posuny abecedy a dělitelnost čísel

Řešení a návod pro učitele

Budeme používat mezinárodní abecedu o 26 písmenech, bez CH, háčků a čárek.

Převod písmen na čísla

Písmena budeme převádět na přirozená čísla od 1 do 26 podle jejich pořadí v abecedě:

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

Nyní můžeme posunování písmene v abecedě převádět na zvyšování nebo snižování jeho pořadí:

Příklad:

Posuneme písmena abecedy o +1, +2 a -3:

	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
+1	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
+2	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
-3	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

Písmena se posunují cyklicky, tedy pokud zvyšujeme pořadí o 1, písmeno Z se posune na A atd. Pokud snižujeme pořadí o 3, pak posuneme C na Z, B na Y, A na X.

Úloha 1

Zašifrujte slovo PROVAZY posunutím písmen o +2 a +5.

Řešení:

$$\text{PROVAZY} \xrightarrow{+2} \text{RTQXCBA}, \quad \text{PROVAZY} \xrightarrow{+5} \text{UWTAFED}$$

Úloha 2

Zjistěte slovo, které po posunutí o -3 se změní na YBGHOLW.

Řešení:

$$\text{YBGHOLW} \xrightarrow{+3} \text{VYDELIT}$$

Úloha 3

Určete slovo, které bylo zašifrováno na KLSPALS posunutím o $+p$, kde p je neznámé prvočíslo.

Řešení:

Stačí posunout písmena postupně o několik prvních prvočísel a určit, které z nich odpovídá p :

	K	L	S	P	A	L	S
-2	I	J	Q	N	Y	J	Q
-3	H	I	P	M	X	I	P
-5	F	G	N	K	V	G	N
-7	D	E	L	I	T	E	L

Všechna písmena zprávy nemusí být šifrována pomocí stejného posunutí. Nejjednodušší takovou šifrou je posunutí písmen na jednotlivých pozicích o daný počet míst.

Úloha 4

Zašifrujte skupinu znaků DPXPJMMZVDTG, a to tak, že první znak posunete o $+1$, druhý znak o $+2$, třetí znak o $+3$ atd.

Řešení:

DPXPJMMZVDTG → ERATOSTHENES

Úloha 5

Dešifrujte skupinu znaků UROQCCCCPK, a to tak, že znaky na prvočíselných pozicích posuňte o $+1$, znaky na pozicích označenými složenými čísly posuňte o -2 .

Řešení:

UROQCCCCPK → USPORADANI

První písmeno se neposouvá, 1 není ani prvočíslo, ani složené číslo. Písmena na prvočíselných pozicích jsou označena oranžově.

Úloha 6

Posuňte každé z písmen skupiny RMRDDJKORR o tolik, kolik je zbytek čísla jeho pozice po dělení čtyřmi.

Řešení:

RMRDDJKORR → SOUDELNOST

Zelená písmena se posunou o $+1$, oranžová o $+2$, červená o $+3$, modrá se neposunou.

Úloha 7

Posuňte ve skupině DJGBSOVPLVZFK ta písmena, jejichž pozice jsou označeny děliteli čísla 30, o -1 , ostatní písmena o $+3$.

Řešení:

DJGBSOVPLVZFK $\rightarrow$ CIFERNYSOUCIN

Písmena na pozicích označených děliteli třiceti jsou vyznačeny oranžově.

Úloha 8

Máme rozluštit skupinu znaků

MHGUC LYBLW HWDNW LMABG KHIDY UFWBG XWDAN WFWLJ CKNSS KNGXN SUYL.

Písmena na pozicích, které jsou násobky 2 nebo 3, posuňte o $+8$, ostatní o $+6$. Najděte požadované číslo v šifře.

Řešení:

SPOCI TEJTE NEJVE TSIHO SPOLE CNEHO DELIT ELETR ISTAA STODV ACET

$$D(300,120) = D(2^2 \cdot 3 \cdot 5^2, 2^3 \cdot 3 \cdot 5) = 2^2 \cdot 3 \cdot 5 = 60$$

Úloha 9

Máme rozluštit skupinu znaků

SLOTL SZNZW TSJJU DUFZV GLPVZ RKJZH YHUHK JZFAZ JZY

Písmena na pozicích s lichým zbytkem po dělení pěti posuňte o -4 , ostatní o -7 .

Řešení:

Dostaneme text NEJME NSISP OLECN YNASO BEKOS MDESA TAPAD ESATS EST (Zeleně jsou značená písmena posouvána o -4).

Didaktické poznámky

Žákům rozdejte tabulky, v ní pak mohou hledat posunutá písmena.

Přiložená prezentace obsahuje vedle vysvětlení i úlohy 1, 2, 3 a 4 spolu s jejich řešením.

Úlohy 1, 2, 3, 4 řešíme společně, s případnou pomocí žákům.

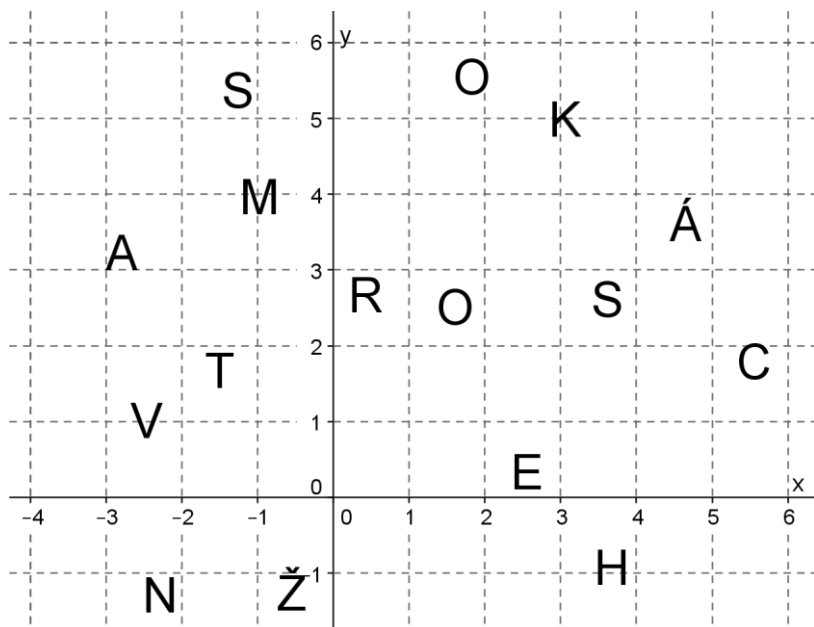
Pracovní list 4 – Šifrování a grafy funkcí

Řešení a návod pro učitele

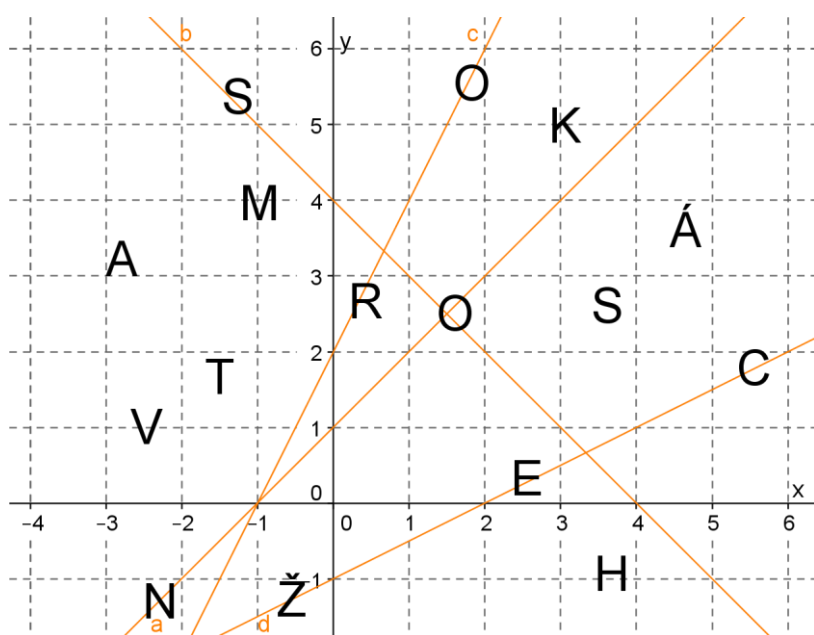
Hesla jsou jména zvířat nebo slova či sousloví s nimi spojená.

Šifra 1

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

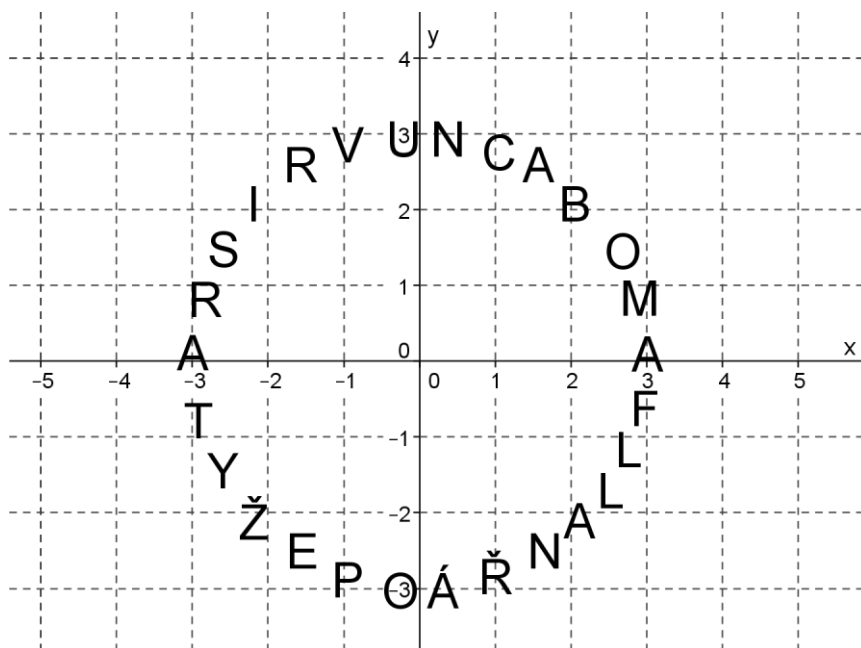


Řešení: NOSOROŽEC

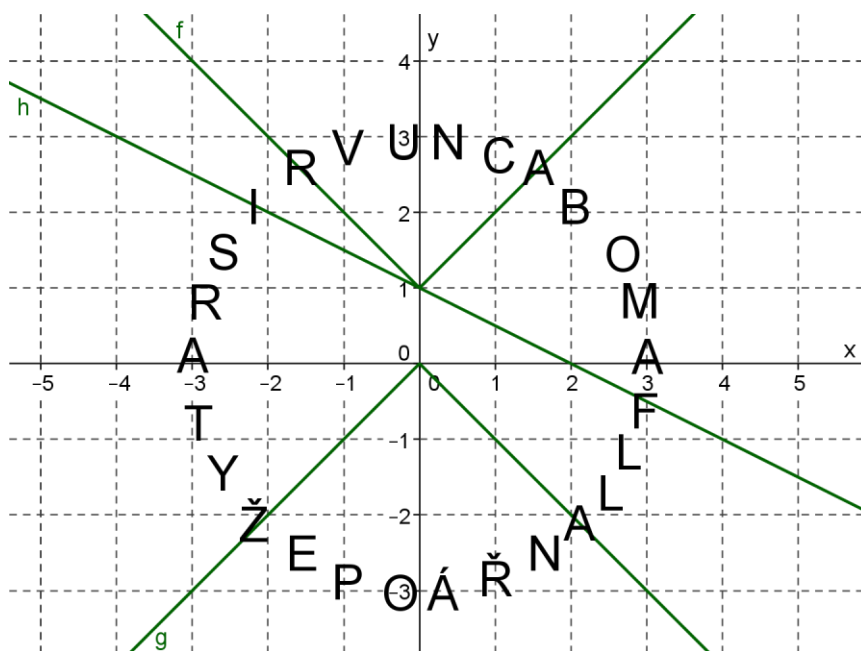


Šifra 2

$$f: y = |x| + 1, \quad g: y = -|x|, \quad h: y = -\frac{1}{2}x + 1$$



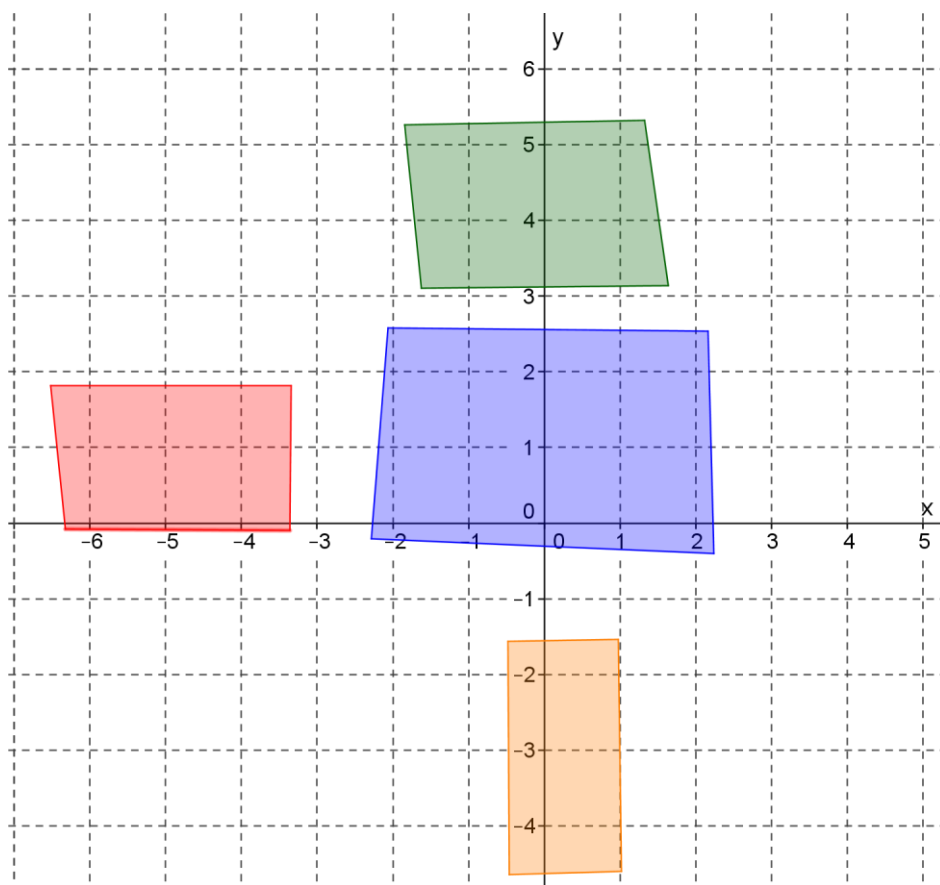
Řešení: ŽIRAFA



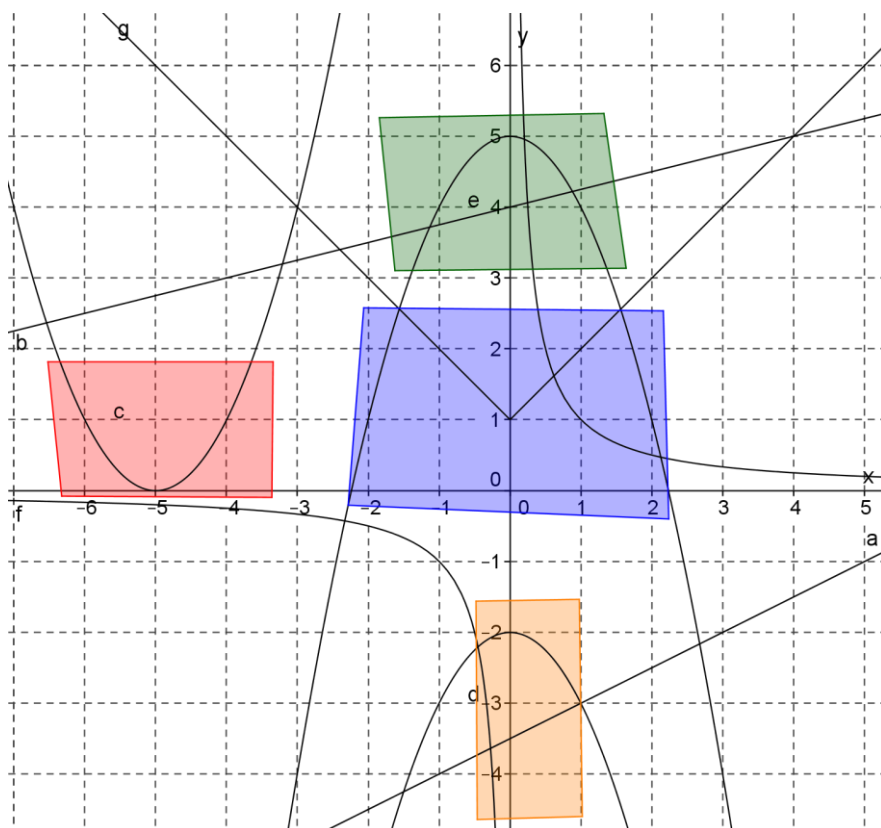
Šifra 3

$$y = \frac{1}{x}, \quad y = \frac{x-7}{2}, \quad y = -x^2 - 2, \quad y = (x+5)^2,$$

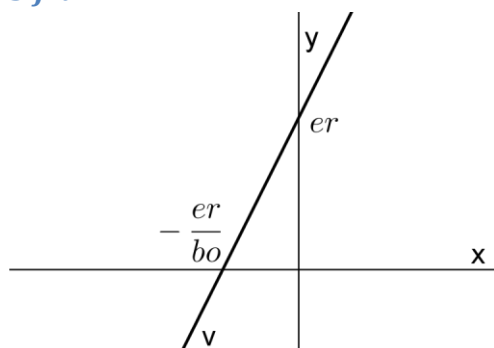
$$y = -x^2 + 5, \quad y = |x| + 1, \quad y = -x^2 + 5, \quad y = \frac{x}{4} + 4$$



Řešení: PUMA



Šifra 4



Řešení: $v: y = bo \cdot x + er$, VYJE BOXER

Šifra 5

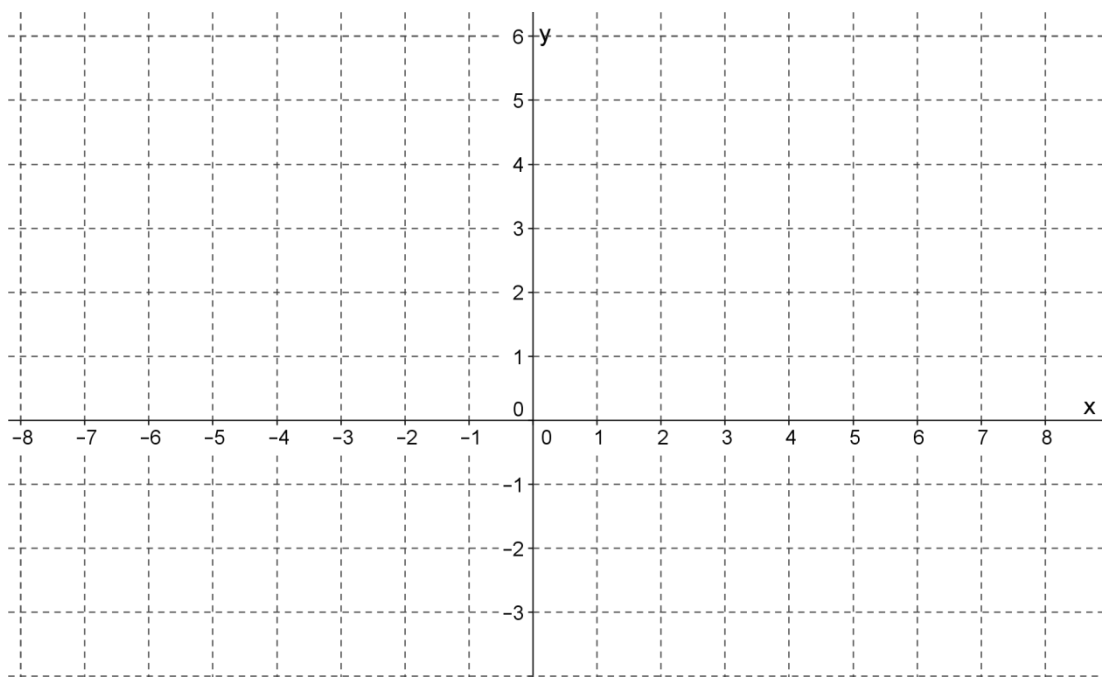
$$y = -|x + 3|; -5 \leq x \leq 0; \quad y = -|x - 3|; 0 \leq x \leq 5;$$

$$y = 4x + 5; -1,6 \leq x \leq -0,6; \quad y = -4x + 5; 0,6 \leq x \leq 1,6;$$

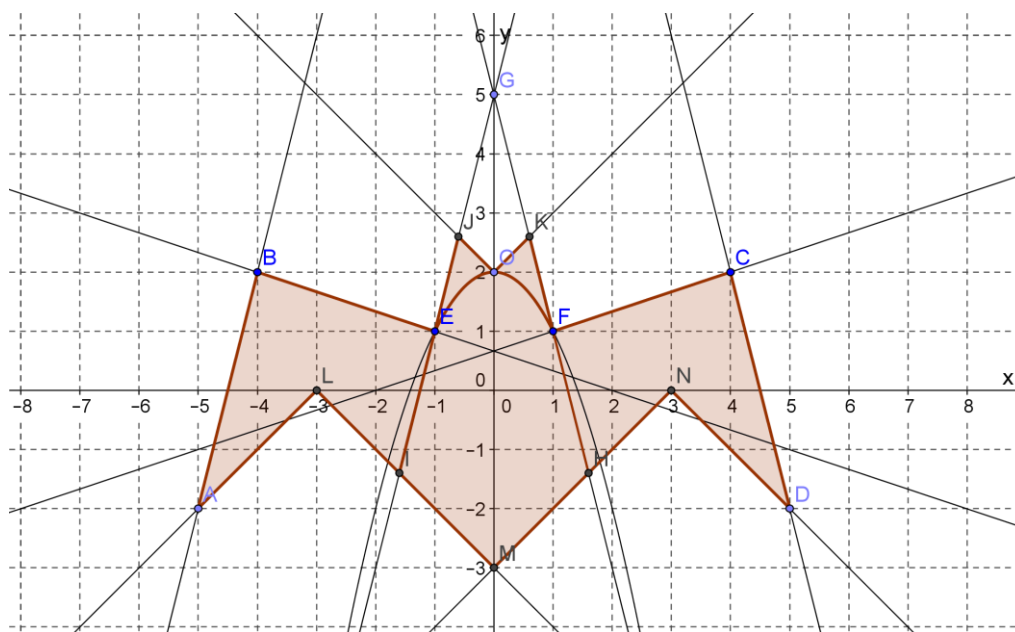
$$y = 4x + 18; -5 \leq x \leq -4; \quad y = -4x + 18; 4 \leq x \leq 5;$$

$$y = \frac{-x + 2}{3}; -4 \leq x \leq -1; \quad y = \frac{x + 2}{3}; 1 \leq x \leq 4;$$

$$y = |x| + 2; -0,6 \leq x \leq 0,6; \quad y = -x^2 + 2; -1 \leq x \leq 1$$



Řešení: NETOPÝR



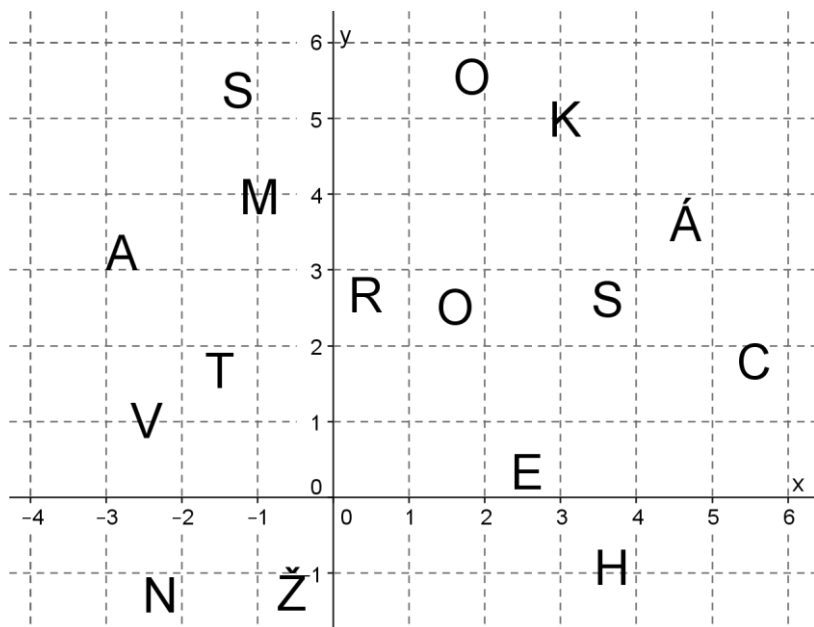
Pracovní list 4 – Šifrování a grafy funkcí

Úlohy

Hesla jsou jména zvířat nebo slova či sousloví s nimi spojená.

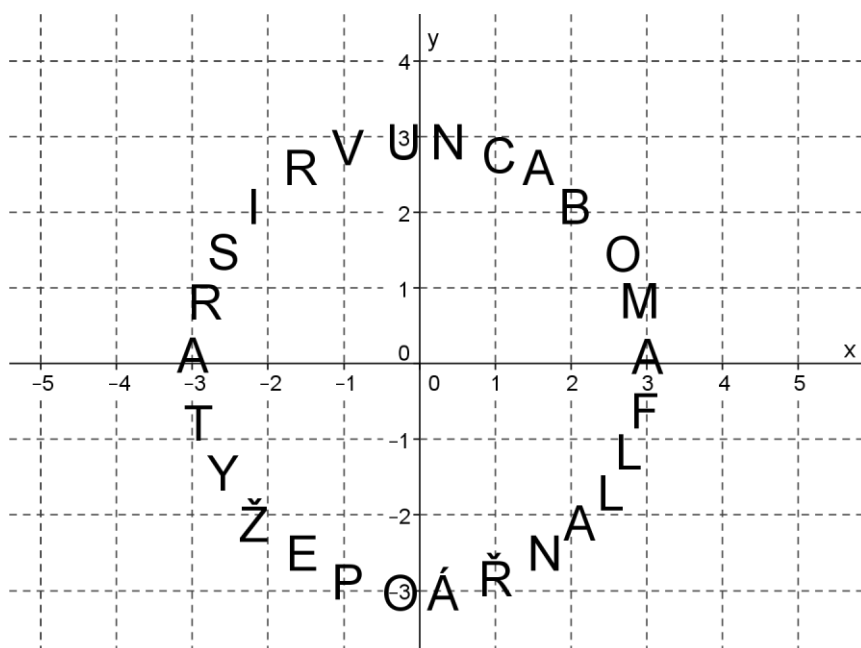
Šifra 1

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



Šifra 2

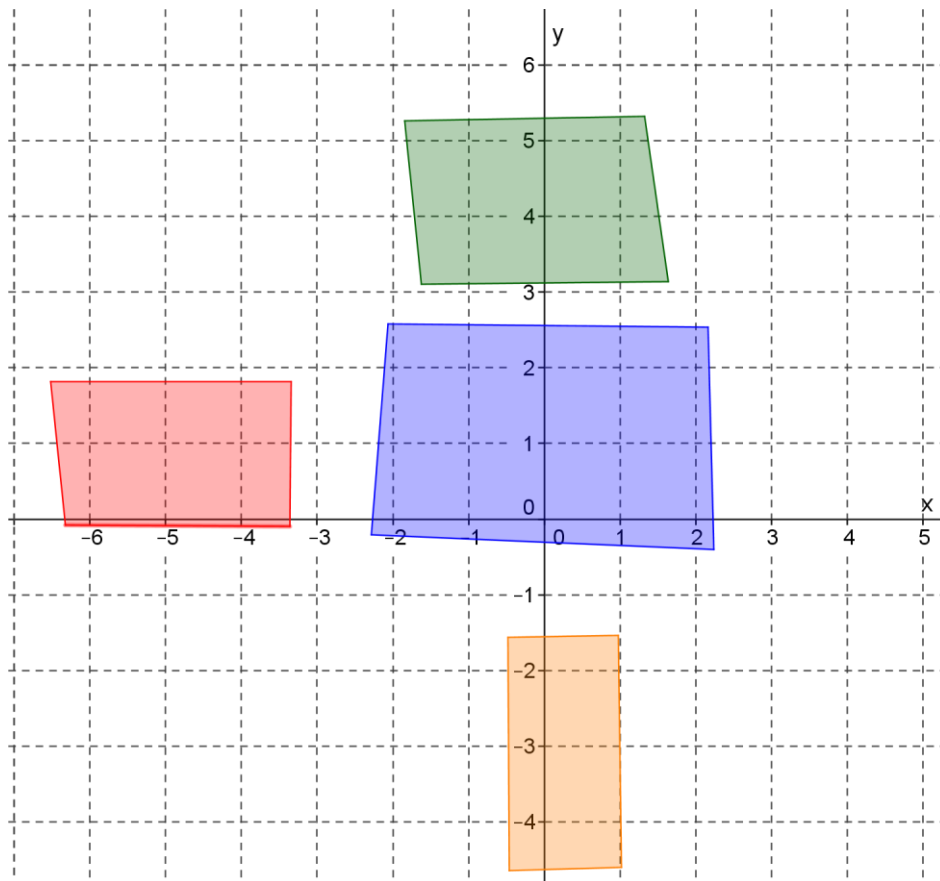
$$f: y = |x| + 1, \quad g: y = -|x|, \quad h: y = -\frac{1}{2}x + 1$$



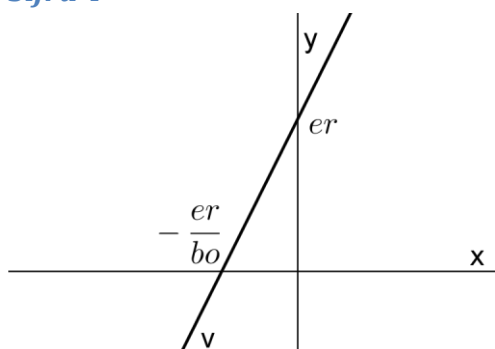
Šifra 3

$$y = \frac{1}{x}, \quad y = \frac{x-7}{2}, \quad y = -x^2 - 2, \quad y = (x+5)^2,$$

$$y = -x^2 + 5, \quad y = |x| + 1, \quad y = -x^2 + 5, \quad y = \frac{x}{4} + 4$$



Šifra 4



Šifra 5

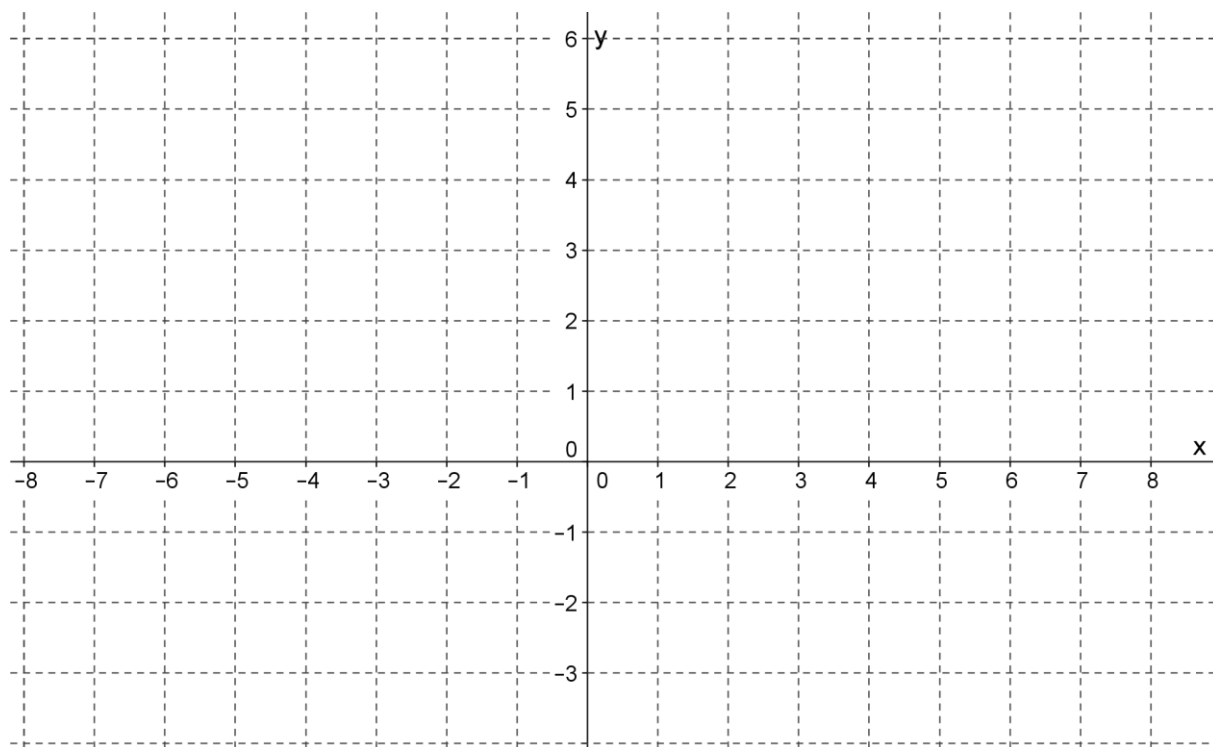
$$y = -|x + 3|; -5 \leq x \leq 0; \quad y = -|x - 3|; 0 \leq x \leq 5;$$

$$y = 4x + 5; -1,6 \leq x \leq -0,6; \quad y = -4x + 5; 0,6 \leq x \leq 1,6;$$

$$y = 4x + 18; -5 \leq x \leq -4; \quad y = -4x + 18; 4 \leq x \leq 5;$$

$$y = \frac{-x + 2}{3}; -4 \leq x \leq -1; \quad y = \frac{x + 2}{3}; 1 \leq x \leq 4;$$

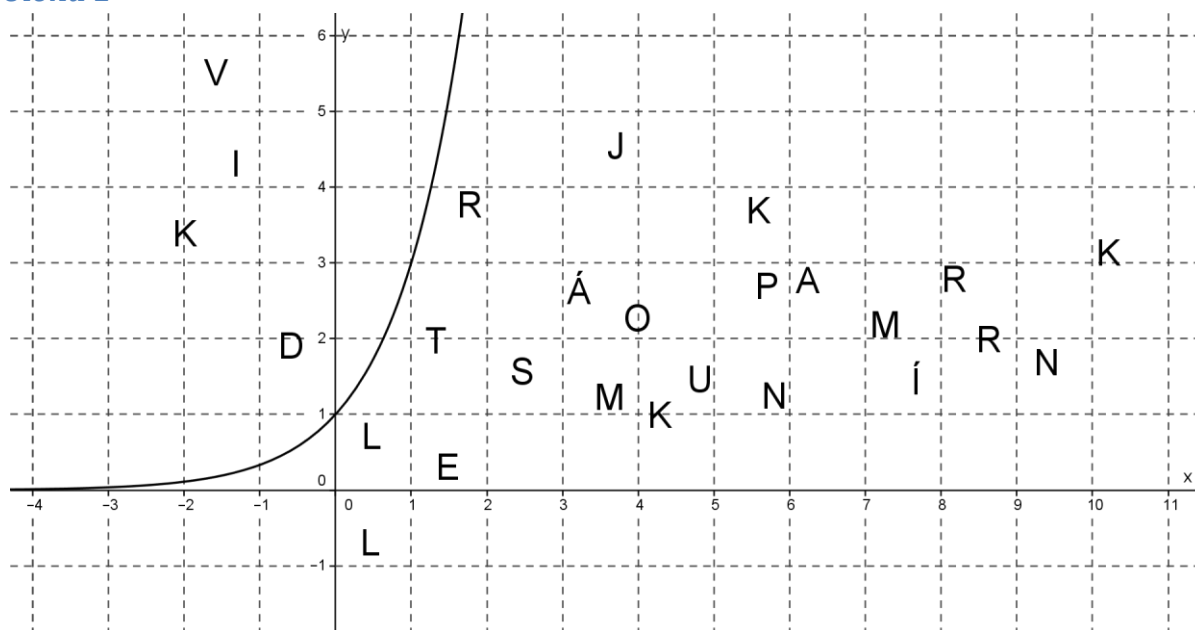
$$y = |x| + 2; -0,6 \leq x \leq 0,6; \quad y = -x^2 + 2; -1 \leq x \leq 1$$



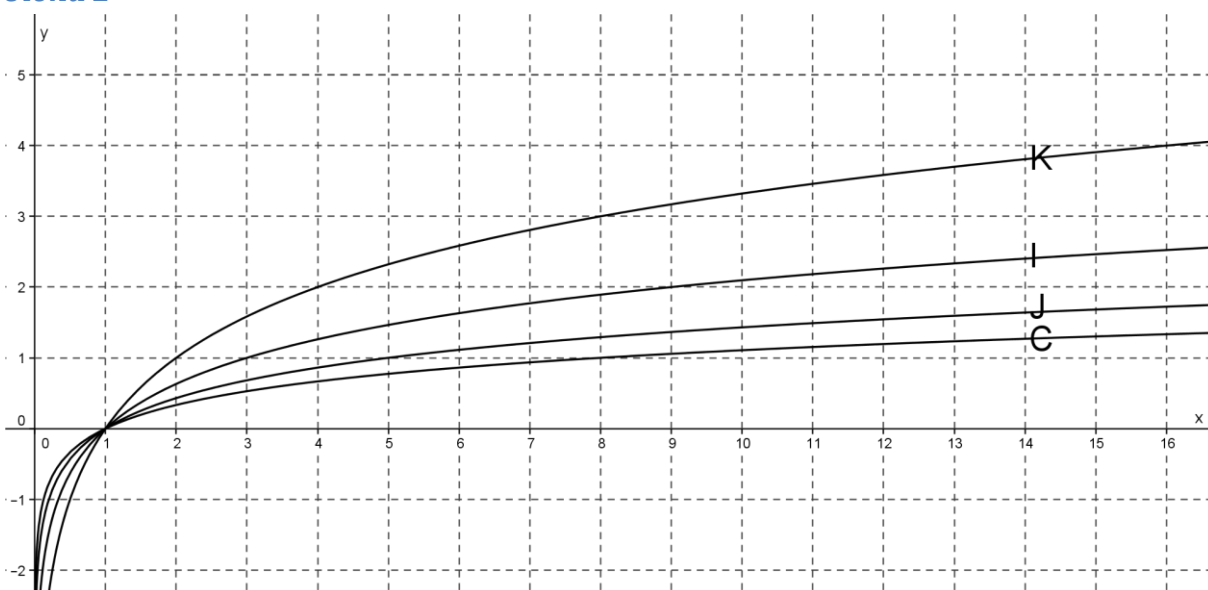
Pracovní list 5 – Graf logaritmické funkce

Používá se abeceda bez CH.

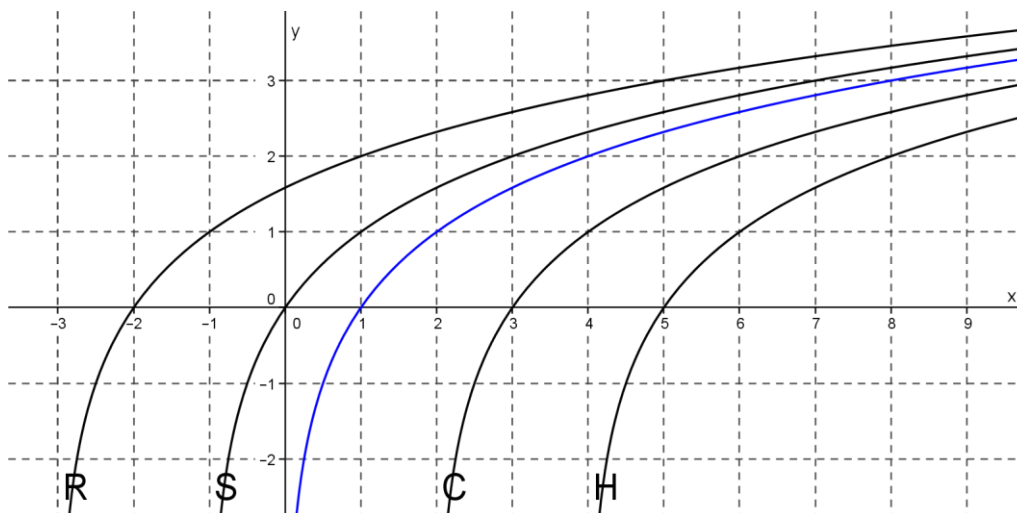
Úloha 1



Úloha 2

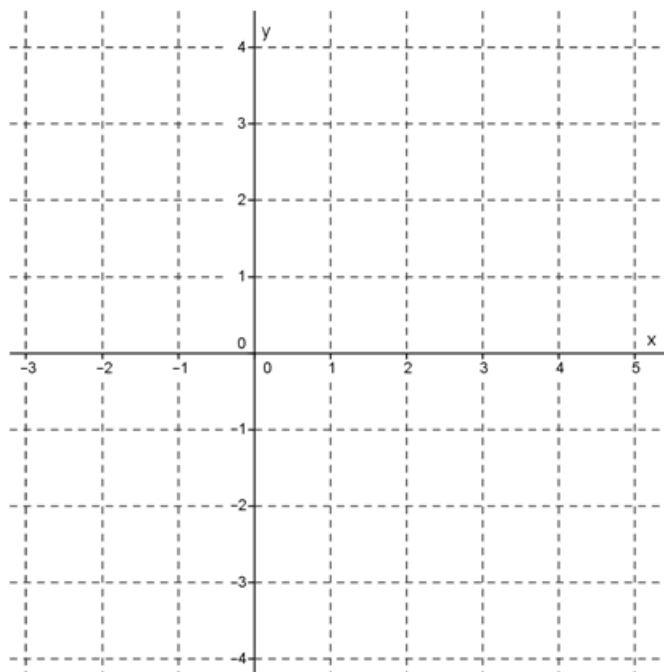
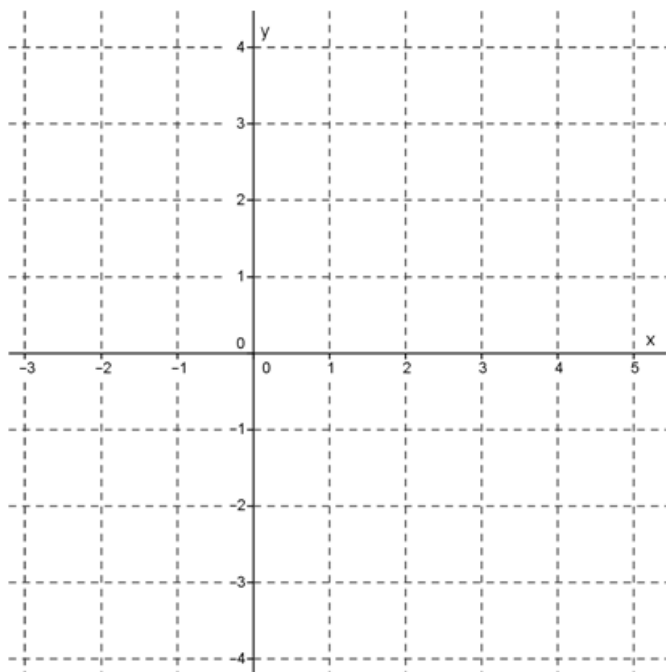


Úloha 3



Úloha 4

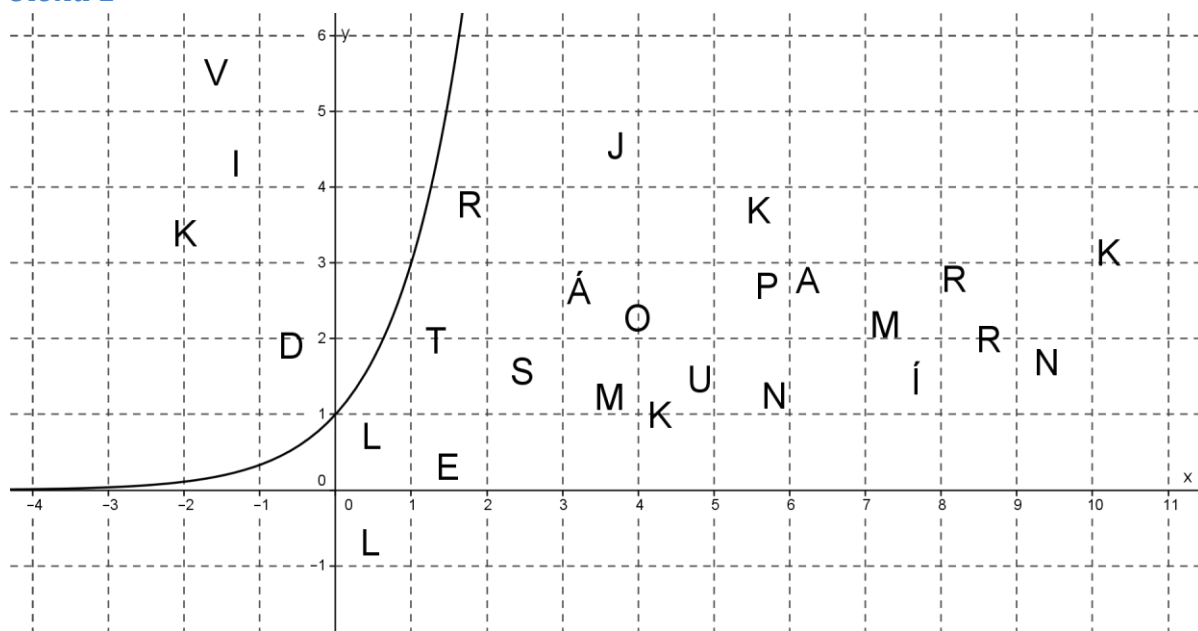
$y = \log_2 x,$ $x \in \langle 0,5; 2,5 \rangle$	$y = \log_2(x - 0,5) + 4,$ $y \in \langle -2; 3 \rangle$	$y = \log_2(x - 0,5) + 4,$ $y \in \langle -1,5; 1,5 \rangle$
$y = -\log_2(x + 1) + 1,$ $x \in \langle 0,5; 3 \rangle$	$y = \log_2(-(x - 3)) + 2,$ $y \in \langle -2; 3 \rangle$	$y = -\log_2(x + 1) + 1,$ $x \in \langle 0,5; 2,5 \rangle$
$y = \log_2(-(x - 3)) + 2,$ $x \in \langle 1; 2,5 \rangle$	$y = -\log_2(x + 1) + 1,$ $x \in \langle 0,5; 3 \rangle$	$y = \log_2 x,$ $x \in \langle 1; 2,5 \rangle$
$y = \log_2(x - 0,5) + 4,$ $y \in \langle -1; 3 \rangle$		



Pracovní list 5 – Graf logaritmické funkce

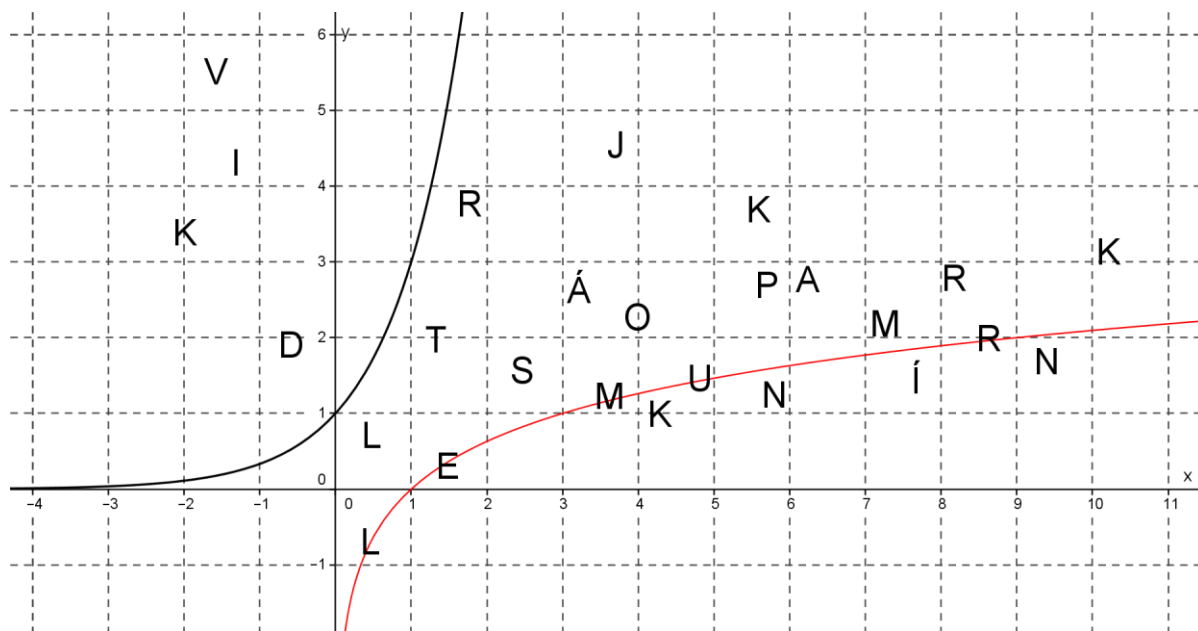
Řešení a návod pro učitele

Úloha 1

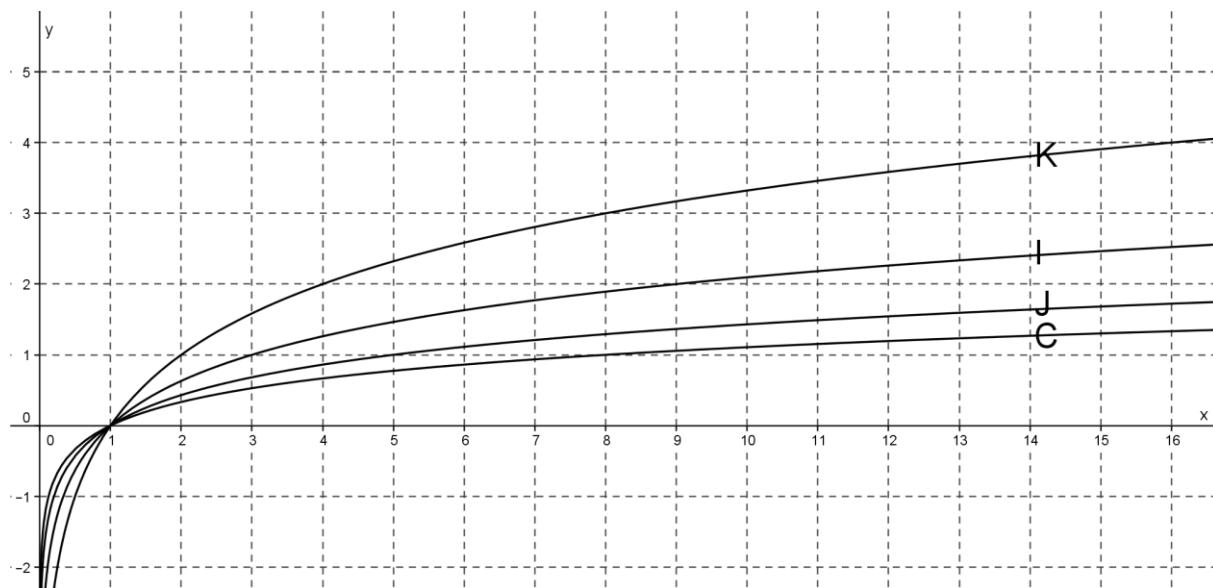


Pokyny: Zakreslete graf inverzní funkce.

Řešení: LEMUR – která písmena protne křivka.



Úloha 2

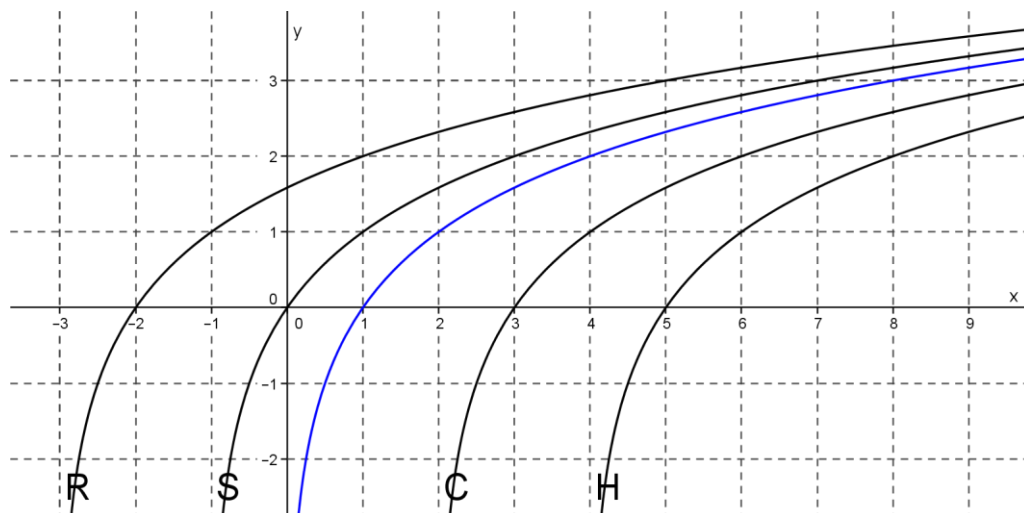


Pokyny: Na obrázku jsou grafy logaritmických funkcí. Čím se liší? Jak by tyto odlišnosti šlo „použít“ na písmena?

Řešení: Logaritmické funkce se liší základy: 2, 3, 5, 8. Pokud posuneme písmeno na daném grafu o tolik pozic, kolik je příslušný základ, dostaneme MLOK:

K	L	M						
I	J	K	L					
J	K	L	M	N	O			
C	D	E	F	G	H	I	J	K

Úloha 3



Pokyny: Na obrázku jsou opět grafy logaritmických funkcí. Čím se liší? Jak by tyto odlišnosti šlo „použít“ na písmena?

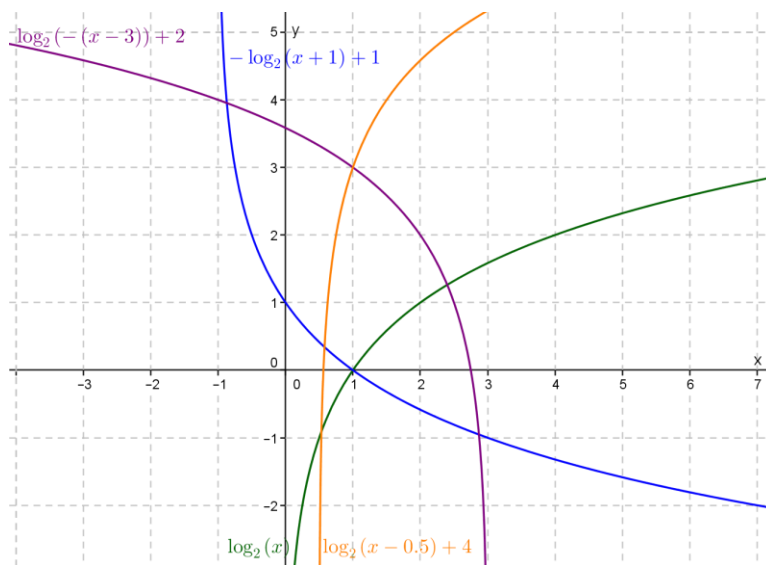
Řešení: Jedná se o grafy dvojkového logaritmu posunutého o 3 doleva, o 1 doleva, o 2 doprava, o 4 doprava. Tedy od R odečteme 3, od S odečteme 1, k C přičteme 2 a k H přičteme 4. Dostaneme OREL.

Úloha 4

$y = \log_2 x, \quad x \in \langle 0,5; 2,5 \rangle$ $y = -\log_2(x+1) + 1, \quad x \in \langle 0,5; 3 \rangle$ $y = \log_2(-(x-3)) + 2, \quad x \in \langle 1; 2,5 \rangle$ $y = \log_2(x-0,5) + 4, \quad y \in \langle -1; 3 \rangle$	$y = \log_2(x-0,5) + 4, \quad y \in \langle -2; 3 \rangle$ $y = \log_2(-(x-3)) + 2, \quad y \in \langle -2; 3 \rangle$ $y = -\log_2(x+1) + 1, \quad x \in \langle 0,5; 3 \rangle$	$y = \log_2(x-0,5) + 4, \quad y \in \langle -1,5; 1,5 \rangle$ $y = -\log_2(x+1) + 1, \quad x \in \langle 0,5; 2,5 \rangle$ $y = \log_2 x, \quad x \in \langle 1; 2,5 \rangle$
--	---	--

Pokyny: Jsou zadány 3 skupiny funkcí. Pod nimi jsou dvě souřadné soustavy, pro řešení však stačí použít jednu z nich, druhá je „rezervní“.

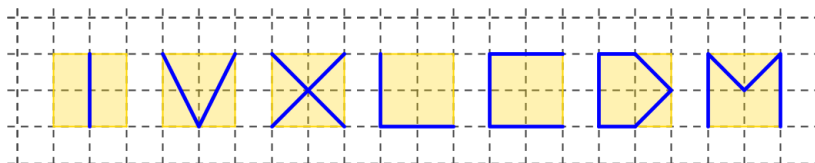
Řešení: Grafy funkcí v jednotlivých skupinách vykreslují písmena slova RAK. Grafy funkcí jsou na obrázku vpravo.



Pracovní list 6 – Římské číslice

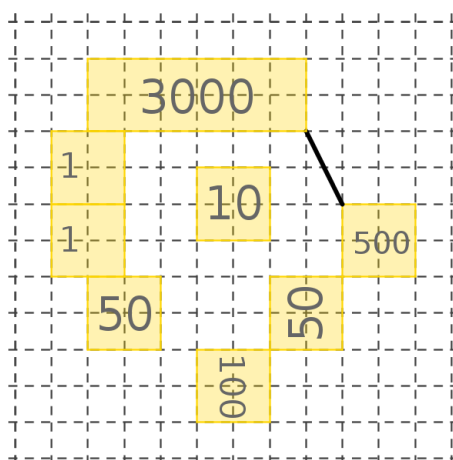
Úlohy

Do čtvercové sítě budeme zakreslovat čísla zapsaná římskými číslicemi. Tvary jednotlivých číslic jsou následující:

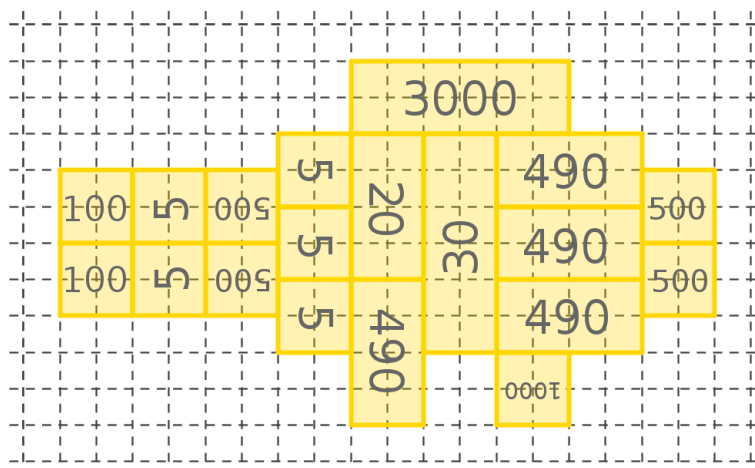


Každá číslice vždy zabírá svůj vlastní čtvereček!

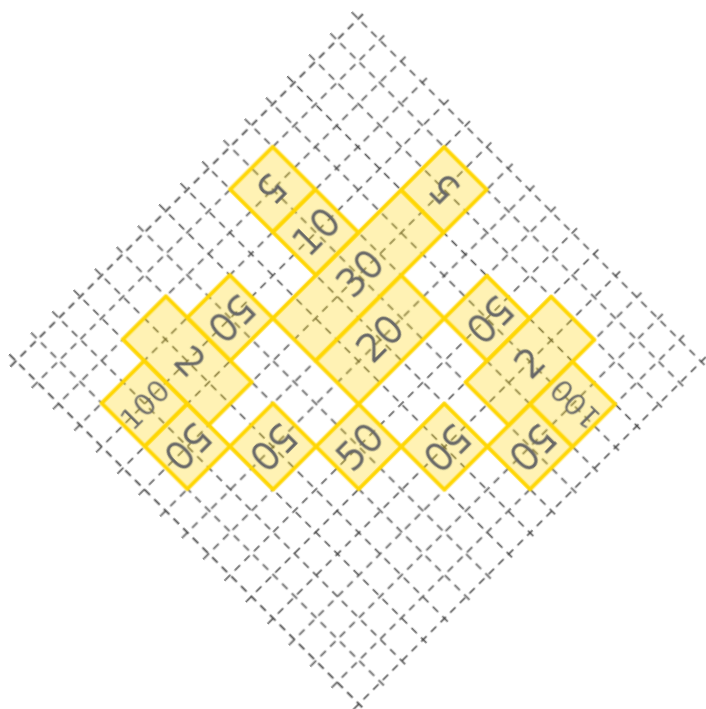
Úloha 1



Úloha 2

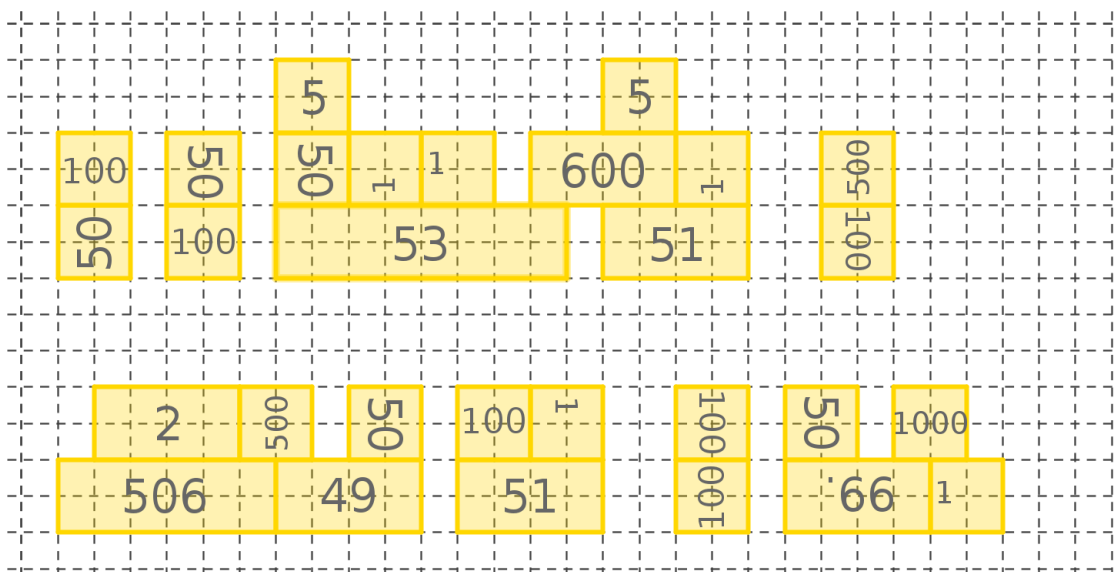


Úloha 3



Úloha 4

V obrázku je číslo 99, ne 66!



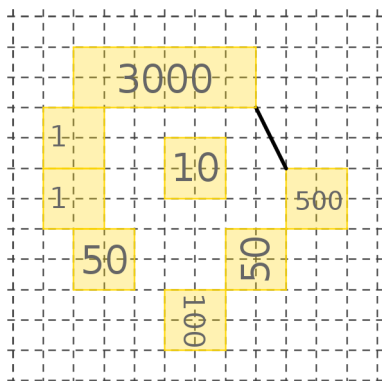
Pracovní list 6 – Římské číslice

Řešení a návod pro učitele

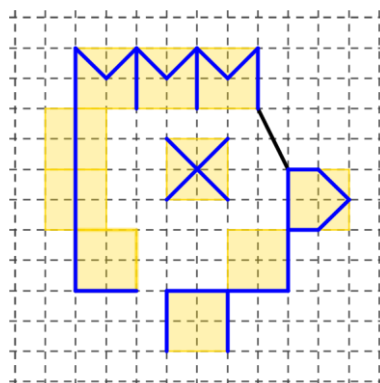
Kromě pracovního listu je vhodné připravit i náhradní psací potřeby (pastelky či tenké fixy) a čtverečkový papír pro závěrečnou aktivitu.

Římské číslice je třeba psát podle předkreslených vzorů a ve směru, jak jsou čísla v obrázcích zapsána.

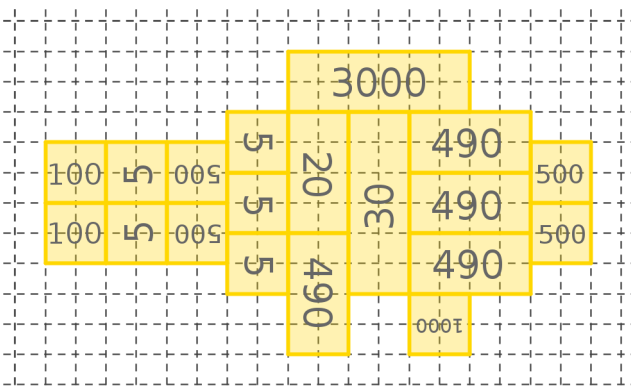
Úloha 1



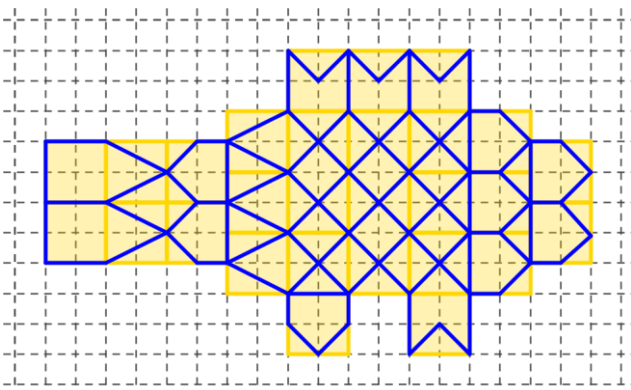
Řešení: HLAVA SLEPICE



Úloha 2

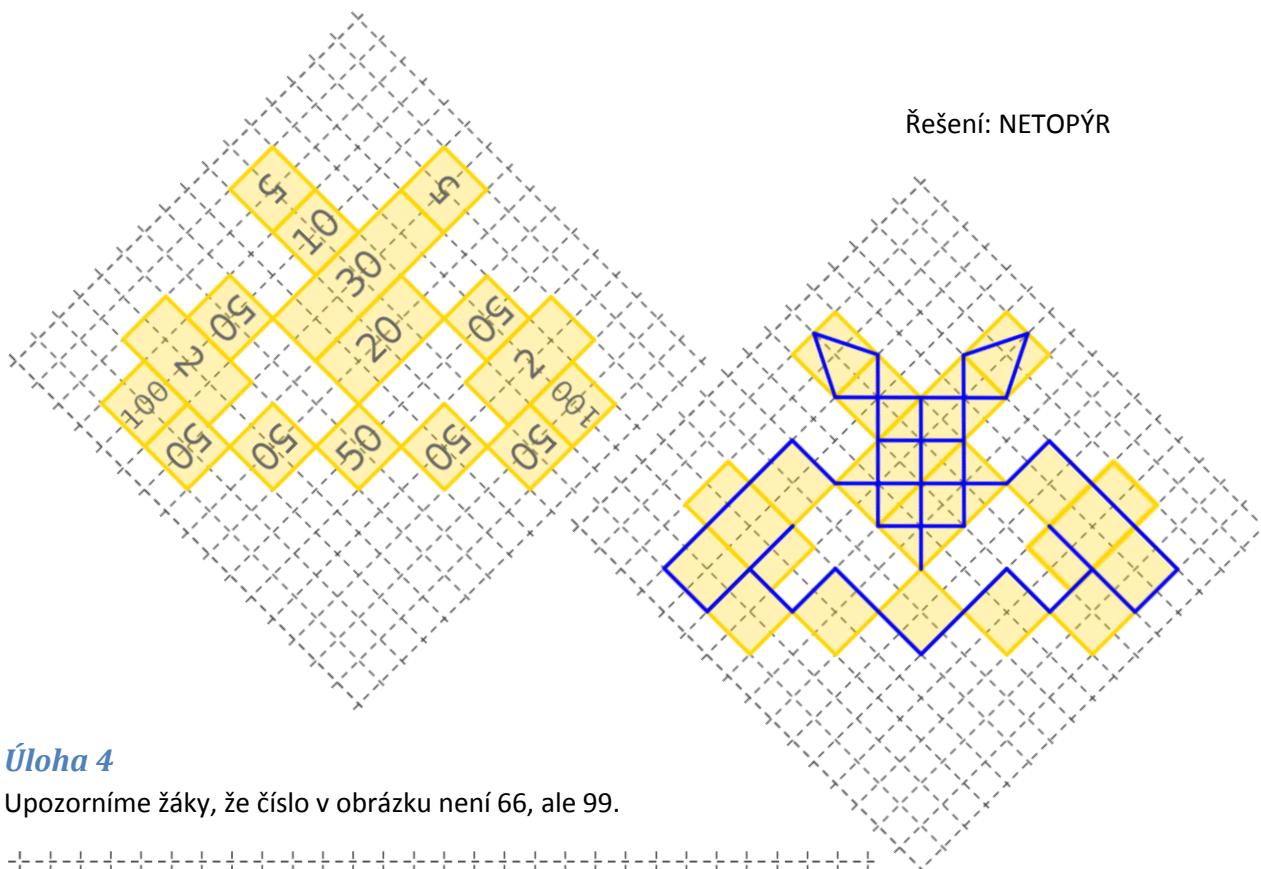


Řešení: RYBA



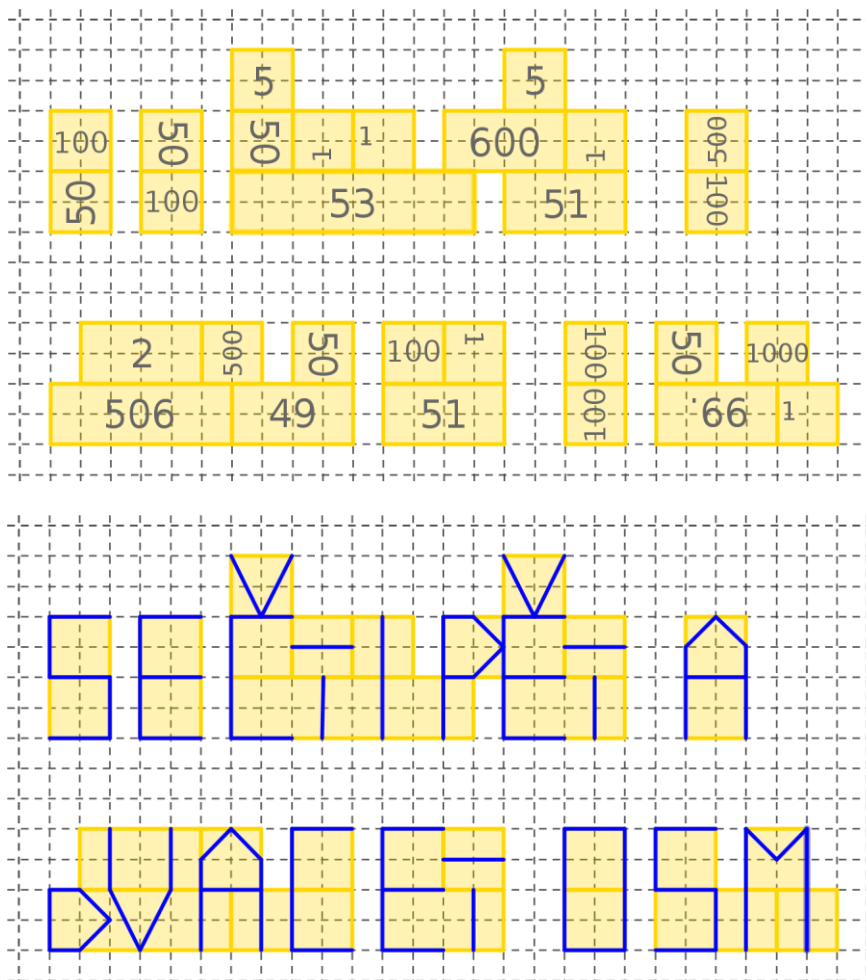
Úloha 3

Řešení: NETOPÝR



Úloha 4

Upozorníme žáky, že číslo v obrázku není 66, ale 99.



Závěrečná aktivita

Žáci se rozdělí do skupin (dvojic) a vytvářejí vlastní obrázky složené z římských číslic. Pracují na čtverečkováném papíře. Vždy jeden žák vytvoří zadání obrázku a předá je jinému žáku ze skupiny. Ten obrázek pak vypracuje.

Rejstřík

A

abeceda

- binární, 14
- mezinárodní, 8
- otevřeného textu, 8
- šifrová, 8
- asociační šifra, 15

B

- Braillovo písmo, 14

C

- Caesarova šifra, 8

F

- frekvenční analýza, 10, 72

G

- grafická šifra, 16

J

- jezdcova procházka, 17

K

- klamač, 10
- kód, 11
 - čárový, 12
- kódování, 11, 73
 - barev, 12
 - znaků v počítači, 12
- kryptologie, 7

M

- Morseova abeceda, 12
 - pomocná slova, 13

O

- otočná mřížka, 18

P

- Playfairova šifra, 18
- plot, 15
- polský kříž, 18
 - malý, 18
 - velký, 18
- Polybiův čtverec, 10
- posun, 8
 - pomocí klíče, 9
- předměty, 16
- přičítání klíče, 11

S

- steganografie, 7
- substituce, 8, 72
 - jednoduchá monoalfabetická, 8, 72
 - polyalfabetická, 11

Š

- šifrovací algoritmus, 8
- šifrovací klíč, 8
- šifrovací systém, 8
- šifry využívající schémata, 17

T

- tabulka, 17
- transpozice, 15, 70

U

- úvodní šifra, 20

V

- víceúrovňová šifra, 19
- Vinegèrova šifra, 11

Z

- závěrečná šifra, 21

Bibliografie

- [1] S. Singh, Kniha kódů a šifer: tajná komunikace od starého Egypta po kvantovou kryptografii, Praha: Dokořán, 2009.
- [2] A. Hodges, „Alan Turing: a short biography - 1,“ [Online]. Available: <http://www.turing.org.uk/>. [Přístup získán 28 července 2014].
- [3] J. J. O'Connor a E. F. Robertson, „Rejewski biography,“ [Online]. Available: <http://www-history.mcs.st-and.ac.uk/history/Biographies/Rejewski.html>. [Přístup získán 28 Červenec 2014].
- [4] „Dantem - generátor čárových kódů,“ [Online]. Available: <http://www.dantem.cz/reseni/generator-carovych-kodu/>. [Přístup získán 28 července 2014].
- [5] „QRgenerator.cz - QR kód, QR generátor,“ [Online]. Available: <http://www.qrgenerator.cz/>. [Přístup získán 28 července 2014].
- [6] „Morseova abeceda,“ [Online]. Available: https://cs.wikipedia.org/wiki/Morseova_abeceda. [Přístup získán 30 července 2014].
- [7] „12.pdf,“ [Online]. Available: <http://www.noctapuru.cz/sifry/2011/12.pdf>. [Přístup získán 5 srpna 2014].
- [8] „Noc tapürů,“ [Online]. Available: <http://www.noctapuru.cz/2011/reseni>. [Přístup získán 5 srpna 2014].
- [9] R. Pelánek (ed.), „Almanach TMOU,“ 2008. [Online]. Available: http://www.radekpelanek.cz/dokumenty/tmou_almanach.pdf. [Přístup získán 11 srpna 2014].