Pedagogická fakulta
Faculty of Education
Jihočeská univerzita v Českých Budějovicích
University of South Bohemia in České Budějovice

Jihočeská univerzita v Českých Budějovicích
Pedagogická fakulta
Katedra matematiky

Diplomová práce

Šifry ve výuce matematiky na 1. stupni základní školy

Vypracovala: Kateřina Boučková
Vedoucí práce: doc. RNDr. Helena Koldová, Ph.D.

České Budějovice 2021

Prohlášení

Prohlašuji, že svoji diplomovou práci na téma Šifry ve výuce matematiky na 1. stupni základní školy jsem vypracovala samostatně pouze s použitím pramenů a literatury uvedených v seznamu citované literatury.

Prohlašuji, že v souladu s § 47b zákona č. 111/1998 Sb. v platném znění souhlasím se zveřejněním své diplomové práce, a to v nezkrácené podobě, elektronickou cestou ve veřejně přístupné části databáze STAG provozované Jihočeskou univerzitou v Českých Budějovicích na jejích internetových stránkách, a to se zachováním mého autorského práva k odevzdanému textu této kvalifikační práce. Souhlasím dále s tím, aby toutéž elektronickou cestou byly v souladu s uvedeným ustanovením zákona č. 111/1998 Sb. zveřejněny posudky školitele a oponentů práce i záznam o průběhu a výsledku obhajoby kvalifikační práce. Rovněž souhlasím s porovnáním textu mé kvalifikační práce s databází kvalifikačních prací Theses.cz provozovanou Národním registrem vysokoškolských kvalifikačních prací a systémem na odhalování plagiátů.

V Českých Budějovicích 13. dubna 2021

Poděkování

V prvé řadě bych chtěla moc poděkovat mé vedoucí práce, paní doc. RNDr. Heleně Koldové, Ph.D., za konzultace a její odborné rady a připomínky při tvorbě diplomové práce. Také bych tímto chtěla poděkovat paní ředitelce ZŠ a MŠ Chlum, paní Mgr. Jaroslavě Procházkové, která mi umožnila vyzkoušet mé pracovní listy v praxi. A v neposlední řadě všem třídním učitelkám ZŠ a MŠ Chlum za poskytnutý prostor a čas ve svých třídách a za jejich užitečné rady a zkušenosti.

Abstrakt

Název: Šifry ve výuce matematiky na 1. stupni základní školy

Diplomová práce s názvem Šifry ve výuce matematiky na 1. stupni základní školy seznamuje čtenáře se základními pojmy týkajících se šifrování, dále také s historií šifer od počátku do současnosti, jejich rozdělením, návazností na rámcově vzdělávací program pro základní vzdělávání a s didaktickou hrou. Dále se zabývá seznámením dětí s jednoduchými šiframi a s jejich šifrováním a dešifrováním. Práce je rozdělena na dvě části, a to teoretickou a praktickou. Teoretická část představuje šifry a jejich využití, základní pojmy, druhy šifer, historii šifer, šifrovací hry a didaktickou hru. Praktická část zahrnuje pracovní listy a didaktické hry, které obsahují jednoduché šifry. Ke každému pracovnímu listu je vytvořen návod použití, řešení, samotné šifry a u vyzkoušených pracovních listů v praxi je napsáno zhodnocení, jak si děti vedly, jejich špatná, ale i správná řešení.

Klíčová slova: šifry, historie šifer, šifrovací hry, didaktická hra, matematika

Abstract

Title: Ciphers in mathematics education at primary school

The diploma thesis “Ciphers in mathematics education at primary school” acquaints readers with basic concepts related to encryption, as well as with the history of ciphers from the beginning to the present, their classification, connection to the framework educational program for primary school and didactic game. It also deals with introducing simple ciphers to children and their encryption and decryption. The work is divided into two parts, theoretical and practical. The theoretical part presents ciphers and their use, basic concepts, types of ciphers, history of ciphers, cryptographic games and didactic game. The practical part includes worksheets and didactic games that contain simple ciphers. Each worksheet contains instructions for use, solutions and the ciphers themselves. Some of the worksheets were tested by children and therefor there is also an evaluation of how the children performed – with the wrong and also correct solutions.

Keywords: ciphers, history of ciphers, cryptographic games, didactic game, mathematics

Obsah

1 Úvod

Již po staletí mají lidé potřebu mezi sebou komunikovat. Jak čas plynul, lidé zjistili, že je často lepší, když jejich komunikaci nemůže nikdo cizí narušit, kontrolovat nebo do ní dokonce vstupovat. A právě v té době začaly vznikat utajené komunikace, šifrování a dešifrování. Některá odhalení tajných komunikací dokonce vedlo k ukončení konfliktů a válek.

V dnešní moderními technologiemi přehlcené době je šifrování samozřejmostí. Setkáme se s ním například v podobě QR kódů, pinů, hesel, rozpoznání obličejů, otisků prstů nebo v obchodě v podobě čárových kódů. Znalost základních principů šifrovacích algoritmů by měla být v současnosti samozřejmostí nejen pro lidi pohybujících se v IT sektoru, ale i pro širší veřejnost.

V současném školství a vyučování matematiky bohužel na šifrování nezbývá v učebních plánech místo. Nenalezneme je tak v učebnicích ani v pracovních sešitech. Přitom šifrování a dešifrování pomáhá u dětí rozvíjet logické myšlení, rozšiřuje obzory a znalosti v historii a navíc u různých druhů šifer dochází k propojení mezipředmětových vztahů, například s českým jazykem, literaturou a dějepisem.

2 Cíl a metodologie práce

2.1 Cíl

Cílem diplomové práce je seznámit pedagogy se základními a jednoduchými šiframi, které lze použít zábavnou formou v hodinách matematiky na 1. stupni základní školy. Pedagogové by měli být namotivováni k zařazení tohoto tématu do výuky. Dále je cílem vytvořit sadu pracovních listů, pomocí kterých se děti seznámí zábavnou formou s různými druhy šifer z minulosti, ale i současnosti a naučí se, jak dešifrovat daný text a zašifrovat vlastní myšlenky a slova.

Ke splnění cílů výše jsou určeny následující dílčí cíle:

- Na základě odborné literatury popsat základní šifry, jejich historii, šifrovací hry a didaktické hry.
- Vytvořit pracovní listy a didaktické hry, které obsahují jednoduché šifry odpovídající učivu na 1. stupni základní školy.
- Zapracovat zkušenosti z praxe, tedy ze zadávání pracovních listů ve třídách.

Diplomová práce je rozdělena na dvě části, a to teoretickou a praktickou. Teoretická část se na základě studia příslušné odborné literatury zabývá základními pojmy z tématu šifer, dále definuje druhy šifer, stručně seznamuje s historií šifer, snaží se vysvětlit návaznosti na rámcově vzdělávací program a popisuje didaktickou hru.

Praktická část se zaměřuje na tvorbu pracovních listů a didaktických her. Popisuje, jak s pracovními listy pracovat nebo jak didaktické hry organizovat, zmiňuje postupy správných řešení. Obsahuje potřebné šifry k didaktickým hrám a samotné pracovní listy, které jsou určeny přímo pro žáky na 1. stupni základní školy. U některých pracovních listů, které byly vyzkoušeny v praxi, se nachází zhodnocení řešení žáků, poznámky a fotografie.

2.2 Metodologie práce

Diplomová práce s názvem Šifry ve výuce matematiky na 1. stupni základní školy je didaktická práce, která je zaměřena na vytvoření souboru pracovních listů, které žáky seznámí zábavným způsobem s různými druhy šifer, které se objevily během historie.

K jejich vytvoření je třeba se seznámit s různými druhy historických šifer – s jejich šifrováním a dešifrováním a nakonec tyto šifry zjednodušeným způsobem zapracovat do jednotlivých pracovních listů tak, aby je pochopili i žáci od 1. do 5. ročníku a uměli jejich šifrování i dešifrování použít i v praxi.

Teoretická část je vypracována na základě literární rešerše a využívá metodu deskripce. Ke zpracování jsou využita sekundární data z oblasti kryptologie a šifer. Informace jsou získávány zejména z odborné literatury a internetových zdrojů. K vypracování literární rešerše je využit jak pohled českých, tak i zahraničních autorů.

Praktická část je zpracována na základě poznatků získaných v teoretické části, a to zejména týkajících se historických druhů šifer. Historické druhy šifer byly zapracovány do tří pracovních listů, které jsou vytvořeny jako didaktická hra a je k nim třeba pohyb po třídě, škole, ale i přírodě a do pěti pracovních listů, které seznamují s určitým druhem šifry. Některé pracovní listy byly vyzkoušeny v praxi, a na základě metody pozorování bylo zjišťováno, jak si žáci jednotlivých tříd vedou s jejich řešením. Dva pracovní listy byly zadány přímo ve třídě a byla tak získána okamžitá zpětná vazba – výsledky práce jednotlivých žáků, jejich myšlení, postupy, problémy, zdary, ale i nezdary. Další dva pracovní listy byly vzhledem k epidemiologické situaci zadány pouze distančně, tudíž není zaručena samostatnost žáků při práci, i když o ni bylo při zadávání žádáno. Z důvodu epidemie nedošlo k zadání více pracovních listů, především těch s didaktickou hrou. Pracovní listy budou řádně vyzkoušeny, až se epidemiologická situace zlepší.

3 Teoretická východiska

V teoretické části práce jsou definovány základní pojmy související s šiframi, jako je kryptologie, kryptografie, kódování, steganografie, hašovací funkce a šifrovací algoritmus. Dále jsou definovány druhy šifer. Teoretická část se také věnuje historii šifer od starověku až do současnosti. V neposlední řadě teoretická část definuje pojmy šifrovací hra, kurikulum a didaktická hra.

3.1 Základní pojmy

„Základním použitím šifer je přenos tajné informace z jednoho místa na druhé.“ (Hanžl, Pelánek, Výborný, 2007, s. 10)

Dříve se šifry používaly především k vojenským účelům, v 19. století se rozšířilo jejich použití do obchodní sféry a na konci 20. století se staly součástí každodenního života všech lidí, kteří používají moderní technologie. Šifry dnes slouží nejen k posílání tajných zpráv, ale využívají se také při uchovávání dokumentů nebo k identifikaci. Dalším způsobem použití šifer je ve hrách jako nástroj zábavy, rozvoje logického myšlení, empatie a technického myšlení. (Hanžl, Pelánek, Výborný, 2007)

3.1.1 Kryptologie

„Kryptologie není naukou o kryptách, jak si hodně lidí myslí, ale o šifrách, a její vliv na světovou historii je fascinující.“ (Singh, 2003, s. 9)

Dle Janečka (1994) je kryptologie věda o šifrách, která je složena ze tří částí: kryptografie, luštění šifer a kryptoanalýzy. Její historie začala již v roce 1900 př. n. l., kdy se ve starém Egyptě začaly používat hieroglyfy. Šifry se pak dále rozvíjely hlavně díky starým Řekům, kteří zdokumentovali vznik prvního transpozičního šifrovacího systému. (Janeček, 1994)

Pazourek v knize Rekreační šifrování (2014) uvádí, že *„Kryptologie je nauka o utajení smyslu zprávy. Dělí se na kryptografii zabývající se tvorbou systému na utajení smyslu zprávy a samotnou kryptologii, jejímž cílem je luštění zpráv bez znalosti systému, popřípadě hesla či klíče.“* (Pazourek, 2014, s. 7)

Piper (2006) definuje kryptologii jako vědu, která se zabývá kryptografií a kryptoanalýzou. Kryptografie se zabývá tvořením šifer. (Piper, 2006)

3.1.2 Kryptografie

Kryptografie pochází z řeckého slova *kryptos* (skrytý). Její cíl není jako u steganografie ukrýt, že zpráva existuje, ale utajit její význam a to tím, že se zpráva zašifruje pomocí šifrování. (Singh, 2003)

3.1.3 Šifrování versus kódování

Tyto pojmy jsou si blízké, ale odlišuje je veliký rozdíl. Šifrování znamená, že provádíme šifrovací algoritmus, tedy transformujeme informace a použijeme k tomu tajný klíč. Kódování také transformuje informace, ale nepoužívá žádné utajené informace. (Jiroušek, 2006)

„Hlavním účelem kódování je převod mezi dvěma abecedami či obecněji dvěma způsoby zápisu zprávy“. (Hanžl, Pelánek, Výborný, 2007, s. 67)

Základem kódování je abeceda. Je důležité si určit, kterou abecedu pro šifrování budeme používat, je totiž více možností. Hanžl, Pelánek a Výborný (2007) rozdělují abecedu na anglickou abecedu, která má 26 znaků, plnou českou abecedu, která má 42 znaků a není moc používána, anglickou abecedu s písmenem ch, která obsahuje 27 znaků, a anglickou abecedu se sjednocenými písmeny i a j, která má 25 znaků. V této abecedě je používáno i místo j, kvůli malé frekvenci písmena j v anglickém jazyce. (Hanžl, Pelánek, Výborný, 2007)

3.1.4 Steganografie

„Komunikace utajená pomocí ukrytí zprávy se nazývá steganografie, podle řeckých slov steganos (schovaný) a graphein (psát).“ (Singh, 2003, s. 20).

Steganografie se rozvíjela během tisíců let. Například ve staré Číně psali na jemné hedvábí, ze kterého poté udělali kuličku, polili ho voskem a nakonec spolkli. Ital Giovanni Porta v 16. století vysvětlil, jak se dá tajná zpráva předat pomocí uvařeného vejce natvrdo a inkoustu vyrobeného z octa a kamence. Napsaný text se napíše na skořápku. Když chceme zprávu přečíst, tak musíme vejce oloupat a přečíst, co je

na bílku. Do steganografie patří i neviditelné inkousty. Stenografie má však jednu zásadní vlastnost – když člověk zprávu jednou objeví, tak je prozrazena naráz. (Singh, 2003)

3.1.5 Hašovací funkce

Hašovací funkce je funkce, kdy informace chceme pouze zašifrovat a víme, že je nikdy nebudeme potřebovat ani chtít dešifrovat. Její název pochází z anglického slova *hash*, také ji můžeme označovat haše funkce nebo označením digitální otisk. Tato funkce transformuje libovolně dlouhé posloupnosti binárních symbolů na určitou délku binární posloupnosti. (Přibyl, 2004)

Hašovací funkce má určité požadavky, které musí splňovat. Prvním požadavkem je, že musí mít pouze jeden směr, tedy že z hodnoty haše nelze odvodit zprávu, která byla původní. Dalším požadavkem je, že z hashe nelze vyvodit dvě různé zprávy. Haš funkce tedy musí být nekolizní. U hašovací funkce musí být stanovena minimální délka výsledného řetězce, který je zašifrovaný, aby funkce byla nekolizní. Aby bylo možné definovat délku haše, je využíván princip tzv. „narozeninového útoku“ *(birthday attack).* Tento útok je založen na principu, že v jedné místnosti, ve které roste počet osob, roste i pravděpodobnost, že v ten samý den budou mít dvě osoby z té jedné místnosti narozeniny. V praxi je to tak, že se zvyšujícím se počtem vstupních textů se zvětšuje pravděpodobnost, že dva texty, které jsou různé, mohou vytvořit stejný haš. Standartní délka haše je 160 bitů. Tato délka je používána také pro digitální podpisy. (Jašek, 2006)

3.1.6 Šifrovací algoritmus a klíč

„Každou šifru můžeme popsat pomocí obecné šifrovací metody, jíž říkáme algoritmus, a pomocí klíče, který specifikuje detaily použitého šifrování.“ (Singh, 2003, s. 25)

K tomu, aby odesílatel mohl zašifrovat zprávu, se používá šifrovací algoritmus, který musí být konktrétně daný pomocí nějakého klíče. Když se aplikuje klíč a šifrovací algoritmus na otevřený text, vznikne nám zašifrovaná tajná zpráva. Pokud příjemce zná klíč i algoritmus, dokáže zašifrovanou zprávu rozluštit a vytvořit z ní původní otevřený text. (Singh, 2003)

3.2 Druhy šifer

Hanžl, Pelánek a Výborný (2007) rozdělují druhy šifer na **jednoduché substituce,** které definuje jako substituce neboli nahrazení jednoho písmene za jiné písmeno či znak. U těchto šifer je originální text napsaný malými písmeny a vzniklá šifra zase velkými. Mezi tyto šifry patří například Caesarova šifra (pevný posun abecedy o tři místa), ROT13 (pevný posun abecedy o třináct míst) nebo také ATBASH (převrácená abeceda), affinní šifra (lineární transpozice) a šifry, které se převádí podle klíčového slova. Její slabé místo spočívá v zachování frekvence znaků.

Dalším druhem je **polyalfabetická substituce**. Je při ní použito několik šifrovacích abeced. Mezi nejznámější příklady patří Vigenerova šifra. Při této substituci je důležité, aby byl použit nekonečný náhodný klíč – nejlépe klíč, který je dlouhý stejně jako původní zpráva. Tento klíč je však bezpečné použít jenom jednou. Nevýhodou této šifry je předávání klíče mezi odesílatelem a adresátem.

Třetím druhem je **polygrafická substituce,** která zvyšuje bezpečnost tím, že se substituce neaplikuje na jednotlivá písmena, ale na bloky písmen. Jelikož je bloků více než jednotlivých písmen, tak je její analýza daleko náročnější. Mezi tyto šifry patří Playfair, bifid a Hillova šifra.

Dalším druhem jsou další substituce, mezi které patří **homofonní substituce.** U té platí, že jedno písmeno se může zobrazit na několik dalších písmen. Nevýhoda u této substituce je, že klíč je více komplikovaný a tím pádem není lehké si ho zapamatovat. Dále sem patří také **klamače, nomenklátory, zkomoleniny,** což jsou kombinované kódy se substitučními šiframi. Některým slovům, která jsou frekventovaná, se přiřadí speciální symbol a těmto slovům říkáme nomenklátory. Šifru lze ještě ztížit tím, že použijeme tzv. klamače – znaky, které nemají význam.

Další druh šifer se nazývá **transpozice dle klíče a mřížky.** Mřížka je vytvořena například z tvrdého papíru a má tvar čtverce. Nejprve se do mřížky vyřežou volná políčka. Mřížka se přiloží k jinému čtverci a do volných políček se napíše zpráva. Do zbytku se napíšou náhodná písmena. Zpráva je rozšifrována pomocí přiložení dané mřížky.

V seznamu druhů následují **produktové šifry,** které jsou založeny na použití kombinace více šifer. Zpráva je zašifrována pomocí jedné šifry a poté ještě pomocí druhé.

Šifrování i dešifrování je proto mnohem složitější a náročnější. Příkladem této šifry je šifra ADFGX, která byla použita Němci v první světové válce. (Hanžl, Pelánek, Výborný, 2007)

3.3 Historie šifer

„Králové, královny a generálové po tisíce let spoléhali na účinné komunikační systémy, jež jim umožňovaly vládnout jejich zemím a velet armádám. Zároveň si vždy byli vědomi, jaké následky by mělo, kdyby jejich zprávy padly do nepovolaných rukou.“ (Singh, 2003, s. 12)

Díky obavám o prozrazení tajných komunikací došlo k rozvoji kódů a šifer, tedy technik, které jsou určené k utajení zprávy před těmi, kterým zpráva nebyla určena. Během historie velké množství lidí pracovalo na co nejbezpečnějším způsobu zašifrování tajných zpráv a naopak na rozluštění cizích šifer. (Singh, 2003)

3.3.1 Starověk

Skytalé

Skytalé (též uváděno anglicky *scytale*) bylo první vojenské šifrovací zařízení, které používali ve Spartě (viz obr. 1). Jednalo se o dřevěnou tyč, kolem které se ovinul proužek pergamenu nebo papíru. Odesílatel poté napsal tajnou zprávu podél tyče a kus papíru odmotal. Na proužku papíru tak vznikly po sobě jdoucí nic neříkající písmena. Příjemce pak zprávu rozluští tak, že ovine proužek papíru na tyč o stejném průměru, který použil původní odesílatel. Tato šifra pomohla k výhře Sparťanů v roce 404 př. n. l., kdy ke králi Sparty dorazil zraněný posel a předal mu zašifrovanou zprávu, kterou král navinutím na tyč o stejném průměru rozluštil a dozvěděl se o plánu perského Farnabazuse na Spartu zaútočit. Díky této zprávě se král Sparty na útok připravil a útok odrazil. (Singh, 2003)

Obrázek 1 Skytalé

Zdroj: wikipedia.org, 2021a

Polybiův čtverec

Další šifrovací metodou, kterou popsal řek Polybios, se nazývá **Polybiův čtverec** nebo také **Polybiova šachovnice**. Vzniká v době kolem 2. století př. n. l. Při této metodě se používá čtverec veliký 5x5, ve kterém je postupně napsána abeceda (viz obr. 2). Písmeno J bývá nahrazeno I nebo může být i varianta, kdy se píše U místo V nebo V místo W. Dále pak mají jednotlivé řádky a sloupce daná čísla. Text zašifrujeme tak, že písmeno vyměníme za dvě číslice, první odpovídá řádku a druhá sloupci. (Prokopič, 2008)

	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

Obrázek 2 Polybiův čtverec

Zdroj: vlastní zpracování

Ceasarova šifra

Caesarova šifra je první zdokumentovaná substituční šifra, která byla použita pro vojenské účely. Jednalo se o posun písmen v abecedě o tři místa dále. Často se používají termíny otevřená abeceda pro původní text a šifrovací abeceda pro znaky, který text tvoří. Pojem Caesarova šifra ovšem nezahrnuje pouze posun o tři pozice, ale je možné použít

posun o jakýkoli počet míst, tzn. od 1 do 25, a tím je možné vytvořit 25 různých šifer. (Singh, 2003)

Například mam rad sifry → PDP UDG VLIUB (posun o tři místa).

„V kryptografii existuje konvence zapisovat znaky otevřené abecedy malými a znaky šifrované abecedy velkými písmeny. Podobně se původní zpráva – otevřený text – píše malými písmeny, zatímco zašifrovaná zpráva – šifrový text – velkými.“ (Singh, 2003, s. 25)

3.3.2 Středověk a raný novověk

Atbaš

V letech 800 až 1200 n. l. probíhalo u Arabů období, kdy se rozvíjela vzdělanost a intelekt. V té samé době se Evropa potýkala teprve se základy kryptografie. Ve Starém zákoně mniši nalezli úseky šifrovaného textu, který byl zašifrován pomocí hebrejské substituční šifry atbaš. Její princip je založen na výměně písmen. Určí se jedno písmeno, které chceme použít, spočítáme, na kolikátém místě se nachází od začátku abecedy, a nahradíme ho písmenem, které je vzdáleno od konce abecedy o stejný počet písmen. (Singh, 2003)

„Sám název šifry atbaš napovídá, jak systém funguje, protože se skládá (ATBŠ) z prvního písmene hebrejské abecedy (alef), po němž následuje poslední (tav), poté druhé písmeno (bet) a nakonec předposlední (šin)“ (Singh, 2003, s. 39)

Vigenerova šifra

Vigenerova šifra začala vznikat v druhé polovině 15. století, kdy Ital jménem Leon Battista Alberti dostal nápad na vytvoření nové substituční šifry, která nepoužívala pouze jednu šifrovou abecedu, ale použila pravidelné střídání dvou a více šifrovacích abeced. Výhodou této šifry je, že když se písmeno opakovaně vyskytuje v otevřeném textu, nemusí docházet k opakovanému výskytu v šifrovaném textu. Bohužel Alberti dále tuto šifru nerozvinul, a tak na něj navázal Johannes Trithemius, dále pak Giovanni Prota a nakonec Blaise de Vigenere, který byl francouzským diplomatem a narodil se v první polovině 16. století. Tento muž šifru dopracoval do konečné podoby, proto také nese jeho jméno. Vigenerova šifra k zašifrování používá 26 různých šifrových abeced.

Alberti ke své nové substituční šifře vynalezl pomůcku, tzv. *scrambler*, který dokázal převádět text do jeho šifrované podoby znak po znaku. Tento Albertiho disk (viz obr. 3) byl vytvořen ze dvou kotoučů z mědi, jeden byl větší – stacionární a druhý menší – otočný. Oba kotouče jsou rozdělené do buněk, na kterých jsou písmena abecedy v běžném pořadí. Výhody tohoto disku se plně projevily až u Vigenerovy šifry. Disk byl později nahrazen složitou Vigenerovou tabulkou. (wikipedia.org, 2021b)

Obrázek 3 Albertiho disk

Zdroj: crypto-world.info, 2006

Prvním krokem k šifrování Vigenerovy šifry je vypsání tzv. Vigenerova čtverce (viz obr. 4), „*což je otevřená abeceda následovaná 26 šifrovými abecedami, z nichž každá je vůči předchozí posunuta o jedno písmeno. První řádek tedy odpovídá šifrové abecedě s Caesarovým posunem 1“*. (Singh, 2003, s. 58).

Princip Vigenerovy šifry je založen na tom, že pro zakódování jednotlivých písmen je použit jiný řádek čtverce, což znamená jinou šifrovou abecedu. K dešifrování textu je třeba vědět, jaký řádek odesílatel použil na jednotlivá písmena, tedy musí být předem daný a dohodnutý systém. Její výhodou je odolnost vůči frekvenční analýze a velké množství klíčů. (Singh, 2003)

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

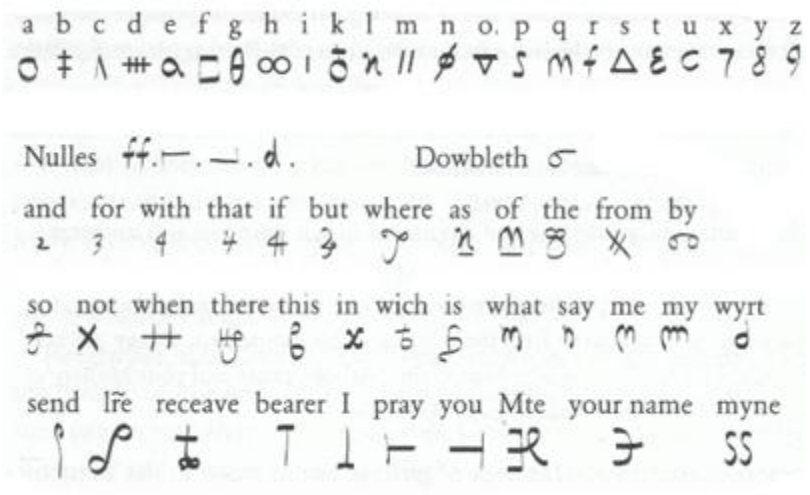
Obrázek 4 Vigenerův čtverec

Zdroj: wikipedia.org, 2021c

Šifra Marie Stuartovny

Dne 15. října 1586 byla Marie Stuartovna, skotská královna, obviněna z velezrady. Byla souzena za spiknutí proti královně Alžbětě, kterou údajně chtěla se svými spojenci zavraždit. U soudu ovšem žalobci neměli žádné pádné důkazy, jelikož její veškerá korespondence se spiklenci byla zašifrována do symbolů. Šifra nebyla typickou substitucí, spíše nomenklátorem (viz obr. 5). Byla vytvořena z 23 symbolů, které nahrazovaly písmena abecedy bez použití písmen j, v a w, a z 35 symbolů, které znázorňovaly slova či fráze. Naneštěstí dopisy byly díky zradě jednoho ze spiklenců doručeny ke dvoru královny Alžběty a byly rozluštěny Thomasem Phelippesem, a tak byla Marie Stuartovna odsouzena k smrti. Popravena byla 8. února 1587. (Singh, 2003)

„Nebylo to poprvé, kdy síla šifry rozhodovala o životě a smrti.“ (Singh, 2003, s. 19)



Obrázek 5 Nomenklátor Marie Stuartovny

Zdroj: svethardware.cz, 2009

Cardanova mřížka

V 16. století vznikl díky renesančnímu matematikovi, fyzikovi, lékaři, astrologovi a filosofovi Jeronýmu Cardanovi nový způsob šifrování. Bylo k němu potřeba šifrovací mřížky, což byla destička, která měla tvar čtverce, a byly v ní na určitých místech vyřezané otvory. Šifrování probíhalo tak, že se přiložila mřížka na papír, do vyřezaných míst se napsal daný text a po sejmutí mřížky se do zbytku volných míst zapsala libovolně písmena nebo symboly. Pouze ten, kdo měl totožnou šifrovací mřížku, která byla klíčem k rozluštění, mohl po jejím přiložení šifrovaný text odhalit. Tato mřížka, které se dnes říká Cardanova mřížka, byla v průběhu několika let zdokonalována. Původně byla stabilní a zdokonalena byla tak, že se stala mřížkou otočnou, která dokáže zašifrovat text do čtyř různých poloh. Vznikne tak tajná zpráva, která je ve tvaru čtverce. Opět je k jejímu dešifrování potřeba totožná otočná mřížka. (epochtimes.cz, 2008)

Velká šifra

V 17. století se ve Francii zrodila Velká šifra, kterou vytvořili otec a syn Rossignolové a používal ji Ludvík XIV. Tato šifra byla velmi bezpečná, a tak po smrti obou Rossignolů upadla v zapomnění, protože ji nikdo nemohl rozluštit. Až v roce 1890 se dostala do rukou Étiennu Bazeriesovi, který se ji snažil rozluštit několik let, a nakonec se mu to povedlo. Byl tak první po dvou stech letech, který se dozvěděl tajemství Ludvíka

XIV. Velká šifra byla použita například na dokumenty, které se týkaly muže se železnou maskou. (Singh, 2003)

3.3.3 19. a 20. století

Morseova abeceda

Během 19. století vznikla Morseova abeceda (viz obr. 6) díky Samuelovi F. B. Morseovi. Nejde o klasickou šifru, ale o skupinu symbolů. Je určena pro komunikaci na dálku bez potřeby třetí osoby. (Hanžl, Pelánek, Výborný, 2007)

„Přiřazení teček a čárek jednotlivým písmenům bylo určeno na základě jejich frekvence v anglické abecedě – frekventovanější písmena mají kratší kódy.“ (Hanžl, Pelánek, Výborný, 2007, s. 68)

Nejprve se používala pro přenos telegrafem, později v rádiu a do roku 1996 byla používána na lodích k tísňovému volání. Tzv. morseovka se stále používá na velké vzdálenosti. V roce 2004 byl do morseovky přidán znak a to zavináč, takže díky ní se dokáží přenést i emailové adresy. (Hanžl, Pelánek, Výborný, 2007)

A ·–	J ·–––	S ···	1 ·———–
B –···	K –·–	T –	2 ··–––
C –·–·	L ·–··	U ··–	3 ···––
D –··	M ––	V ···–	4 ····–
E ·	N –·	W ·––	5 ·····
F ··–·	O –––	X –··–	6 –····
G ––·	P ·––·	Y –·––	7 ––···
H ····	Q ––·–	Z ––··	8 –––··
I ··	R ·–·	0 –––––	9 ––––·

Obrázek 6 Morseova abeceda

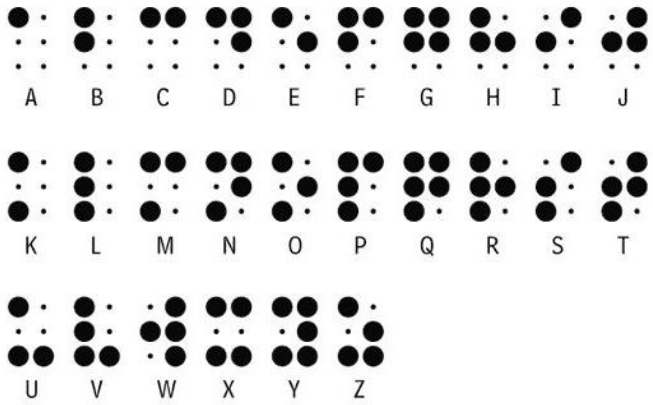
Zdroj: militaryrange.com, 2019

Braillovo písmo

„Braillovo písmo je určené pro nevidomé a je uzpůsobeno pro čtení hmatem. Písmena se skládají z různých kombinací šesti teček umístěných v obdélníku 2x3.“ (Hanžl, Pelánek, Výborný, 2007, s. 69)

V 19. století také vzniká Braillovo písmo (viz obr. 7), což je slepecké písmo, které pomáhá nevidomým lidem se vzděláváním a jejich rozvojem. Vymyslel ho malý chlapec jménem Louis Braille, který si jako tříletý poranil jedno oko a na druhé přestal vidět v pozdějším věku. Dlouhá léta však toto písmo učitelé odmítali, jelikož izolovalo nevidomé od vidomých. (Hanžl, Pelánek, Výborný, 2007)

„Braillova písmena jsou vytvořena ze dvou vertikálních sloupců o třech bodech. Rozměry písmen zhruba odpovídají rozměrům ukazováků, kterými se čte. Soustava je skutečnou abecedou rozměrem i obsahem. Je plně ortografická. Je proto rovnocenná kterémukoliv kulturnímu písmu. Má zvláštní znaky pro interpunkce i pro velká písmena, je ho možné použít i v jazycích, které mají písmena s diakritickými znaky. Je použitelná k zápisu každého jazyka, jak se později ukázalo i piktografického.“ (apogeum.info, 2006)



Obrázek 7 Braillovo písmo
Zdroj: svetloprosvet.cz, 2014

3.3.4 První světová válka

Během 1. světové války, i přes snahy kryptologů, nevznikla žádná šifra, která by nebyla prolomena. Všechny byly postupně odhaleny a rozšifrovány. (Singh, 2003)

Playfairova šifra

Playfairovu šifru v roce 1854 vymyslel Angličan Charles Wheatston a pojmenoval ji po jejím největším šiřiteli a svém dobrém příteli baronu Lyonu Playfairovi. (Piper, 2006) Dle Singha (2003) byla tato šifra ministerstvem zahraničí

odmítnuta pro svoji složitost. Nakonec ji ale Britové uplatnili v Búrské válce a první světové válce.

Zimmermannův telegram

Zimmermannův telegram je zpráva, která byla poslána německým ministrem zahraničí Arthurem Zimmermannem německému velvyslanci ve Washingtonu hraběti Johannu von Bernstorffu a byla zachycena a rozšifrována členy Room 40 (dešifrovací tým britské námořní admirality za první světové války). Bylo v ní napsáno, že Německo vyhlásí ponorkovou válku a blokádu Británie. (Piekalkiewicz, 2004)

Šifra ADFGX

Šifra ADFGX byla jednou z nejslavnějších německých šifer používána od roku 1918. Tato šifra je to kombinace substituce a transpozice. Podařilo se ji rozluštit francouzskému kryptoanalytikovi Georgesi Painvinovi. (Singh, 2003)

Vernamova šifra

Ke vzniku Vernamovi šifry na konci 1. světové války přispěli Američané a pro její základ použili Vigenerovu šifru, která měla cyklickou povahu. Inovace spočívala v tom, že délka klíče byla stejně dlouhá jako délka zprávy. (Singh, 2003)

Klíčem k Vernamově šifře mohou být zcela náhodné znaky nebo například kniha, na které se odesílatel a příjemce shodnou. V případě, že jde o klíč se zcela náhodnými znaky, označuje se tato šifra jako *one-time pad* a dodnes se používá, když je třeba předat tajnou zprávu. Jde totiž o tzv. perfektní kryptosystém, to znamená, že i když známe šifrovaný text, tak se nedozvíme nic o zprávě. Klíč hned po použití je třeba zničit, aby nedošlo k prozrazení zprávy ani v budoucnu. (Menezes, 1997)

3.3.5 Druhá světová válka

Enigma

Enigma (viz obr. 8) je šifrovací stroj, který byl používaný za 2. světové války. První patent na něj získal Artur Scherbius v roce 1918. Stroj vážil 12 kilogramů a měl podobu kompaktní skříňky. Pro jeho vysokou cenu o něj neměl ze začátku nikdo zájem. Němci ho docenili až v roce 1923, kdy napomohl k rozluštění dvojice britských

dokumentů. Stroj se skládá ze tří částí, které jsou vzájemně propojené: klávesnice, šifrovací jednotka a signální deska, která je tvořena lampičkami. Jeho nejdůležitější částí je *tzv. scrambler*, což je masivní gumový kotouč, který je protkaný dráty. (Singh, 2003)

„Po nějakou dobu se zdálo, že Enigma sehraje důležitou roli ve vítězství nacistů, nakonec se však významně podílela na Hitlerově pádu.“ (Singh, 2003, s. 140)

Z počátku se jevila enigma jako nerozluštitelná šifra. Velká řada lidí různých národností pracovala na jejím rozluštění. Nakonec se to povedlo díky Polákům a díky skupině kryptoanalytiků z Bletchley Parku, skupině složené z matematiků, lingvistů, specialistů na porcelán, kurátora pražského muzea a mistra v šachu a expertů na bridž. (Singh, 2003)

Obrázek 8 Enigma

Zdroj: svethardware.cz, 2017

3.3.6 Současnost

„Rozvoj šifrování ve 20. století souvisí také s morálními otázkami fungování demokratické a svobodné společnosti, konkrétně s rozporem mezi soukromím a bezpečností.“ (Hanžl, Pelánek, Výborný 2007, s. 22)

V dnešní době používá člověk šifrování neustále, a to ve všech možných oblastech. Například při nakupování na internetu, jelikož komunikace mezi nakupujícím a prodávajícím musí probíhat zašifrovaně, kvůli přenosu dat, které je možné snadno zachytit a zneužít. Dalším příkladem jsou mobilní telefony. Signál, který vysílá mobilní telefon, by se dal snadno zachytit a odposlouchávat, a proto jsou tyto signály zašifrovány.

Dále také identifikace uživatelů, které probíhají pomocí hesel a pinů se musí šifrovat, aby nemohlo dojít k jejich zneužití. Například i u identifikace u kreditní karty a bankomatů dochází k používání kryptografických protokolů. Stále více se v dnešní době používají elektronické podpisy, které se zajišťují s využitím šifer. (Hanžl, Pelánek, Výborný 2007)

Moderní šifry

„Klíčovým prvkem současného šifrování jsou počítače, které umožňují snadnou automatizaci mechanických početních úkonů, a tím poskytují novou dimenzi jak kryptografii, tak i kryptoanalýze.“ (Hanžl, Pelánek, Výborný, 2007, s. 95)

Příkladem moderní šifry jsou symetrické šifry. Patří mezi ně například Vernamova šifra, která je digitální podobou Vigenerovy šifry. Díky počítačům a technice bylo rozluštěno mnoho šifer, které se dříve jevily jako nerozluštitelné. Tyto šifry můžeme dělit na proudové šifry, u kterých jejich bezpečnost spočívá v nepravidelnosti klíče, který se nejprve vytvoří krátký, a z krátkého se vygeneruje dlouhý klíč a poté se teprve zpráva může zašifrovat. Proudové šifry jsou založeny na práci s bity. Druhým příkladem moderních šifer jsou blokové šifry, které jsou založeny na principu rozdělení zprávy na bloky pevné délky, které se poté šifrují samostatně. Patří sem polygrafické šifry jako je šifra Playfair (bloky délky 2) a bifid (bloky délky 5). (Hanžl, Pelánek, Výborný, 2007)

DES

Po druhé světové válce začala oblast kryptologie ještě více vzkvétat. Díky rozrůstajícímu počítačovému průmyslu vyvstala otázka, jak ochránit důležitá data, která dokáží po síti téct z jednoho počítače do druhého. Dříve se šifry používaly jen pro vládní, vojenské a špionážní účely, ale s vynálezem počítačů přišlo rozšíření a začaly je používat banky, úřady a poté je začali používat i podnikatelé. V roce 1975 byl tento systém uznán za standart a nechala si ho patentovat firma IBM a DES (Data Encryption Standard). DES byl kritizován kvůli délce klíče. Podle zaměstnanců Stanfordské univerzity se tato šifra dala prolomit pomocí stroje. Tento systém se však velice rychle rozšířil a byl oblíbený. V roce 1997 agentura RSA vyhlásila soutěž o rozluštění DESu. Podařilo se to za krátkých 5 měsíců. (Bitto, 2005)

AES

V roce 1997 byla vyhlášena soutěž, aby byl systém DES nahrazen. Vyhrál algoritmus Rijnadel, který vymysleli Belgičané Joan Deamen a Vincent Rijmen. Tento systém se nakonec nazval AES a v roce 2001 byl přijat za standart. (Bitto, 2005)

Shamirův algoritmus

Největší problém, který má symetrická šifra, je předání klíče. Adi Shamir proto vymyslel algoritmus, u kterého distribuce klíče nebyla třeba. Odesílatel zašifruje zprávu a pošle ji příjemci, který ji znovu zašifruje podle sebe a pošle zpět původnímu odesílateli. Ten zprávu rozšifruje podle svého klíče a pošle ji opět příjemci, který také použije svůj klíč a dostane tak původní zprávu. Problém je ovšem v tom, že je potřeba komutativní šifra a tu není jednoduché nalézt. (Bitto, 2005)

RSA

Zaměstnanci Stanfordovy univerzity, kteří kritizovali DES, popsali v Diffie-Hellmanově protokolu ideu prvočísel. Byl tak položen základ asymetrického šifrování. U těchto šifer jsou použity dva klíče. Jeden veřejný a druhý je soukromý. Problémem však bylo zabezpečit, aby se z veřejného klíče nedal odvodit ten soukromý. V roce 1977 se to konečně povedlo a vznikl tak algoritmus, který se nazýval RSA (Rivest, Shamir, Adleman – vynálezci). (Bitto, 2005)

Autentizační protokol

Kryptologie se v dnešní době používá i na ověřování identity neboli autentizaci. Máme tři způsoby, jak lze uživatele ověřit. Prvním způsobem je použití něčeho originálního, například hlasu nebo otisku prstů. Druhým způsobem je použití něčeho, co známe jenom my, například heslo nebo PIN. Třetí způsob autentizace je možný pomocí něčeho, co vlastníme jenom my, příkladem je identifikační karta. Při tomto procesu naše důvěrné informace kolují po síti a je důležité, aby nedošlo k jejich zneužití, proto se zde uplatňuje šifrování. (Bitto, 2005)

Čárové kódy

Čárové kódy jsou jedny z moderních kódů. V dnešní době jsou velice populární a používají se ve výrobních i nevýrobních oborech. Patří mezi optické technologie,

jelikož jejich princip je založen na vlastnostech tmavé a světlé plochy, které jsou rozdílné. Dále je k tomu třeba laserový paprsek, který tmavé a světlé plochy ozáří. (Sixta & Mačát, 2005)

Čárový kód (viz obr. 9) se objevil už v projektu výběru zboží z katalogu roku 1932. Skladník, který zboží vydával, měl speciální čtečku, kterou naskenoval kupón a zboží vydal. (Tihon, 2009)

Obrázek 9 Čárový kód

Zdroj: national-geographic.cz, 2012

QR kódy

QR kód (viz obr. 10) je druh čárového kódu, který patří do kategorie dvourozměrných. I když patří mezi čárové kódy, tak se neskládá z čar a mezer. Jeho konstrukce se skládá z černobílých bloků tvořících obrazce, které mají tvar čtverců. Lze s nimi přenést mnohem více informací než u klasického čárového kódu. Dokáží přenést kontaktní informace, textovou zprávu nebo webové stránky. Obrazce také obsahují informace, které jsou potřebné pro jejich dekódování, které probíhá pomocí QR čtečky. (eprin.cz, 2010)

Obrázek 10 QR kód

Zdroj: vytvořeno autorkou pomocí qr-code-generator.com

3.4 Šifrovací hry

„Šifry v hrách mají i výchovný efekt – procvičují trpělivost, soustředění, logické uvažování a také intuici, odhad či empatii.“ (Hanžl, Pelánek, Výborný, 2007, s. 27)

Šifry přitahují lidi nejen z profesionálního hlediska, ale také protože jsou pro ně skvělou výzvou a snaží se je pro zábavu rozluštit. Výzvy k prolomení šifer jsou mnohdy zveřejněny (například na internetu) a lidé pak při jejich luštění bojují o odměnu. Známou výzvu o rozluštění šifer vyhlásil i spisovatel Edgar Allan Poe. V jeho próze se objevovaly kryptologické prvky a on sám byl velmi dobrý luštitel. Edgar Allan Poe jednou vyzval své čtenáře, aby mu poslali šifry, které poté rozluštil a zveřejnil. Dále také zveřejnil dvě šifry, které kvůli nedostatku času nerozluštil a vyzval ostatní, aby se o to pokusili. Tyto šifry nikdo nerozluštil dalších 150 let. Až v roce 1992 byla rozluštěna první šifra a na tu druhou byla vypsána odměna 2500 dolarů. Nakonec byla prolomena v roce 2000. V knize, která vyšla v českém jazyce – Kniha kódů a šifer od s. Singha – nalezneme na konci výzvu, která obsahuje deset šifer, u kterých roste složitost. Tato výzva byla vyřešena 13 měsíců od jejího vydání. Některé výzvy v knihách dokonce ještě nejsou vyřešeny, například mechanický šifrovací systém *Chaocipher*. Šifry inspirovaly nejen spisovatele, ale i sochaře. Například Jim Sanborn vytvořil sochu „Kryptos“, která byla vytvořena pro agenturu CIA. Jsou na ní prvky různého šifrování. I když není dodnes tato šifra rozluštěna, tak velká část už je známa. (Hanžl, Pelánek, Výborný, 2007)

3.4.1 Příklady šifrovacích her

Příkladem šifrovacích her je například *Pokladovka.* Její pravidla jsou taková, že se v přírodě rozmístí různé šifry, které po vyřešení odkazují na polohu další šifry. Kdo se první dostane do cíle, vyhrává. Dalším příkladem je *Luštitelský pohár,* kdy se soutěžícím dá určitý počet šifer a časový limit, za který jich musí co nejvíce vyřešit. Další šifrovací hrou je *Šifrovací pohár,* kdy se děti rozdělí na týmy a každý tým vymyslí šifru, kterou se pak ostatní týmy snaží rozluštit. Mezi šifrovací hry patří i *Na Alici a Boba,* při které se hraje na týmy. Půlka týmu je Alice a druhá Bob. Úkol zní tak, že Alice musí předat zašifrovanou zprávu Bobovi dřív, než ji rozluští ostatní týmy. A posledním příkladem je hra s názvem *Poklad krále Ašóky,* při níž se v lese rozmístí texty, které musí hráči najít a rozluštit. (Hanžl, Pelánek, Výborný, 2007)

V současnosti si šifrovací hry získávají na popularitě. V České republice organizuje šifrovací hry například společnost Cryptomania s. r. o., která také vydává šifrovací hry jako stolní hry nebo on-line hry. Několik jejich her je venkovních. Šifrovací hry nabízí také jako téma netradičního teambuildingu. Dalším pořadatelem šifrovacích her po celé České republice jsou šifrovačky.cz. Venkovní týmové hry plné šifer pořádá i Silex, s. r.o. prostřednictvím svého webu chytra-zabava.cz. V zahraničí je oblíbený například webový portál CryptoClub (cryptoclub.org), který návštěvníky webu seznamuje s kryptologií a nabízí možnost hraní on-line šifrovacích her od lehké po těžkou obtížnost.

3.5 Kurikulum a rámcově vzdělávací program

Kurikulum definovala velká spousta autorů. Maňák (2008) charakterizuje kurikulum jako *„souhrn znalostí, které si má osvojit člen dané společnosti, odráží úroveň jejího rozvoje i potřeby života“.* (Maňák, 2008, s. 13)

Bečvářová (2003) ho ve své publikaci popisuje jako *„pohyb určitým směrem po určité cestě, k určitému cíli“* a jako *„pohyb, který doprovází dítě“*. (Bečvářová, 2003, s. 28)

Pojem kurikulum také nalezneme v pedagogickém slovníku, ve kterém se nachází hned tři jeho definice. První definicí je vzdělávací program, projekt nebo plán, druhou definicí je průběh studia a nakonec je pojem definován jako všechny získané zkušenosti ve škole. (Průcha, Walterová, Mareš, 2009)

Kurikulární dokumenty se v České republice tvoří na dvou úrovních, a to na úrovni státní a úrovni školní. Státní úroveň tvoří Národní program rozvoje vzdělávání, tedy Bílá kniha a také RVP (Rámcově vzdělávací programy), které jsou vytvořené pro všechny fáze vzdělávání – předškolní, základní, umělecké, jazykové a střední vzdělávání. (Svobodová, 2010)

Rámcově vzdělávací program je národní program, který udává strategie vzdělávání a vymezuje konkrétní závazné rámce. Rámcově vzdělávací program pro základní vzdělávání (RVP ZV) platí pro základní vzdělávání a z něj si jednotlivé školy vytváří vlastní školní vzdělávací programy. (nuv.cz, 2017)

Tato diplomová práce je zaměřena na oblast Matematika a její aplikace. *„Vzdělávací oblast Matematika a její aplikace je v základním vzdělávání založena především na aktivních činnostech, které jsou typické pro práci s matematickými objekty a pro užití matematiky v reálných situacích.“* (nuv.cz, 2017, s. 30)

Vzdělávací obsah je rozdělen na čtyři tematické okruhy. Prvním okruhem jsou Čísla a početní operace. Tento okruh je určen pro první stupeň. Na druhém stupni na něj navazuje Číslo a proměnná. Druhý tematický okruh je Závislosti, vztahy a práce s daty, třetí je Geometrie v rovině a v prostoru a čtvrtým jsou Nestandartní aplikační úlohy a problémy. (nuv.cz, 2017)

Diplomová práce se zaměřuje zejména na první a čtvrtý okruh. Díky pracovním listům také dochází k rozvoji mezipředmětových vztahů. V RVP ZV diplomová práce dosahuje až do okruhu Českého jazyka a literatury, Člověk a jeho svět, Člověk a společnost, konkrétně do dějepisu do okruhu Moderní doba, jehož součástí je zneužití moderních technologií ve světových válkách.

3.6 Didaktická hra

Na prvním stupni základní školy by měla být jako jedna z nejdůležitějších metod zařazena didaktická hra. Všeobecně hra je pro děti přirozená potřeba, které se věnují velmi rády a používají při nich všechny schopnosti, které mají. Hra dokáže v dětech vyvolat aktivitu jako u málokteré činnosti. (Houška, 1991)

Současné školství stále překonává vyučovací metody, které byly používány v minulosti. Propojení školy s běžným životem nebylo podstatnou součástí a bylo upozaďováno. Oproti historii se změnila i pozice žáka, kterou má v procesu učení. V překonávání vyučovacích metod používaných v minulosti ve školství by mohla přispět i didaktická hra. (Maňák, 2003)

V dnešní době existuje obrovské množství her, které lze ve škole využít. Bohužel hry se vyskytují převážné v mimoškolních aktivitách a v klasických školách ve vyučování se spíše objevují jako odměna než běžná součást vyučovacích hodin. (Střelec, 2004)

Především na prvním stupni základních škol by měla hra tvořit jednu z hlavních činností ve vyučování. Hra používaná ve vyučovacím procesu se liší od hry, kterou si dítě

vymyslí samo ve volném čase. Chybí jí úplná svoboda, ale za to rozvíjí žákovi smysly, fantazii a postřeh. Stejně jako běžná hra je pro žáka zábavná a díky ní je pro žáka učení zajímavější. Také chování dětí při hře napoví učiteli, jaký je třídní kolektiv. (Manniová, 2001)

3.6.1 Charakteristika didaktické hry

Didaktickou hru definuje mnoho autorů. Podle Houšky (1993) je didaktická hra *„činnost, ve které dítě spontánně uplatňuje poznávací aktivity a realizuje poznávací činnosti pod primárním vlivem příslušného pravidla, které způsobuje, že poznávání a učení probíhá nenásilně a jako by ve druhém plánu.“* Na spontánnosti se shodne Houška i s Průchou (2003), ten didaktickou hru charakterizuje jako *„analogii spontánní činnosti dětí, která sleduje (pro žáky ne vždy zjevným způsobem) didaktické cíle“.* Maňák a kolektiv (1997) zase popisují didaktickou hru jako kategorii hravých činností, která má své primární využití při učení.

3.6.2 Řízení didaktických her

Příprava vyučovací hodiny, kde se bude realizovat didaktická hra, je velice náročná pro daného učitele. Je potřeba zajistit potřebný materiál, detailně realizaci didaktické hry promyslet, vybrat vhodnou hru a zadávat ji profesionálně a kvalifikovaně ve vhodnou dobu. (Kalhous & Obst, 2002)

Než je hra zařazena do vyučovací hodiny, je třeba vytvořit časový plán, sepsat pravidla a pomůcky, stanovit cíle a kritéria, podle kterých budou výsledky hodnoceny. V případě, že didaktická hra vyžaduje rozdělení na družstva, tak musí být jejich síly vyrovnané jak počtem žáků, tak jejich znalostmi a schopnostmi. Od učitele je nutná spravedlnost a objektivní a nestranné vyhodnocování výsledků. (Maňák, 1997)

3.6.3 Rozdělení didaktických her

Kotrba a Lacina (2011) dělí didaktické hry podle délky trvání na dlouhodobé nebo krátkodobé, které trvají jen pár minut. Dále podle místa odehrávání – třída, hřiště, školní zahrada, tělocvična a podobně. Poslední skupinou je dělení podle účelu a zaměření – například rozvoj dovedností, pohybové didaktické hry nebo opakovací.

Zormanová (2014) dělí didaktické hry na tři skupiny a to na interakční, do kterých patří učební hry, hry společenské a hry s pravidly. Dále také na simulační, což znamená názorné přehrání situace z reálného života, a scénické, které navazují na divadelní hry.

Jednoduše můžeme hry rozdělit na interakční a neinterakční. Při interakčních hrách na sebe žáci působí, musí mezi sebou komunikovat, radit se a ovlivňovat se. Hráči musí přizpůsobit své chování a naučit se dělit práci a celkově kooperovat. Naopak u neinterakčních her hrají hráči každý sám za sebe a nevyskytuje se zde žádná spolupráce a hráči navzájem nekomunikují a neovlivňují se. Všichni řeší jeden určitý problém, který je pro všechny stejný. Mezi neinterakční hry patří například kvízy, přesmyčky, pexesa, slepé mapy, diagnostické a vědomostní testy, doplňovačky, deskové hry, šifrované texty, atd. (Kotrba a Lacina, 2011)

Do didaktických her intelektuálních patří hry, které mají za cíl rozvoj myšlení, pozornosti, pohotovosti a paměti. Patří sem hlavolamy, rébusy, hádanky, šifry a další. (Santlerová, 1995)

4 Praktická část

Praktická část diplomové práce se věnuje sestavování souboru osmi pracovních listů, na kterých se objevují různé druhy šifer. První tři pracovní listy jsou vytvořeny jako didaktická hra, ve které je zapojen pohyb žáků nejen po škole, ale i v přírodě, a během které žáci musí řešit jednotlivé šifry a postupně odhalují další nápovědy nebo tajenky. Dalších pět pracovních listů seznamuje postupně s různými druhy šifer, které byly vymyšleny, používány a odhaleny během dlouhé historie a lze je použít v běžné vyučovací hodině v budově školy. Tyto pracovní listy mají dětem na prvním stupni základní školy přiblížit téma šifry a ukázat jim, že i šifrování a dešifrování může být zábava. Mají také za úkol jim dokázat, že se jim znalost šifer může hodit při jejich vlastních tajných písemných komunikacích, které si mohou předávat se svými spolužáky nebo sourozenci a kamarády, a utajit tak jejich obsah před ostatními.

U každého pracovního listu jsou uvedeny následující komponenty: doporučený ročník, ve kterém se mají pracovní listy zadávat; časová náročnost řešení pracovního listu; předpokládané znalosti žáků ke správnému vyřešení pracovních listů; očekávané výstupy; pomůcky potřebné k řešení; organizační forma a také popis, jak s pracovním listem pracovat a jak se na vyučovací hodinu s pracovním listem připravit. Další komponentou u pracovních listů je návod s postupem, jak šifry vyřešit a také konečné správné řešení. Nakonec následuje zadání, které je možné předat rovnou žákům. Některé pracovní listy obsahují i potřebné materiály, jako třeba pracovní list č. 3, kde jsou vytvořeny potřebné QR kódy. U vyzkoušených pracovních listů v praxi lze nalézt popis průběhu vyučovací hodiny, dále problémy, na které zadavatel (autorka) pracovních listů narazil a poznámky. Dále také řešení jednotlivých žáků a úlohy, které jim dělaly největší potíže.

K vypracování pracovních listů byl použit program Microsoft Office.

4.1 Pracovní listy

4.1.1 Pracovní list č. 1

Hra: Hledání pokladu

Ročník: 1. – 2. ročník

Časová náročnost: 1 vyučovací hodina (45 minut)

Předpokládané znalosti: znalost barev, znalost celé abecedy

Očekávané výstupy: chápat jednoduché souvislosti, nacházet společné znaky, orientace v barvách, orientace podle šipek, rozvíjí mezipředmětové vztahy (český jazyk a literatura)

Pomůcky: šifry, něco na psaní (pero, tužka, pastelka nebo fixa)

Organizační forma: práce ve skupinách

Popis činnosti:

Nejprve si před začátkem vyučovací hodiny učitel připraví všechny potřebné pomůcky. Schová poklad a ukryje všechny šifry na správná místa. Pořadí kam ukrýt šifry si může určit vyučující sám.

Na začátku hodiny pedagog děti namotivuje příběhem *O bohatém pirátovi* nebo si každý učitel může vymyslet vlastní příběh, aby seděl na jejich školu, popřípadě jiné místo, kde děti poklad naleznou.

Příběh o bohatém pirátovi

„Byl jednou jeden bohatý pirát, který procestoval celý svět. Během svých cest navštívil snad všechna krásná místa a z každého si přivezl cenný suvenýr. Také oloupil mnoho žen i mužů. Jelikož neměl to štěstí a nenarodilo se mu žádné dítě, neměl komu svůj poklad předat. Rozhodl se, že své bohatství ukryje tak, aby ho mohl najít jen ten, kdo si ho opravdu zaslouží a to tím, že vyřeší všechny hádanky, které on sám vymyslel. Vyrazil tedy hledat místo, kde by své bohatství mohl zakopat nebo bezpečně ukrýt. Hledal a hledal, až našel v jedné malé vesnici ve Středočeském kraji budovu, která se mu na to perfektně hodila. Stála uprostřed návsi hned vedle gotického kostela. Ukryl zde

poklad a všechny nápovědy, které k pokladu vedou. A děti představte si, že já jsem dnes ráno jednu takovou nápovědu našla, když jsem se byla podívat na školní půdě.“

Poté se dětem dá první nápověda, která je nasměruje blíže k pokladu. Nápověda obsahuje šifru, kterou se děti společnými silami snaží rozluštit. Další nápovědu s druhou šifrou objeví ukrytou na místě, na které je nasměrovala předchozí rozluštěná šifra. Poslední nápověda, na které se opět nachází šifra, je navede ke konečnému místu, kde naleznou vytouženou truhlu s pokladem. Poklad může být cokoliv, co děti ocení, například čokoládové penízky, které znázorňují mince a tudíž i pravý poklad nebo stačí i obyčejné bonbóny.

Poznámka:

Dávejte pozor na to, aby se pokusili zapojit všichni žáci. Pokud máte ve třídě větší počet dětí, můžete je rozdělit na více skupin. V tomto případě je možné je „vypouštět“ postupně nebo pro každou skupinu vytvořit jiné šifry.

Po nalezení pokladu je dobré s dětmi projít řešení šifer, kdo měl jaký nápad, jak různé skupiny postupovaly a kterým způsobem nakonec všechny šifry dokázaly rozluštit.

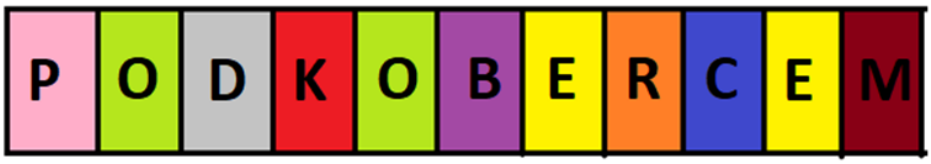
Pokuste se dětem do jejich nápadů na řešení a do jejich debat nezasahovat.

Pracovní list č. 1: Řešení

1. šifra

Návod řešení: Písmena přiřazujeme do daných okének podle barev. Barva okénka se shoduje s barvou písmena.

Správné řešení:



P D K O E

B C R M

2. šifra

Návod řešení: Do křížovky doplňujeme názvy princezen, aby nám seděl počet i pořadí písmen.

Správné řešení:

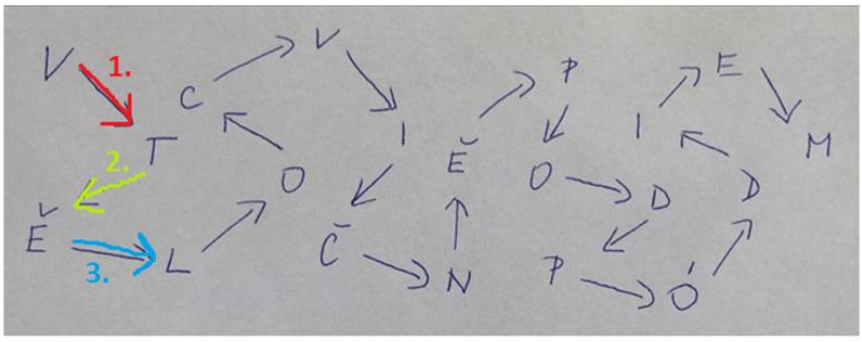
PRINCEZNY

	Z	L	A	T	O	V	L	Á	S	K	A
				P	Y	Š	N	Á			
P	O	P	E	L	K	A					
						T					
		R	Ů	Ž	E	N	K	A			
				S	N	Ě	H	U	R	K	A

2. šifra

Postup řešení:

Začneme od písmenka V a dále postupuje podle šipek V → T → …



Správné řešení:

V TĚLOCVIČNĚ POD PÓDIEM

Pracovní list č. 1: Zadání

1. **šifra**

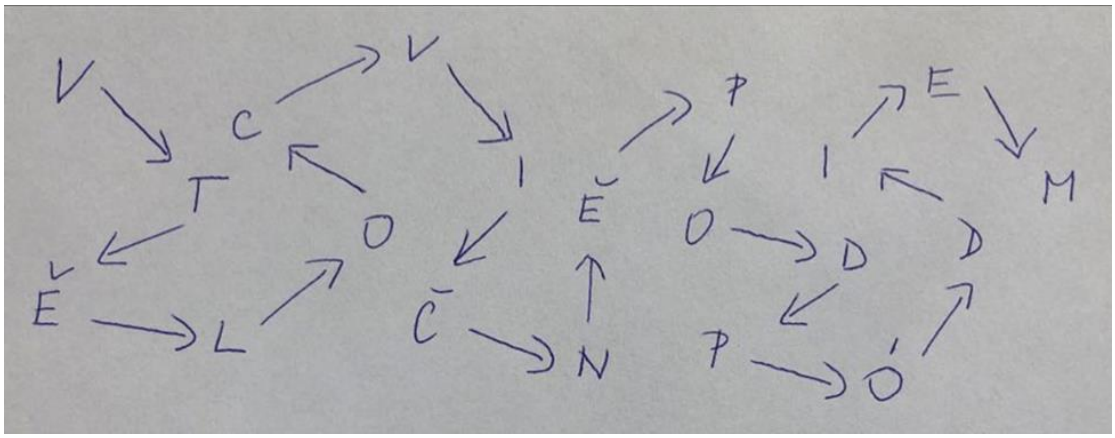
P D K O E

B C R M

2. **šifra:** PRINCEZNY

	Z		A		O		L		S		A
					Y		N				
	O		E		K						
						T					
			Ů		E		K				
					N		H		R		A

3. **šifra**



Popis po vyzkoušení v praxi:

Tento pracovní list byl zadán ve 2. ročníku, vyučovací hodiny se zúčastnilo 14 žáků. Všechny děti velmi dobře reagovaly na motivaci pohádkou. Byly velice nadšené a do luštění šifer se vrhly s velkou vervou. Problémem bylo, že zadavatel pracovních listů pracoval se všemi žáky najednou, takže ti průbojnější a bystřejší byli rychlejší a nenechali pomalejší děti přemýšlet a rovnou danou šifru vyřešili. Pomalejší děti se sice snažily zapojit a po vyřešení utíkaly na další místo určení, aby dokázaly najít, kde se ukrývá následující šifra, ale bohužel nad jejich řešením tolik nepřemýšlely. Příště by bylo vhodné si děti rozdělit do menších skupin.

Šifry byly pro žáky 2. ročníku dost jednoduché. Největší problém jim dělala druhá šifra, ve které měli odhalit jména princezen. Žáci v této třídě spíše koukají na kreslené pohádky, takže jména princezen moc neznali. Příště by bylo vhodné o den dříve zopakovat pohádky a jména princezen například v rámci literatury. Fotografie z vyučovací hodiny jsou v příloze stejně jako ukázka řešení pracovních listů žáky.

4.1.2 Pracovní list č. 2

Hra: Chyťte zloděje!

Ročník: 2. – 3. ročník

Časová náročnost: 1 vyučovací hodina (45 minut)

Téma: Šifry

Předpokládané znalosti: znalost abecedy, znalost číselné řady, čtení, psaní

Očekávané výstupy: rozvoj mezipředmětových vztahů (český jazyk a literatura)

Pomůcky: papír, tužka, připravené „důkazy“ (šifry)

Organizační forma: skupinová práce

Popis činnosti:

Nejprve si před začátkem vyučovací hodiny učitel připraví všechny potřebné pomůcky. Domluví se se „zlodějem“, předá mu třídního maskota a připraví ho na příchod třídy po vyřešení případu.

Na začátku hodiny učitel vběhne do třídy a sehraje scénku, ve které sdělí dětem, že se ve škole stala krádež. Ukraden byl třídní maskot nebo cokoliv jiného. Poví dětem, že po cestě našel na chodbě důkazy, které mohou pomoci dopadnout zloděje. A dá dětem první nápovědu. Postupně děti řeší šifry a po vyřešení všech důkazních materiálů dají hlavy dohromady a zkusí přijít na to, kdo je pachatelem. Nakonec si dojdou za pachatelem svého třídního maskota vyzvednout a zachránit.

Po záchraně projděte společně se všemi dětmi dané „důkazy“. Zjistěte, jak děti vyřešily šifry a proč je zrovna napadl tento pachatel.

Poznámky:

Dávejte pozor, aby se snažily zapojit všechny děti. Pokud máte ve třídě více žáků, můžete děti rozdělit na týmy a vyhlásit soutěž o to, kdo dříve nalezne pachatele a zachrání třídního maskota.

Pracovní list č. 2: Řešení

1. nápověda

Návod řešení: Do prvního řádku doplníme čísla, jak jdou po sobě. Zbytek řádků doplníme podle toho, jak jdou za sebou písmena v abecedě.

4	5	6	7	8
R	S	T	U	V
P	Q	R	S	T
G	H	I	J	K
B	C	D	E	F
Y	Z	A	B	C

Správné řešení: 6 TRIDA → 6. TŘÍDA

2. nápověda

Návod řešení: přečteme daný text pozpátku – zleva doprava

KYZAJ ÝKCILGNA

Správné řešení: ANGLICKÝ JAZYK

3. nápověda: JMÉNA

Návod řešení: Doplníme písmenka tak, aby nám vznikla křestní jména.

P	R	O	K	O	P	E	T	R		
			E	V	A	D	A	M		
	F	I	L	I	P	A	V	E	L	
	P	A	V	L	Í	N	A			
		P	E	T	R	A	D	E	K	
	D	E	N	I	S	I	M	O	N	A
	D	A	V	I	D	A	N	I	E	L
J	A	R	O	M	Í	R				
	A	R	T	U	R	O	M	A	N	
			I	V	O	L	G	A		
				D	U	Š	A	N		

Správné řešení: PAPÍR S DÍROU

Po vyřešení všech šifer dáme dohromady nápovědy a zjistíme, že naším pachatelem je pan učitel na anglický jazyk. Anglický jazyk, protože ho vyučuje, 6. třída, protože je třídní učitel 6. třídy a papír s dírou je hra, kterou s dětmi nejčastěji hraje.

Pracovní list č. 2: Zadání

1. **šifra**

4	5	.	7	8
R	S	.	U	V
P	Q	.	S	T
G	H	.	J	K
B	C	.	E	F
Y	Z	.	B	C

2. **šifra**

KYZAJ ÝKCILGNA

3. **šifra**

JMÉNA

P	R	O	K	O	.	E	T	R		
			E	V	.	D	A	M		
	F	I	L	I	.	A	V	E	L	
	P	A	V	L	.	N	A			
		P	E	T	.	A	D	E	K	
	D	E	N	I	.	I	M	O	N	A
	D	A	V	I	.	A	N	I	E	L
J	A	R	O	M	.	R				
	A	R	T	U	.	O	M	A	N	
			I	V	.	L	G	A		
				D	.	Š	A	N		

4.1.3 Pracovní list č. 3

Ročník: 4. – 5. ročník

Časová náročnost: 2 vyučovací hodiny (90 minut)

Téma: QR kódy

Předpokládané znalosti: práce s technologiemi, znalost celé abecedy, znalost Caesarovy šifry

Očekávané výstupy: orientace v přírodě podle mapy, práce s moderními technologiemi (mobilní telefon, tablet)

Pomůcky: QR kódy, tužka, papír, mapa

Organizační forma: Skupinová práce v přírodě

Popis činnosti:

Nejprve si učitel před začátkem vyučování připraví všechny potřebné materiály. Rozmístí dané očíslované QR kódy někde v přírodě v okolí školy nebo při špatném počasí i uvnitř budovy. Zakreslí daná místa do předem připravené mapy a tu nakopíruje na počet, který je třeba.

Pokud není k dispozici dostatečný počet mobilních telefonů nebo tabletů ve škole, poprosí učitel o den dříve děti, ať si do školy přinesou vlastní zařízení se staženým programem na čtení QR kódů. Tento program se dá zdarma snadno stáhnout na internetu, některé telefony ho mají rovnou zabudovaný ve fotoaparátu.

Učitel s dětmi dojde na dané místo, kde jsou ukryté QR kódy. Rozdělí děti na skupiny alespoň po dvojicích a dá dětem mapy s vyznačenými místy. Děti učitel vypouští po 5 minutách, aby nedošlo k „hromadné“ spolupráci a všechny děti neběžely společně.

Když dítě doběhne na místo s QR kódem, tak ho naskenuje na svůj mobilní telefon, popřípadě tablet a zobrazí se mu šifra, kterou musí společně se svou dvojicí vyřešit a zapsat si její řešení. Pokud dvojice zvládne dešifrovat všechny šifry, dají dohromady tajenku. Žáky, kteří zvládnou vyřešit všechny šifry a tím pádem budou znát

celou tajenku, čeká malá sladká odměna. Tato odměna může být cokoliv, například bonbóny.

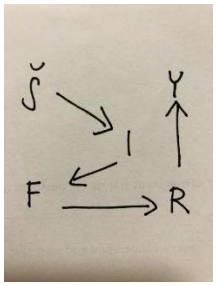
Poznámky:

Na konci je dobré s dětmi projít všechny šifry a jejich řešení. Zkoumat, jaké různé postupy děti použily.

Pracovní list č. 2: Řešení

1. šifra

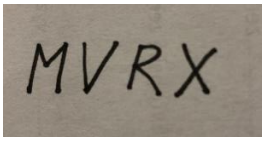
Návod řešení: Začneme u písmena Š a dále pokračujeme podle šipek Š → I →…



Správné řešení: ŠIFRY

2. šifra

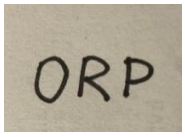
Návod řešení: Caesarova šifra: klíč: posun o 3 písmena



Správné řešení: JSOU

3. šifra

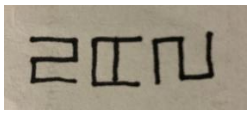
Návod řešení: Přečteme slovo zleva doprava



Správné řešení: PRO

4. šifra

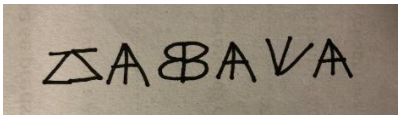
Návod řešení: Stačí se podívat na obrázek z boku. Uvidíme tím pádem hranatá písmena.



Správné řešení: NAS → NÁS

5. šifra

Návod řešení: Na obrázku jsou písmena, která jsou zdvojená



Správné řešení: ZABAVA → ZÁBAVA

Celá tajenka je: ŠIFRY JSOU PRO NÁS ZÁBAVA

Pracovní list č. 3: Zadání

1. Podle mapy doběhni na místo označené číslem 1. Až doběhneš na místo, naskenuj QR kód, který najdeš a vyřeš šifru. Výsledný text si zapiš.

…….

2. Další v pořadí hledej místo označené číslem 2. Opět naskenuj QR kód, vyřeš šifru, zapiš a pokračuj dál.

……..

3. Stanoviště číslo 3, najdi ho podle mapy, naskenuj QR kód, vyřeš šifru a zapiš.

……...

4. Číslo 4 na mapě označuje další místo, kde najdeš potřebný QR kód k vyřešení celé tajenky, vyřeš šifru, kterou ukrývá, a zapiš si řešení.

…….

5. Poslední QR kód, který potřebuješ k odhalení tajenky, najdeš na mapě s číslem 5. Až ho najdeš, naskenuj ho, vyřeš šifru a zapiš.

……...

6. Napiš výslednou tajenku a vrať se zpět na start.

……

Potřebný materiál pro pracovní list č. 3

1.QR kód

2.QR kód

3.QR kód

4.QR kód

5.QR kód

Mapa: Zámecký park Nalžovice

Nápovědy:

1.VSTUP

2.DŘEVĚNÉ BUDKY

3.HŘIŠTĚ

4.HASIČSKÉ PŘEKÁŽKY

5.ROHOVÁ ZEĎ

4.1.4 Pracovní list č. 4

Ročník: 2. – 5.

Časová náročnost: 1 vyučovací hodina (45 minut)

Téma: Morseova abeceda

Předpokládané znalosti: znalost celé abecedy

Očekávané výstupy: znalost Morseovy abecedy, rozvíjení mezipředmětových vztahů (český jazyk a literatura)

Pomůcky: QR kódy, tužka, papír, mobilní telefon nebo tablet, baterka

Organizační forma: samostatná práce

Popis činnosti:

Nejprve si před začátkem vyučovací hodiny učitel připraví vše potřebné. Ve třídě někam umístí QR kódy. Pokud není možnost dostatečného počtu mobilních telefonů nebo tabletů ve škole, poprosí učitel děti, ať si do školy přinesou vlastní zařízení se staženým programem na čtení QR kódů.

Nejprve na začátku hodiny učitel děti seznámí s tím, co je Morseova abeceda, na co se používala v minulosti a k čemu se používá v současnosti. Poté rozdá dětem pracovní list, kde najdou různé úkoly. Například vzkaz napsaný v Morseově abecedě a jejich úkol bude ho rozluštit. Nebo naopak zprávu přepsat do Morseovy abecedy. Při neznalosti Morseovy abecedy se děti vydají ke QR kódu, u kterého po naskenování naskočí nápověda v podobě celé Morseovy abecedy. (Pokud nemáte ve škole ani u dětí doma možnost zařízení na čtení QR kódu, tak je možné Morseovu abecedu pouze vytisknout a k pracovnímu listu dětem přiložit.)

Nakonec s dětmi projdeme jejich řešení a zkusíme je naučit vyťukávat tajné vzkazy v Morseově abecedě.

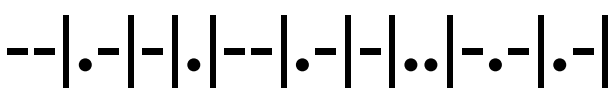
Poznámka:

Dávejte pozor, ať se každý žák snaží pracovat samostatně.

Pracovní list č. 4: Řešení

1. úkol

Návod řešení: Postupně si v tabulce Morseovy abecedy najdeme jednotlivé tvary a přiřadíme k nim písmeno. První je M, další A, …



Správné řešení: MATEMATIKA

2. úkol

Návod řešení: Postupně si v tabulce Morseovy abecedy najdeme daná písmena a převedeme je do Morseovy abecedy.

ŠIFROVÁNÍ → SIFROVANI – Slovo musíme přepisovat bez diakritických znamének.

Správné řešení: 

3. úkol

Návod řešení: Každý si napíše své jméno a převede ho do Morseovy abecedy. Kontrolu provedou děti mezi sebou.

4. úkol

Návod řešení: Naučit děti vyťukávat své jméno. Nejprve si každý vyzkouší sám a poté předvede před třídou.

5. úkol

Postup řešení: Naučit děti vyslat své jméno pomocí světelného signálu z baterky. Nejprve si každý žák vyzkouší sám a poté zkusí předvést před třídou.

Pracovní list č. 4: Zadání

1. **úkol:** Rozlušti tajný vzkaz napsaný v Morseově abecedě.

--|.-|-|.|--|.-|-|..|-.-|.-|

Řešení: ……

2. **úkol:** Převeď slovo ŠIFROVÁNÍ do psané podoby Morseovy abecedy.

Řešení: ……

3. **úkol:** Napiš své jméno v Morseově abecedě.

Řešení: ……

4. **úkol:** Zkus pomocí Morseovy abecedy vyťukat do lavice své jméno.

5. **úkol:** Zkus pomocí světelné baterky vyslat vzkazem své jméno spolužákovi.

Potřebný QR kód:

SCAN ME

Řešení dětí pracovního listu č. 4 jsou v příloze.

Popis po vyzkoušení v praxi:

Tento pracovní list byl v praxi vyzkoušen ve 2. třídě. Vyučovací hodiny se zúčastnilo 14 žáků. Při počátečním povídání a seznámení s Morseovou abecedou bylo zjištěno, že ani jeden žák neví, o co se jedná a k čemu se tato abeceda používala. Po objasnění a vyprávění se žáci už těšili na práci. Po rozdání pracovních listů se celá třída pustila do práce a žáci samostatně vyplňovali dané úkoly. Na problém se narazilo až ve chvíli, kdy došlo na vyťukávání o lavici a na vysílání signálů pomocí světelné baterky, to bohužel dětem moc nešlo, tak zadavatel musel zaimprovizovat a zadat úkol navíc, který zněl: Zašifruj moje jméno (třídní učitelka) a jména asistentek, které dnes jsou s námi ve třídě, tzn. Katka, Monika, Blanka. Úkoly s vyťukáváním a s vysíláním signálů pomocí světelné baterky lze tedy zařadit při práci ve vyšších ročnících jako je 4. a 5. ročník.

Na konci vyučovací hodiny byly děti nadšené. Nechávaly si u sebe rozdanou Morseovu abecedu a o přestávce si v lavici šifrovaly texty, které chtěly dát doma rodičům, jestli dokáží jejich tajný vzkaz rozluštit. Fotografie z vyučovací hodiny jsou v příloze.

4.1.5 Pracovní list č. 5

Ročník: 2. – 5. ročník

Časová náročnost: 1 vyučovací hodina (45 minut)

Téma: Caesarova šifra

Předpokládané znalosti: Znalost abecedy a čísel (minimálně do 3)

Očekávané výstupy: znalost Caesarovy šifry, šifrování a dešifrování Caesarovy šifry, propojuje mezipředmětové vztahy (český jazyk a literatura, člověk a svět: historie)

Pomůcky: tužka, pracovní list

Organizační forma: samostatná práce

Popis pracovního listu:

Tento pracovní list slouží k seznámení dětí s Caesarovou šifrou. Naučí je pracovat s posunem písmen, dešifrovat a zjistit tajný text a zároveň i šifrovat svůj vlastní text, který nechtějí, aby přečetl někdo „nežádoucí“.

Popis práce s pracovním listem:

Žákům učitel rozdá nakopírovaný pracovní list a nechá je samostatně pracovat. Menším nebo těm méně zdatnějším dětem se může snažit trochu pomoci tím, že jim ukáže a dovysvětlí daný klíč.

Po dokončení a vytvoření vlastního zašifrovaného textu vlastním klíčem může učitel žáky nechat prohodit pracovní listy a vyzkoušet si, kdo zvládne text svého spolužáka rozluštit. Některé rychlejší děti mohou vyzkoušet dešifrovat více textů od více spolužáků.

Pracovní list č. 5: Řešení

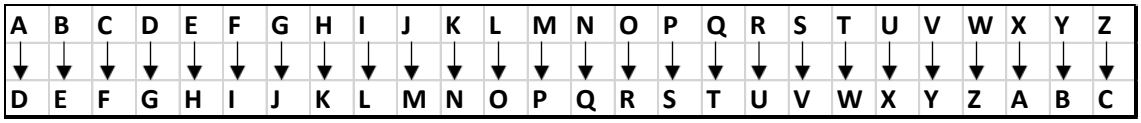
Úkol č. 1 **Řešení:** Zvladl jsem rozlustit tuto sifru. Jsem sikula.

Úkol č. 2 **Řešení:** XC XPLP VLIURYDW.

Pracovní list č. 5: Zadání

1. **Úkol:** Rozlušti daný text podle tohoto klíče.

Klíč:



Text:

CYODGO MVHP URCOXVWLW WXWR VLIUX. MVHP VLNXOD.

Řešení: ……

2. **úkol:** Ukryj daný text podle stejného klíče, který si použil u úkolu č. 1.

Text: Uz umim sifrovat.

Řešení: ……

3. **úkol:** Vymysli si svůj vlastní text a ukryj ho. Řešení nikomu neprozraď. Můžeš vymyslet i více textů nebo nějaký pořádně dlouhý.

……
……
……
……

4.1.6 Pracovní list č. 6

Ročník: 4. – 5. ročník

Časová náročnost: 1 vyučovací hodina (45 minut)

Téma: Matematické šifry

Předpokládané znalosti: znalost geometrických tvarů, sčítání, odčítání a násobení přirozených čísel

Očekávané výstupy: rozvoj pozornosti a logického myšlení

Pomůcky: psací potřeba (tužka, pero), sirky nebo špejle

Organizační forma: samostatná práce

Popis činnosti:

Učitel si před začátkem vyučovací hodiny připraví potřebné materiály. Vytiskne každému žákovi pracovní list a připraví potřebný počet sirek nebo špejlí.

Po zvonění učitel rozdá dětem pracovní listy a nechá je samostatně pracovat. Je možné děti motivovat odměnou, aby se pokusily pracovat všichni. Odměnou může být razítko, jednička nebo nějaká sladkost.

Během hodiny učitel prochází kolem lavic a pozoruje dětské řešení a jejich pokusy a omyly, kterými se dostanou ke správnému výsledku.

Na konci si řešení s dětmi společně probereme a ukážeme si různé postupy, které děti použily. Pokud se stane, že nějaký žák něco nezvládne, ostatní žáci mu mohou pomoci a pokusí se ho navést na správnou cestu, jak úkol vyřešit.

Poznámky:

Dávejte pozor, ať se na začátku snaží každý žák pracovat samostatně. Pokud některé dítě vyřeší všechny úkoly a zbyde mu čas, může pomoci ostatním a zkusit je navést na správnou cestu, kterou se dostane k řešení daných úkolů.

Pracovní list č. 6: Řešení

1. úkol

Návod řešení: Nejprve si vyřešíme jednotlivé příklady, abychom zjistili, jaká čísla představují jednotlivé obrázky. Poté vypočítáme poslední příklad. Pozor na to, co všechno obsahují jednotlivé obrázky a která početní operace má přednost.

Správné řešení:

→ 30 : 3 (obrázky) = 10 → 10 + 10 + 10 = 30

→ 9 : 3 (obrázky) = 3 → 3 + 3 + 3 = 9

→ 21 : 3 (obrázky) = 7 → 7 + 7 + 7 = 21

→ 10 + 3 = 13

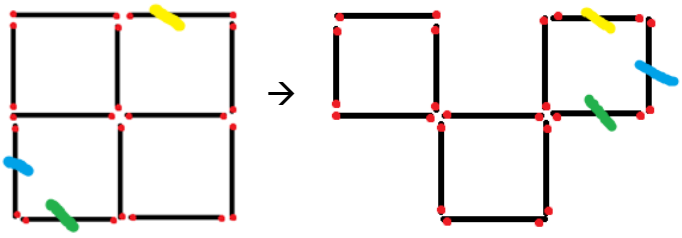
→ 10 + 3 + 7 = 20

→ 13 + 20 × 3 (pozor násobení má přednost)

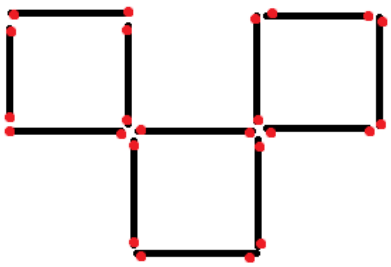
20 × 3 = 60 60 + 13 = 73

2. úkol

Návod řešení: Dítě tento úkol může řešit pokusem a omylem.



Správné řešení:



3. úkol

Návod řešení: Tajenku luštíme tak, že první číslo znázorňuje číslo obdélníku a druhé číslo v pořadí znázorňuje kolikáté písmeno v rámečku to je.

42 → obdélník č. 4, 2. písmeno = J

72 → obdélník č. 7, 2. písmeno = S

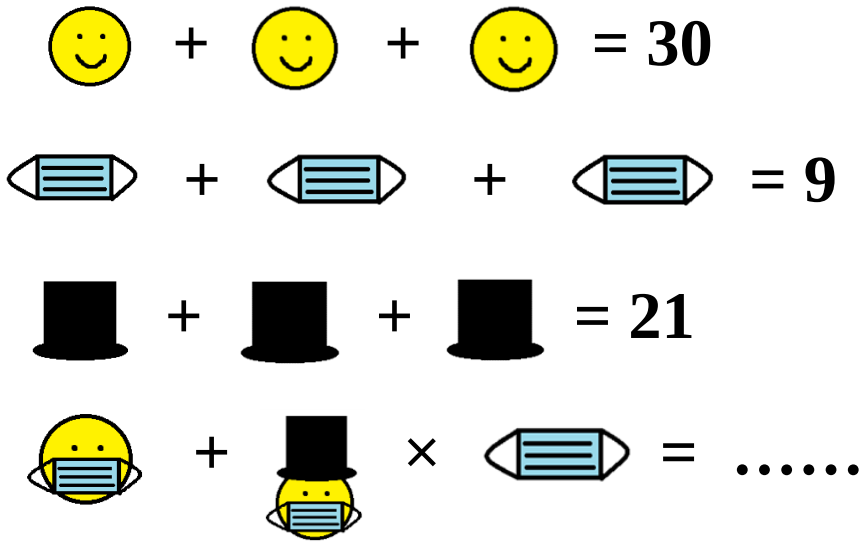
41 → obdélník č. 4, 1. písmeno = I

Správné řešení:

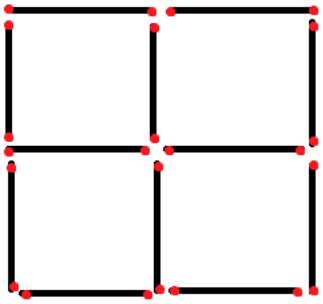
42 72 41 72 41 43 81 51 11
J S I S I K U L A

Pracovní list č. 6: Zadání

1. Vypočítej



2. Přendejte 3 tyčky tak, aby vznikly 3 stejné čtverce. Zkus si obrázek seskládat ze sirek nebo špejlí. Výsledný obrázek nakresli do volného prostoru.



3. Vylušti tajenku.

42 72 41 72 41 43 81 51 11

… … … … … … … … …

A B C **1**	**D E F** **2**	**G H CH** **3**
I J K **4**	**L M N** **5**	**O P Q** **6**
R S T **7**	**U V W** **8**	**X Y Z** **9**

Řešení dětí pracovního listu č. 6 jsou v příloze.

Popis po vyzkoušení v praxi:

Tento pracovní list byl zadán žákům k samostatné práci ve 4. třídě. Bohužel epidemiologická situace nedovolila zadat tyto pracovní listy osobně a pozorovat práci žáků, jejich pokusy, omyly a problémy. Úkol byl sice určen k vyplnění samostatně bez pomoci rodičů, sourozenců nebo kamarádů, ale bohužel není zaručeno, že to tak opravdu bylo.

Ze zpětné vazby získané od žáků lze vyvodit, že je řešení zadaných úkolů velmi bavilo. Nejtěžší pro ně bylo 2. cvičení, kde museli přendat 2 sirky, párátka nebo špejle a vytvořit tak tři stejné čtverce.

Jak jednotliví žáci řešili úkol číslo 1 – špatná řešení:

1. Nejčastějším špatným řešením byl výsledek 99. Žáci k tomuto výsledku došli tak, že zapomněli, že násobení má v počítání vždy přednost před sčítáním, a tak musí nejprve čísla vynásobit a poté teprve další číslo přičíst.
   Počítali tedy, že 13 + 20 = 33 a poté teprve násobili 3 → 33 × 3 = 99.
2. Dalším špatným řešením, které se objevilo u jednoho žáka, byl výsledek 90. Tento žák se k tomuto výsledku dopočítal tak, že u prvního obrázku zapomněl připočíst roušku, která měla hodnotu 3 a dále počítal se samostatným smajlíkem, který měl hodnotu 10 a opět jako u prvního špatného řešení zapomněl, že v počítání má vždy přednost násobení před sčítáním. Počítal tedy, že 10 + 20 = 30 a poté teprve násobil 3 → 30 × 3 = 90.
3. Posledním špatným řešením, které se v této třídě objevilo u jednoho žáka, byl výsledek 51. Tento žák očividně vůbec nepochopil zadání, protože počítal tak, že u prvního obrázku zapomněl připočíst roušku, která měla hodnotu 3 a dále počítal se samostatným smajlíkem, který měl hodnotu 10, u druhého obrázku dokonce vynechal smajlíka i roušku a počítal dál jenom s kloboukem, tedy s hodnotou 7 a nakonec ještě jako u ostatních špatných řešení zapomněl, že v počítání má vždy přednost násobení před sčítáním. Počítal tedy, že 10 + 7 = 17 a poté teprve násobil 3 → 17 × 3 = 51

Jak jednotliví žáci řešili úkol 2 – špatná řešení:

Špatné řešení se mezi všemi našlo pouze jedno, viz obrázek řešení dětí v příloze. Žák sice přendal dvě špejle a vznikly mu tři stejné čtverce, ale bohužel mu dvě přendané špejle netvořily žádný tvar a pouze samostatně trčely. Díky tomuto řešení jsem se zamyslela nad svým zadáním, do kterého bych připsala, že všechny sirky se musí použít na strany jednotlivých čtverců.

Tři žáci se přiznali, že si s tímto úkolem i po dlouhém lámání hlavy nevěděli rady a nakonec jim pomohl někdo z rodiny.

Jak jednotliví žáci řešili úkol 3 – špatná řešení:

Špatné řešení tohoto úkolu se v této třídě vyskytlo pouze jedno. Žákovi vznikla tato tajenka: JE SE JB SE JB JH VB MB BB. Žák ze začátku postupoval správně. Koukl se na první číslo a našel si podle toho příslušný obdélník v klíči. Bohužel dále už pokračoval špatně. V nalezeném obdélníku totiž opsal prostřední písmeno, napsal ho a pokračoval. Podíval se na druhé číslo, našel si další obdélník a opět zapsal prostřední písmeno.

Pracoval tedy tak, že našel obdélník 4, zapsal prostřední písmeno J, našel obdélník 2, zapsal písmeno E a pokračoval na další dvojčíslí. Bohužel si neuvědomil, že místo dvou čísel se zapíše pouze jedno písmeno.

Další 2 žáci toto cvičení vůbec nevyplnili, protože si s ním nevěděli rady. Jeden z nich byl žák, který má individuálně vzdělávací plán (IVP).

4.1.7 Pracovní list č. 7

Ročník: 4. – 5. ročník

Časová náročnost: 1 vyučovací hodina (45 minut)

Téma: Braillovo písmo

Předpokládané znalosti: znalost celé abecedy

Očekávané výstupy: seznámení s Braillovým písmem, rozvíjí mezipředmětové vztahy (český jazyk a literatura)

Pomůcky: psací potřeba (pero, tužka), tabulka Braillova písma, počítač nebo tablet s internetem

Organizační forma: samostatná práce

Popis činnosti:

Před začátkem vyučovací hodiny si učitel připraví potřebné pomůcky. Vytiskne všem dětem vlastní pracovní list a také tabulku Braillova písma. Zařídí také dostatečný počet tabletů nebo počítačů. Pokud není možnost přístupu na internet, lze úkoly č. 2 a 3 vynechat nebo mohou děti zkusit odpověď odhadnout a na konci hodiny si společně s učitelem své nápady projdou a vyberou ty správné.

Na začátku hodiny se dětem rozdá pracovní list a tabulku s Braillovým písmem a nechají se samostatně pracovat. Pokud někdo skončí dříve než ostatní, může pomoci těm dětem, které nepřišly na to, jak pracovat.

Po skončení práce si všichni společně řeknou správná řešení a odpovědi. Žáci si s učitelem popovídají o tom, co je to vlastně Braillovo písmo, komu a k čemu je určené a ukáží si, jak skutečně vypadá ve vyražené formě. Pokud zbyde čas, mohou si žáci navzájem zkontrolovat svá jména a příjmení, jestli je všichni zvládli správně zakreslit.

Poznámky:

Dávejte pozor, ať se na začátku snaží každý žák pracovat samostatně.

Pracovní list č. 7: Řešení

1. úkol

Návod řešení: V tabulce s Braillovým písmem vyhledáme daný obrázek a podíváme se, které písmenko představuje. Poté si písmenko zapíšeme a snažíme se nalézt další znaky.

Správné řešení: Braillovo písmo

2. úkol

Návod řešení: Děti hledají na internetu nebo zkoušejí odhadovat.

Správné řešení: Braillovo písmo je určené lidem, kteří jsou nevidomí, slabozrací nebo se zbytky zraku.

3. úkol

Návod řešení: Děti hledají na internetu nebo zkoušejí odhadovat.

Správné řešení: Jedná se o plastické body vyražené do materiálu a čtenář je dokáže vnímat pomocí hmatu.

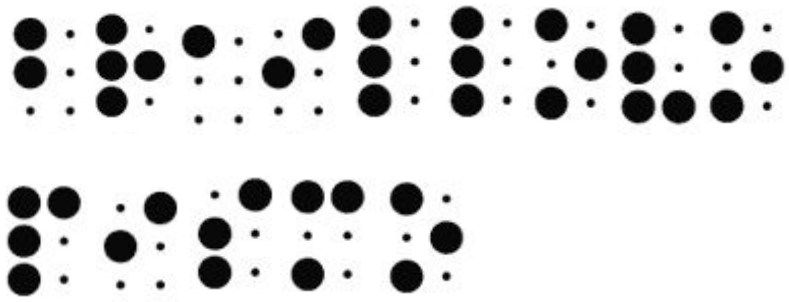
4. úkol

Návod řešení: Každý žák si napíše své jméno a postupně hledá znaky, které mu na daná písmena sedí. Například Kateřina → První si žák najde písmeno „K“, překreslí obrázek, hledá písmeno „A“, překreslí obrázek, hledá písmeno „T“, překreslí obrázek, atd.

Správné řešení: Každý žák má své vlastní správné řešení. Pokud zbyde čas ve vyučovací hodině, mohou si je zkontrolovat navzájem. Pokud už ale žádný čas nezbyde, může tento úkol zkontrolovat učitel po vybrání pracovních listů.

Pracovní list č. 7: Zadání

1. Rozlušti tajný vzkaz.



Řešení: …… ……

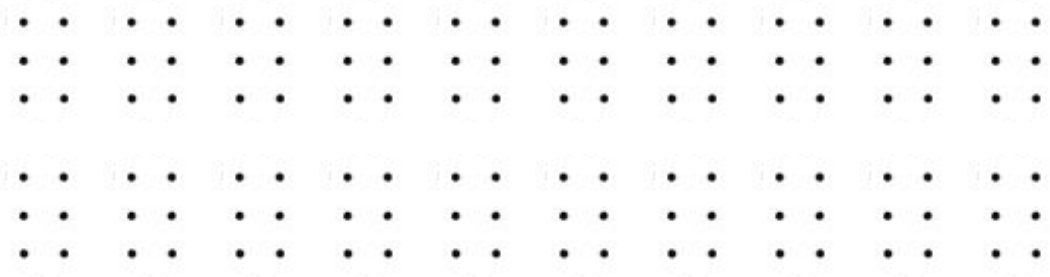
2. Pomocí internetu zkus zjistit, komu je toto písmo určené.

…….

3. Pomocí internetu zkus zjistit, jak tito lidé dokáží toto písmo přečíst.

…….

4. Napiš své jméno a příjmení pomocí tohoto písma.



Popis po vyzkoušení v praxi:

Tento pracovní list byl k samostatnému vyplnění zadán 5. třídě. Bohužel epidemiologická situace nedovolila zadat pracovní listy osobně a pozorovat jednotlivá řešení žáků, jejich pokusy, omyly a problémy. Žáci byli požádáni o samostatnou práci bez pomoci rodičů, sourozenců nebo kamarádů, ale bohužel nemůže být zaručeno, že tomu tak opravdu bylo.

Po zpětné vazbě od jednotlivých žáků je zřejmé, že je vyplňování a řešení pracovního listu bavilo. Je překvapivé, že velká spousta dětí vůbec netušila, co Braillovo písmo je, proto je dobře, že s ním byli žáci pomocí pracovního listu seznámeni, jelikož nevidomí lidé jsou součástí našeho světa a nikdy nevíme, kdy se s tímto písmem v životě setkáme. Problémy u žáků díky pomocné tabulce s Braillovým písmem nebyly. Díky internetu děti dokázaly samostatně vyhledat i odpovědi na otázky.

Řešení dětí pracovního listu č. 7 je v příloze.

4.1.8 Pracovní list č. 8

Ročník: 4. – 5. ročník

Časová náročnost: 1 vyučovací hodina (45 minut)

Téma: Polybiův čtverec a Skytalé

Předpokládané znalosti: znalost přirozených čísel do 5, znalost celé abecedy, znalost základních geometrických tvarů

Očekávané výstupy: znalost šifry zvané Polybiův čtverec a znalost šifry zvané Skytalé, rozvíjí mezipředmětové vztahy (český jazyk a literatura, člověk a svět)

Pomůcky: psací potřeba (tužka, pero), věci ve tvaru válce, papír, tablety nebo počítače, nůžky

Organizační forma: samostatná práce

Popis činnosti:

Před začátkem vyučovací hodiny si učitel připraví všechny potřebné pomůcky a materiály. Vytiskne si pracovní listy pro všechny děti a zajistí techniku s přístupem na internet: tablety nebo počítače. Také je třeba v tělocvičně rozmístit věci, které mají tvar válce, aby z nich bylo možné vytvořit Skytalé, například násadu od koštěte, hudební nástroj dřívka, obal od brambůrek (Pringles), skleničku, atd.

Po zvonění pedagog dětem rozdá pracovní listy a nechá je samostatně pracovat. Žák, který splní první dva úkoly, si vezme nůžky, papír a tužku a odchází do tělocvičny, kde hledá věci ve tvaru válce a snaží se zašifrovat vlastní text. Poté se i se svým vzkazem na papírku vrací do třídy a papírek hodí do určené nádoby.

Poté, co všechny děti zašifrují své texty a vhodí je do nádoby, tak si každý vylosuje jeden papírek a společně vyráží do tělocvičny a každý se snaží svou vylosovanou šifru rozluštit.

Poznámky:

Dávejte pozor, ať každý žák pracuje samostatně. Je dobré, pokud máte možnost, vyslat do tělocvičny dospělou osobu, asistentku, která se postará o klid a bude dávat pozor na bezpečnost a pracovní nasazení dětí.

Pracovní list č. 8: Řešení

1. úkol

Návod řešení: Jedná se o Polybiův čtverec. První číslo udává číslo řádku a druhé číslo udává číslo sloupce.

55 → 5. řádek, 5. sloupec → Z

24 → 2. řádek, 4. sloupec → I/J

Správné řešení: ZJISTI CO JE SKYTALE.

2. úkol

Žáci si najdou na internetu popis a obrázek a obrázek zjednodušeně nakreslí.

3. – 4. úkol

Žáci hledají to, co má tvar válce. Ustříhnou proužek papíru a namotají ho na válec, poté napíšou do řádků tajný vzkaz, zbytek písmen napíší náhodně. Poté papírek odmotají a odchází zpět do třídy.

5. úkol

Žáci se vrací zpět do tělocvičny a snaží se hledat všechny věci, které mají tvar válce. Postupně zkouší na každý z nich svůj vylosovaný proužek papíru namotat a hledají ten správný, který danou šifru odhalí.

Pracovní list č. 8: Zadání

1. Podle klíče rozlušti tajnou zprávu.

55 24 24 43 44 2413 3424 1543 25 54 44 11 31 15

……..…….……...

	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

2. Nakresli to, co ti vyšlo v tajné zprávě.

3. Vezmi si tužku a papír a jdi do tělocvičny, kde se pokus sestrojit to, co ti vyšlo v tajné zprávě.

4. Zašifruj pomocí toho svou tajnou zprávu a někam ji ukryj.

5. Vylosuj si jeden lísteček s tajným vzkazem od svého spolužáka a pokus se ho rozluštit.

……

……

……

4.2 Reflexe pracovních listů

Po zadání pracovních listů v praxi a jejich vyplňování ať už společně s žáky nebo jejich samostatnou prací jsem došla k závěru, že je práce s šiframi velmi bavila. Děti aktivně spolupracovaly a těšily se, až své umění ukrýt text do tajného písma ukáží dalším lidem v jejich okolí. Všechny mnou zadané pracovní listy zvládla většina žáků vyplnit samostatně bez pomoci, takže jsem dokázala odhadnout jejich znalosti. Naopak bych řekla, že některé šifry mohly být o něco těžší, aby si nadanější žáci museli více lámat hlavu s jejich řešením, ale naopak jsem ráda, že i slabší žáci zažili pocit úspěchu z jejich vyřešení.

Mrzí mě, že jsem kvůli epidemiologické situaci neměla možnost vidět práci a snahu u řešení pracovních listů dětí ve 4. a 5. ročníku. Dva pracovní listy jsem musela zadat distančně a poté zpětně s dětmi diskutovat o tom, jak jednotlivá cvičení řešily, jak se jim dařilo, co a proč jim přišlo těžké. Také mě mrzí, že vzhledem k pandemii koronaviru nebyla možnost vyzkoušet více didaktických her, ve kterých se vyskytuje řešení šifer. Zvláště by mě zajímala didaktická hra, kterou najdete jako pracovní list č. 3, kde by děti řešily nejen šifry, ale i orientaci podle mapy v přírodě a navíc by k práci musely použít moderní technologie, jako jsou tablety a mobilní telefony. Navíc by se naučily, jak pracovat s QR kódy. Doufám, že tento pracovní list budu mít možnost v co nejbližší době vyzkoušet v praxi.

5 Závěr

V diplomové práci jsem se především zaměřila na pojem šifry, na jejich druhy, historii a jejich využití ve světě dnes a v minulosti.

Cílem diplomové práce bylo seznámit pedagogy se základními a jednoduchými šiframi, které lze použít v hodinách matematiky na 1. stupni základní školy. Dále bylo cílem vytvořit sadu pracovních listů, pomocí kterých se děti seznámí zábavnou formou s různými druhy šifer z minulosti, ale i současnosti a naučí se, jak dešifrovat daný text a zašifrovat vlastní myšlenky a slova. Na základě odborné literatury byly popsány základní šifry, jejich historie, šifrovací hry a didaktické hry. Byly vytvořeny pracovní listy a didaktické hry, které obsahují jednoduché šifry odpovídající učivu na 1. stupni základní školy.

Práce se dělí na teoretickou část a na praktickou část. V teoretické části je popis základních pojmů, které souvisejí s šifrováním, druhy šifer, jejich historie od počátku až po současnost. Šifrování je dnes již běžnou součástí našeho života a setkáváme se s ním prakticky všude. Dále také uvádím příklady šifrovacích her. Propojuji šifry s kurikulem, neboli uvádím, jakou mají šifry návaznost na rámcově vzdělávací program pro základní vzdělávání (RVP ZV), a nakonec vysvětluji, co je to vůbec didaktická hra. V praktické části se věnuji především tvorbě pracovních listů, jejich popisu, jak s nimi pracovat, co k danému pracovnímu listu potřebujeme za pomůcky, jaké znalosti žáci potřebují ke správnému řešení a naopak jaké znalosti by žáci měli po vyplnění jednotlivých pracovních listů získat. Dále v praktické části naleznete u každého pracovního listu návody řešení, jak dané šifry řešit, jejich správná řešení a také zadání, které lze předat žákům k vypracováním. Nakonec u vyzkoušených pracovních listů v praxi jsem popsala jednotlivá řešení žáků, jejich správná, ale i špatná řešení a jejich celkový přístup ke hrám. Lze tedy konstatovat, že cíl i dílčí cíle práce byly splněny.

Závěrem bych chtěla poděkovat všem lidem, kteří byli ochotni mi s psaním mé diplomové práce pomoci. I když tvorba této práce zabrala spoustu času, tak jsem ráda, že jsem mohla zpracovávat právě toto téma. Moc mě bavilo vytvářet pracovní listy s šiframi a ještě více mě bavilo je zadávat dětem a vidět jejich nadšení a to, že je práce s nimi moc baví. Vypracování pracovních listů mělo smysl, což mě nabilo energií a optimismem.

Určitě je během své pedagogické praxe ještě několikrát použiji a budu ráda, když je využijí i ostatní pedagogové a seznámí tak i svoje žáky s šiframi.

6 Zdroje

Literární zdroje

BEČVÁŘOVÁ, Zuzana. *Současná mateřská škola a její řízení.* Praha: Portál, 2003. ISBN 80-7178-537-7.

BITTO, Ondřej. *Šifrování a biometrika, aneb, Tajemné bity a dotyky.* Kralice na Hané: Computer Media, 2005. ISBN 80-86686-48-5.

HANŽL, Tomáš, Radek PELÁNEK a Ondřej VÝBORNÝ. *Šifry a hry s nimi: kolektivní outdoorové hry se šiframi.* Praha: Portál, 2007. ISBN 978-80-7367-196-9.

HOUŠKA, Tomáš. *Škola hrou: knížka pro učitele a rodiče všech školáků.* Praha: Tomáš Houška, 1991. ISBN 80-900704-7-7.

HOUŠKA, Tomáš. *Škola je hra.* 2. přeprac. a rozš. vyd. Praha: vl. n., 1993. ISBN 80-900704-9-3.

JANEČEK, Jiří. *Odhalená tajemství šifrovacích klíčů minulosti: ruční šifry.* Praha: Naše vojsko, 1994. Mozaika (Naše vojsko). ISBN 80-206-0462-6.

JAŠEK, Roman. *Informační a datová bezpečnost.* Zlín: Univerzita Tomáše Bati ve Zlíně, 2006. ISBN 80-7318-456-7.

JIROUŠEK, Radim. *Principy digitální komunikace*. Voznice: Leda, 2006. ISBN 80-7335-084-X.

KALHOUS, Zdeněk a Otto OBST. *Didaktika sekundární školy*. Olomouc: Univerzita Palackého, 2003. ISBN 80-244-0599-7.

KOTRBA, Tomáš a Lubor LACINA. *Aktivizační metody ve výuce: příručka moderního pedagoga*. 2., přeprac. a dopl. vyd. Brno: Barrister & Principal, 2011. ISBN 978-80-87474-34-1.

MAŇÁK, Josef. *Alternativní metody a postupy*. Brno: Masarykova univerzita, 1997. ISBN 80-210-1549-7.

MAŇÁK, Josef, Tomáš JANÍK a Vlastimil ŠVEC. *Kurikulum v současné škole*. Brno: Paido, 2008. Pedagogický výzkum v teorii a praxi. ISBN 978-80-7315-175-1.

MAŇÁK, Josef a Vlastimil ŠVEC. *Výukové metody*. Brno: Paido, 2003. ISBN 80-7315-039-5.

MANNIOVÁ, Jolana. *Tvorivosť a didaktická hra vo vyučovaní.* Pedagogická orientace č. 3. Brno: Česká pedagogická společnost v nakladatelství KONVOJ, 2001.

MENEZES, Alfred J., Paul C. van OORSCHOT a Scott A. VANSTONE. *Handbook of applied cryptography*. Boca Raton: CRC Press, 1997. ISBN 0-8493-8523-7.

PIEKALKIEWICZ, Janusz. *Historie špionáže: agenti - systémy - akce*. Praha: Naše vojsko, 2004. ISBN 80-206-0738-2.

PIPER, Fred a MURPHY, Sean. *Kryptografie: Průvodce pro každého*. Praha: Dokořán, 2006. ISBN 80-7363-074-5.

PROKOPIČ, David. *Historie šifrování od starověku do novověku* [Bakalářská práce]. Praha: Univerzita Karlova, Filozofická fakulta, 2008.

PRŮCHA, Jan, Eliška WALTEROVÁ a Jiří MAREŠ. *Pedagogický slovník*. 6.,aktualiz. a rozš. vyd. Praha: Portál, 2009. ISBN 978-80-7367-647-6.

PRŮCHA, Jan, Jiří MAREŠ a Eliška WALTEROVÁ. *Pedagogický slovník*. 4. aktualiz. vyd. Praha: Portál, 2003. ISBN 80-7178-772-8.

PŘÍHODA, Václav. *Úvod do pedagogické psychologie*. Praha: Státní pedagogické nakladatelství, 1956.

SANTLEROVÁ, Květoslava. *100 didaktických her ve výuce čtení a psaní*. Vydání druhé. Brno: Učebnice a knihy, 1995.

SINGH, Simon. *Kniha kódů a šifer: tajná komunikace od starého Egypta po kvantovou kryptografii*. Praha: Dokořán, 2003. Aliter (Argo: Dokořán). ISBN 80-86569-18-7.

SIXTA, Josef a Václav MAČÁT. *Logistika: teorie a praxe*. Brno: CP Books, 2005. Business books (CP Books). ISBN 80-251-0573-3.

STŘELEC, Stanislav. *Studie z teorie a metodiky výchovy I.* 2. vyd. Brno: Katedra pedagogiky Pedagogické fakulty MU, 2004. ISBN 80-86633-21-7.

SVOBODOVÁ, Eva. *Vzdělávání v mateřské škole: školní a třídní vzdělávací program*. Praha: Portál, 2010. ISBN 978-80-7367-774-9.

TIHON, Karel. *Implementace čárového kódu do výrobního procesu malé firmy* [Diplomová práce]. Brno: Vysoké učení technické, Fakulta elektrotechniky a komunikačních technologií, 2009.

VONDRUŠKA, Pavel. *Kryptologie, šifrování a tajná písma*. Praha: Albatros, 2006. Oko (Albatros). ISBN 80-00-01888-8.

ZORMANOVÁ, Lucie. *Obecná didaktika: Pro studium v praxi*. Praha: Grada Publishing, 2014. ISBN 978-80-247-4590-9.

Elektronické zdroje

APOGEUM, 2006. *Josef Smýkal: Tyflopedický lexikon jmenný – BRAILLE, Louis* [online]. [cit. 2021-03-24]. Dostupné z: <http://www.apogeum.info/tlex/heslo.php?id=137>

CRYPTO-WORLD, 2007. *Leon Battista Alberti (první polyalfabetický šifrový systém, kotouč)* [online]. [cit. 2021-03-24]. Dostupné z: <http://crypto-world.info/casop9/crypto06_07.pdf>

EPRIN, 2010. *Historie čárového kódu* [online]. [cit. 2021-03-24]. Dostupné z: <http://www.eprin.cz/reseni/technologie/obecne-carove-kody>

MILITARY RANGE, 2019. *Historie Morseovy abecedy* [online]. [cit. 2021-03-21]. Dostupné z: <https://militaryrange.com/novinka-historie-morseovy-abecedy--1>

NÁRODNÍ ÚSTAV PRO VZDĚLÁVÁNÍ, 2017. *RVP ZV 2017* [online]. [cit. 2021-03-24]. Dostupné z: <http://www.nuv.cz/t/rvp-pro-zakladni-vzdelavani>

NATIONAL GEOGRAPHIC, 2012. *60 let s čárovým kódem: pochopte jeho anatomii* [online]. [cit. 2021-03-24]. Dostupné z: <https://www.national-geographic.cz/clanky/60-let-s-carovym-kodem-pochopte-jeho-anatomii.html?photo=1>

SVĚT HARDWARE, 2017. *Profesor koupil "psací stroj" za 100 EUR, byla to Enigma za 45.000 EUR* [online]. [cit. 2021-03-10]. Dostupné z: <

https://www.svethardware.cz/profesor-koupil-psaci-stroj-za-100-eur-byla-to-enigma-za-45-000-eur/44794>

SVĚT HARDWARE, 2009. *Šifrování a biometrie pod drobnohledem* [online]. [cit. 2021-03-20]. Dostupné z: <https://www.svethardware.cz/sifrovani-a-biometrie-pod-drobnohledem/25723>

SVĚTLO pro svět, 2014. *4.1. - Světový den Braillova písma* [online]. [cit. 2021-03-20]. Dostupné z:<https://www.svetloprosvet.cz/41-svetovy-den-braillova-pisma>

THE EPOCH TIMES, 2008. *Tajemství šifer - po stopách kryptografie a steganografie V* [online]. [cit. 2021-03-24]. Dostupné z: <https://www.epochtimes.cz/200807295638/Tajemstvi-sifer-po-stopach-kryptografie-a-steganografie-V.html>

WIKIPEDIA, 2021a. *Skytalé* [online]. [cit. 2021-03-24]. Dostupné z: < https://cs.wikipedia.org/wiki/Skytal%C3%A9>

WIKIPEDIA, 2021b. *Alberti cipher* [online]. [cit. 2021-03-24]. Dostupné z: <https://en.wikipedia.org/wiki/Alberti_cipher>

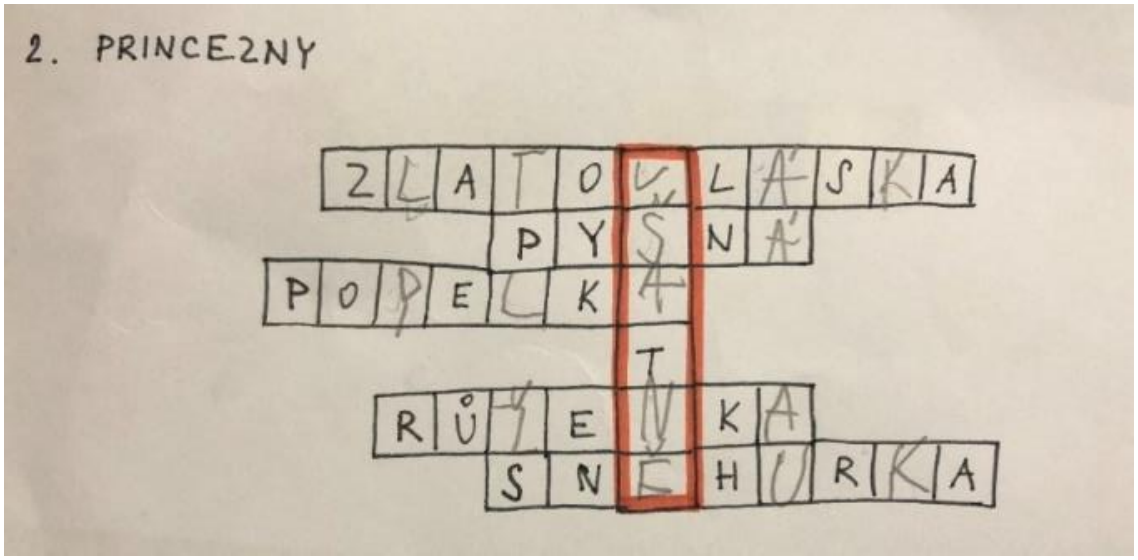
WIKIPEDIA, 2021c. *Vigenèrova šifra* [online]. [cit. 2021-03-24]. Dostupné z: < https://cs.wikipedia.org/wiki/Vigen%C3%A8rova_%C5%A1ifra>

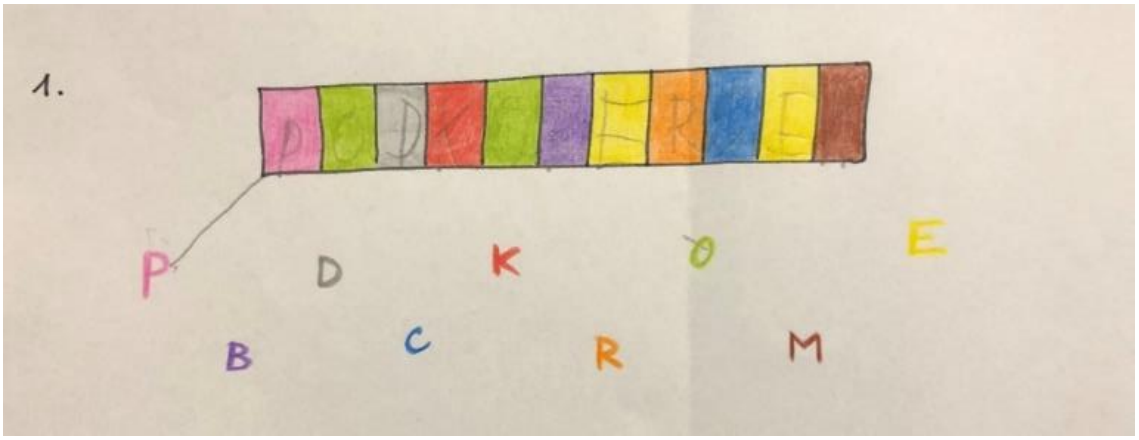
7 Seznam obrázků

8 Seznam příloh

9 Přílohy

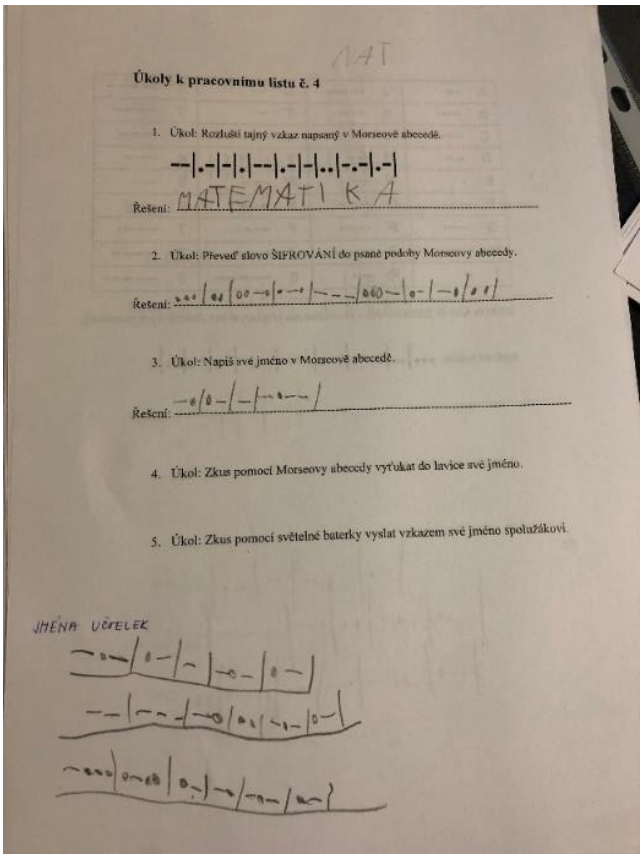
Příloha č. 1 Řešení dětí pracovního listu č. 1





Příloha č. 2 Fotografie žáků při řešení pracovního listu č. 1

Příloha č. 3 Řešení dětí pracovního listu č. 4



Úkoly k pracovnímu listu č. 4

1. Úkol: Rozluští tajný vzkaz napsaný v Morseově abecedě.

--|.-|-|.|--|.-|-|..|-.-|.-|

Řešení: MATEMATIKA

2. Úkol: Převeď slovo ŠIFROVÁNÍ do psané podoby Morseovy abecedy.

Řešení:

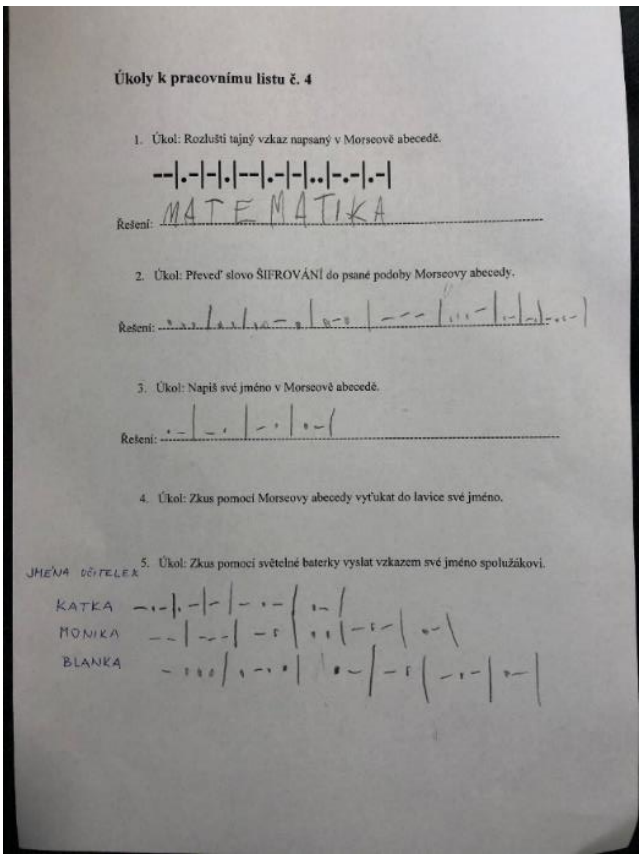
3. Úkol: Napiš své jméno v Morseově abecedě.

Řešení:

4. Úkol: Zkus pomocí Morseovy abecedy vyťukat do lavice své jméno.

5. Úkol: Zkus pomocí světelné baterky vyslat vzkazem své jméno spolužákovi.

JMÉNA UČITELEK



Úkoly k pracovnímu listu č. 4

1. Úkol: Rozluští tajný vzkaz napsaný v Morseově abecedě.

--|.-|-|.|--|.-|-|..|-.-|.-|

Řešení: MATEMATIKA

2. Úkol: Převeď slovo ŠIFROVÁNÍ do psané podoby Morseovy abecedy.

Řešení:

3. Úkol: Napiš své jméno v Morseově abecedě.

Řešení:

4. Úkol: Zkus pomocí Morseovy abecedy vyťukat do lavice své jméno.

5. Úkol: Zkus pomocí světelné baterky vyslat vzkazem své jméno spolužákovi.

JMÉNA UČITELEK

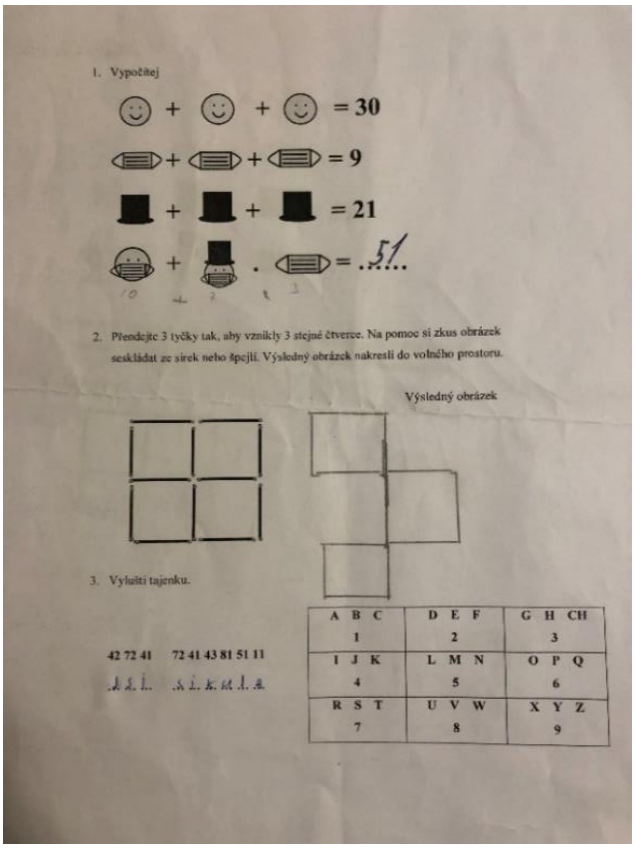
KATKA

MONIKA

BLANKA

Příloha č. 4 Fotografie žáků při řešení pracovního listu č. 4

Příloha č. 5 Řešení dětí pracovního listu č. 6



1. Vypočítej

☺ + ☺ + ☺ = 30

😷 + 😷 + 😷 = 9

🎩 + 🎩 + 🎩 = 21

😷 + 🎩 . 😷 = 51

10 + 2 · 3

2. Přendejte 3 tyčky tak, aby vznikly 3 stejné čtverce. Na pomoc si zkus obrázek seskládat ze sirek nebo špejlí. Výsledný obrázek nakresli do volného prostoru.

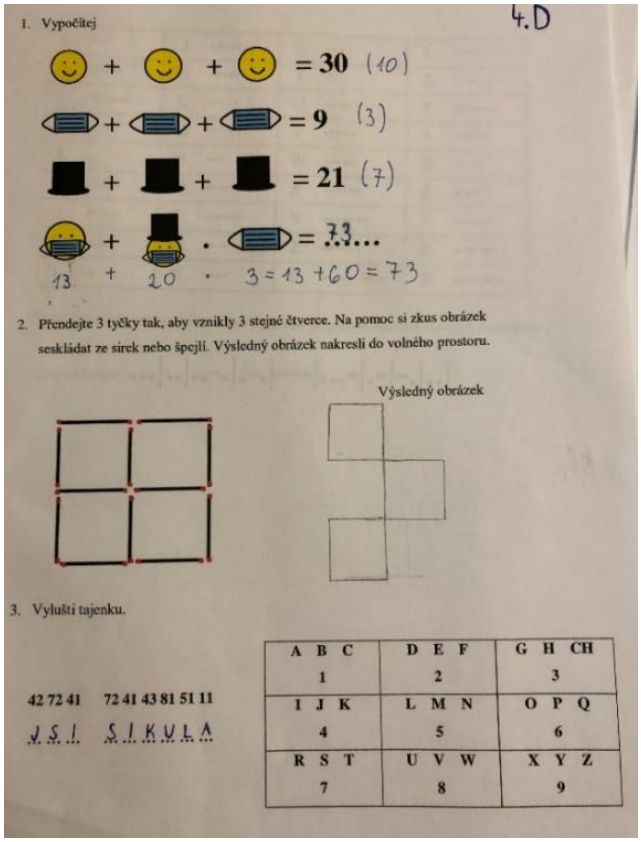
Výsledný obrázek

3. Vyluští tajenku.

A B C	D E F	G H CH
1	2	3
I J K	L M N	O P Q
4	5	6
R S T	U V W	X Y Z
7	8	9

42 72 41 72 41 43 81 51 11

J S I S I K U L A



1. Vypočítej

4.D

☺ + ☺ + ☺ = 30 (10)

😷 + 😷 + 😷 = 9 (3)

🎩 + 🎩 + 🎩 = 21 (7)

😷 + 🎩 . 😷 = 73...

13 + 20 · 3 = 13 + 60 = 73

2. Přendejte 3 tyčky tak, aby vznikly 3 stejné čtverce. Na pomoc si zkus obrázek seskládat ze sirek nebo špejlí. Výsledný obrázek nakresli do volného prostoru.

Výsledný obrázek

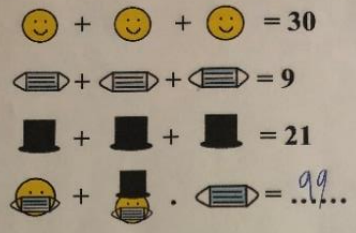
3. Vyluští tajenku.

A B C	D E F	G H CH
1	2	3
I J K	L M N	O P Q
4	5	6
R S T	U V W	X Y Z
7	8	9

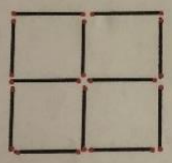
42 72 41 72 41 43 81 51 11

J S I S I K U L A

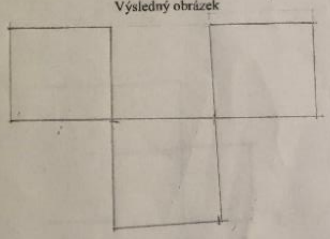
1. Vypočítej



2. Přendejte 3 tyčky tak, aby vznikly 3 stejné čtverce. Na pomoc si zkus obrázek seskládat ze sirek nebo špejlí. Výsledný obrázek nakresli do volného prostoru.



Výsledný obrázek



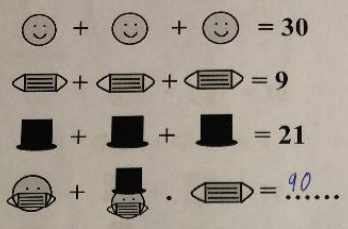
3. Vylušti tajenku.

A B C	D E F	G H CH
1	2	3
I J K	L M N	O P Q
4	5	6
R S T	U V W	X Y Z
7	8	9

42 72 41 72 41 43 81 51 11

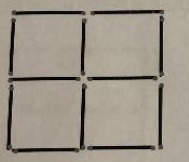
JSI SIKVLA

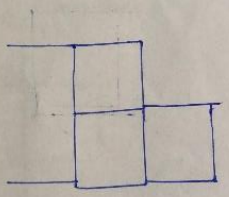
1. Vypočítej



2. Přendejte 3 tyčky tak, aby vznikly 3 stejné čtverce. Na pomoc si zkus obrázek seskládat ze sirek nebo špejlí. Výsledný obrázek nakresli do volného prostoru.

Výsledný obrázek





3. Vylušti tajenku.

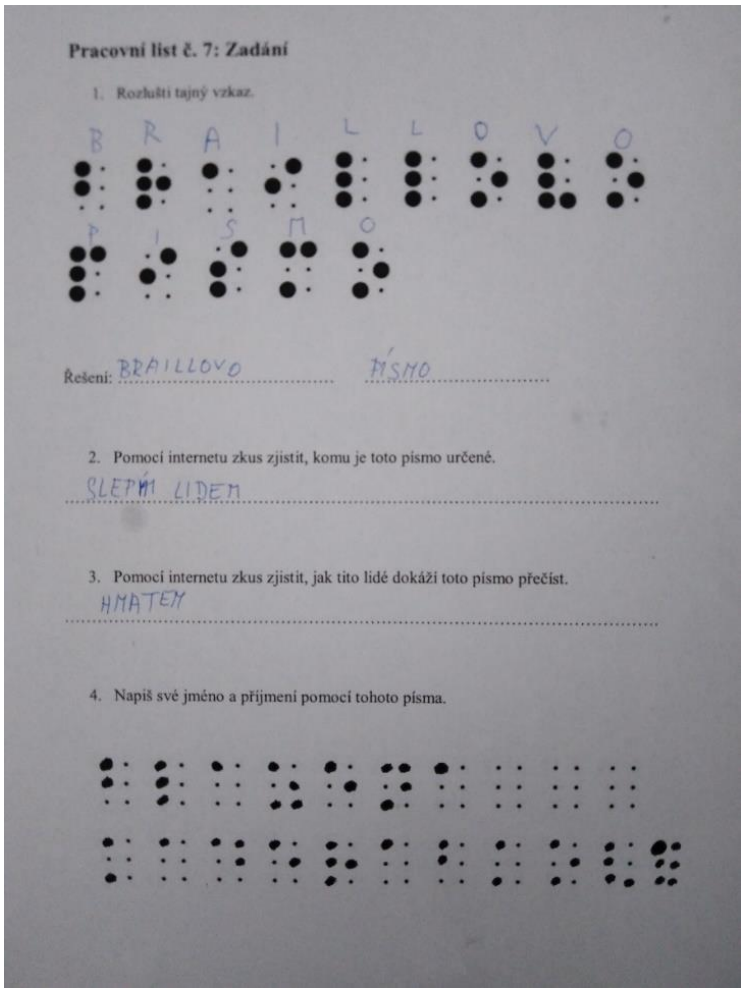
A B C	D E F	G H CH
1	2	3
I J K	L M N	O P Q
4	5	6
R S T	U V W	X Y Z
7	8	9

42 72 41 72 41 43 81 51 11

... ...

JSI SIKVLA

Příloha č. 6 Řešení dětí pracovního listu č. 7



Pracovní list č. 7: Zadání

1. Rozluštěte tajný vzkaz.

B R A I L L O V O

P I S M O

Řešení: BRAILLOVO PÍSMO

2. Pomocí internetu zkus zjistit, komu je toto písmo určené.

SLEPÝM LIDEM

3. Pomocí internetu zkus zjistit, jak tito lidé dokáží toto písmo přečíst.

HMATEM

4. Napiš své jméno a příjmení pomocí tohoto písma.