




Čas přípravy	Čas realizace	Prostor	Roční období	Počet účastníků	Věková kategorie
120 minut	**90–120 minut**	**kdekoli**	**kdykoli**	**4 a více**	**6.–7. třída**

JE NEBO NENÍ KRYPTOLOGIE OD SLOVA KRYPTA?

Obecný cíl:

Rozvoj těchto kompetencí: k řešení problémů, komunikaci, sociální a personální.

Konkrétní cíl:

Dítě se učí při řešení úloh hledat shodné, podobné a odlišné znaky a na základě toho zkouší aplikovat známé metody a postupy. Chápe potřebu efektivní spolupráce a účinně spolupracuje v týmu.

Motivace:

Potřeba zaslat tajnou zprávu tak, aby ji nežádaný nálezce nebo nepřítel, který odhalí posla, nerozluštil, vznikla již v dávné době. Například Julius Caesar používal pro vojenskou komunikaci v šifrování zpráv posun o tři místa v abecedě. Tento způsob kódování popsal ve svých Zápiscích o válce galské a po něm nese i označení Caesarova šifra.

Pokud máme k dispozici klíč, je pro nás vyluštění zprávy snadné, ale někdy se stane, že potřebujeme vyluštit zprávu, ke které klíč nemáme, a tady nastupuje bádání a hledání podobných znaků, které nám napoví, jaký způsob pro vyluštění zakódované zprávy použít. Vychází-li kódování z některého známého postupu, stačí jej najít. Není-li žádný běžný způsob použit, může nás čekat mravenčí práce, než zprávu rozluštíme.

Legenda:

Legenda č. 1: **Robot**

Jsme v roce 2049, roboti se pro lidstvo stali naprosto nepostradatelnými. V poslední době ale začali roboti sestrojení pro práci v nebezpečných oblastech mizet. Tým odborníků se domnívá, že jejich operační systém napadá virus, který má za následek, že jejich řízení přebere někdo jiný a roboti prostě zmizí. Váš tým techniků dostal za úkol jednoho ze zmizelých robotů třetí generace najít. Jeho ztráta by pro lidstvo byla velmi citelná. Naštěstí je tento robot vybaven bezpečnostním systémem a robot začal vysílat krátké zakódované zprávy tak, aby je „únosce“ nemohl vystopovat. Jeho poslední srozumitelná zpráva byla: Byl proveden zásah do operačního systému, spouštím bezpečnostní systém. Další zpráva už byla v zašifrované podobě.

Legenda č. 2**: Honba za pokladem**

Starý korzár ukryl svůj pohádkový poklad na ostrově, u kterého jste právě přistáli. Proto, aby vždy našel správnou cestu ke skrýši s pokladem, si cestou nechával kratičké zprávy, které rozluštil jenom sám. Ono také tehdy neumělo mnoho pirátů číst a psát. Povede se vám poklad najít? Stačí jít po jeho stopách a hledat zakódované zprávy, které vás k pokladu zavedou.

Legenda č. 3: **Záchranná mise**

Průzkumná jednotka byla při plnění svého úkolu zajata nepřítelem. Z místa, kde byli vojáci zajati, se jim podařilo ještě zaslat poslední zprávu. Protože jeden ze zajatých průzkumníků, kdysi působil v šifrovacím středisku a umí kódovat zprávy tak, aby je nepřítel nedokázal rozluštit, domnívá se velení, že by se mohl cestou pokusit zanechat informaci o jejich pozici. Vy jste vybráni jako členové záchranné mise, která má za úkol vypátrat, kde nepřítel zajatce ukrývá, a osvobodit je. Podrobnější instrukce vám budou předány písemně.

Provedení:

Šifrovací hru je dobré zařadit až potom, co si o šifrování a kódování zpráv s dětmi popovídáme a základní způsoby kódování (například Morseovu abecedu, malý a velký polský kříž,…) probereme a vyzkoušíme je s nimi.

Samotná šifrovací hra je nastavena tak, že na své cestě děti nacházejí zašifrované zprávy, kdy po vyluštění zprávy zjistí, kam mají dále pokračovat.

Pro tuto aktivitu nejprve vytipujeme trasu, po které by se měla cesta ubírat, všímáme si zajímavých míst, která bude možné použít jako orientační body a budeme je moci zakódovat do zpráv.

Tam, kde to není zcela jasné, je důležité upřesnit, zda je používáno písmeno CH nebo jej skládáme ze znaků pro C a H.

Pokud děti neumí různé abecedy a šifry z paměti, poskytneme jim k řešení úloh sadu šifrovacích pomůcek (některé mohou být i navíc.)

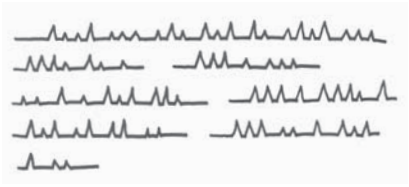
Morseovka stokrát jinak

Pro využití Morseovy abecedy ke kódování zpráv potřebujeme minimálně dva rozdílné typy znaků (tečka, čárka) případně lze ještě využít další znaky pro oddělování písmen a slov.

Zprávu je možné zakódovat například na plát pily, kdy využijeme celých a ulomených zubů, dále lze použít ve zprávě malá a velká písmena, kdy malé písmeno značí tečku a kapitálka čárku.

K zakódování zprávy je možné využít klasické provedení, tedy tečky a čárky. Pokud však chceme, aby byla zpráva zajímavější, můžeme k zakódování zprávy využít tzv. klínové písmo. Ležatý znak je tečka a stojatý znak je čárka.

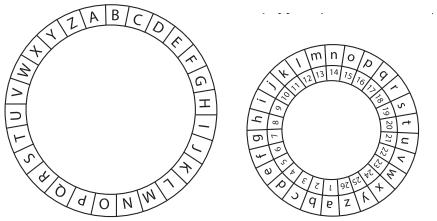
Příklad zprávy: *pokračovat sto metrů severním směrem*



Ke kódování lze využít i obrácené znaky, tedy v tomto případě dlouhý zub pily značí tečku a krátký zub pily značí čárku. Použijeme-li při luštění zprávy předpoklad, že krátký zub je tečka a dlouhý zub je čárka, je již z prvních shluků zubů (XSRKN) patrné, že nám nevychází smysluplný text. Následující znak • – • – v morseově abecedě nenajdeme a lze usuzovat, že způsob kódování je převrácený, tedy velký zub je tečka a malý zub je čárka.

Dětem, pokud je to nutné, můžeme způsob řešení naznačit, případně mohou získat nápovědu, která bude penalizována například jedním trestným bodem (to v případě, že se jedná o šifrovací soutěž).

Caesarova šifra nebo abecední posun



Velmi často lze použít k zakódování zprávy i abecední posun. Posun může být například o předem dohodnutý počet znaků například +2 (v tom případě se správné písmeno posouvá o dvě písmena vpřed tedy A je v zašifrovaném textu C) nebo -5 (v tom případě se správné písmeno posouvá o pět písmen zpět tedy A je v zašifrovaném textu V).

Pokud chceme dětem šifrování usnadnit, je dobré do šifrovacích pomůcek přidat i šifrovací kolečko. Nebo si jej děti mohou na schůzkách vyrobit.

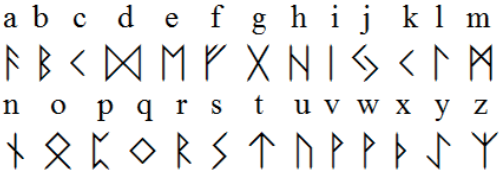
Příklad zprávy: *nyní vpravo až tam, kde se kříží velké cesty*

Můžeme to provést tak, že použijeme standardní Caesarovu šifru, kdy je posun v abecedě o 3 písmena vpřed, tedy N=K, Y=V, a zašifrovaný text, použijeme-li abecedu bez CH, bude vypadat:

KVKF SMOXSL XW QXJ, HAB PB HOFWF SBIHB ZBPQV

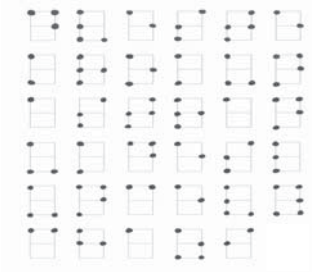
Runové písmo a speciální abecedy

Pokud používáme k zakódování speciální abecedu – například runové písmo, je nutné dětem klíč k abecedě poskytnout. Budeme-li tvořit vlastní abecedu, musíme dát pozor na to, aby znaky byly vždy jednoznačné a vzájemně nezaměnitelné.



Příklad zprávy: *dvě stě kroků na stranu, kde slunce vychází*

Využít můžeme například staré runové písmo (Starší futhark, který má 24 znaků a používaly jej germánské národy), které se objevilo i v knihách spisovatele J. R. R. Tolkiena. Pokud tuto abecedu budeme používat, je nutné děti upozornit na to, že je totožný znak pro C a K a totožný znak pro V a W. Děti pak musí vyzkoušet, který znak se do vyluštěného textu hodí lépe. Případně si můžeme znaky upravit tak, aby byly jednoznačné.



K zakódování zprávy lze využít i Braillovo písmo. Toto písmo je vytvořeno pro nevidomé, kdy jednotlivá písmena se skládají ze tří teček ve dvou sloupcích. Chceme-li dětem šifrování usnadnit, naznačíme spojnice mezi jednotlivými tečkami, aby byla písmenka snáze rozpoznatelná. Využijeme-li toto písmo k zakódování zprávy, je vhodné dětem do šifrovacích pomůcek tuto abecedu přidat.

Písmenka v mřížkách

Pro šifrování můžeme použít i klasické šifry, které vycházejí z rozložení písmen do různých tabulek.

Příklad zprávy: *označený strom sto padesát kroků na jihozápad*

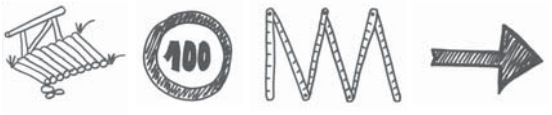
Pro vyluštění zprávy zašifrované Velkým polským křížem nemusíme dětem dávat žádné pomůcky. Pouze se musíme domluvit na tom, zda používáme všechna písmena – tedy i Ch.

Pokud použijeme Malý polský kříž, nezapomeneme při nácviku této šifry zdůraznit skutečnost, že v mřížkách není využité písmeno Ch.

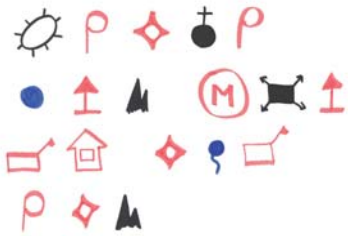
Obrázkové zprávy

Mezi oblíbené šifry patří ty obrázkové. Možná proto, že si luštitelé myslí, že je nečekají žádné komplikované posuny, nemusí pracovat se šifrovacími pomůckami a být tak pozorní.

Příklad zprávy: *lávka 100 metrů vpravo*



Jednoduché obrázky poskládané za sebou navedou luštitele správným směrem. Stačí je jen správně pojmenovat – lávka, 100, metr, vpravo.



Pro zakódování zprávy můžeme použít například i mapové značky. Kdy pro rozluštění zprávy je použito vždy první písmeno názvu mapové značky. Zpráva pak může vypadat takto: lom, autobusová zastávka, vyhlídka, kostel, autobusová zastávka, studánka, turistický přístřešek, osamělá skála, muzeum, elektrárna, turistický přístřešek, restaurace, ubytovna, vyhlídka, pramen, restaurace, autobusová zastávka, vyhlídka, osamělá skála). Zároveň taková šifra je i vhodným nástrojem pro procvičení znalosti mapových značek.

Zdánlivě něco jiného

Zpráva může být ukryta například v textu nebo ve zdánlivě jiném tvaru – například křížovce. Zde už je ale třeba počítat s větší časovou dotací na tvorbu šifry.

Příklad zprávy: *kostel třetí schod*

Chceme-li zašifrovat zprávu do textu, můžeme zvolit například báseň, bajku nebo popis sportovního zápasu. V textu potom použijeme slova, která mají stejné znaky a z nich potom první písmena. V naší bajce jsou to první písmena z názvů zvířat (králík, osel, slavíci, tetřev,..). Dětem dáme zašifrovaný text bez tučně vyznačených počátečních písmen.

Bajka o zvířeti, které chtělo létat

Králík se zase vydal na jednu ze svých výprav a potkal **o**sla. Ten hýkal tak nešťastně, že i **s**lavíci si přestali prozpěvovat. „Proč jsi tak smutný?“ ptal se ho **t**etřev, který o kousek dál vyzobával zrníčka ze země. „Ále, viděl jsem obrázek s ptákem **e**mu a přál bych si být jako on a létat. „Ty jsi ale **l**ama“, řekl **t**etřev. „**R**opucha mi povídala, že **e**mu je běžec a nelétá. To by sis moc nepomohl.“ A **t**etřev pokračoval „To už je lepší, být **i**bis. Ten létá.“ **S**rna, která to všechno pozorovala zpovzdálí, řekla: „To já bych raději byla **ch**řástal. Patří mezi tažné opeřence a podívá se i po světě.“ **O**sel se nad tím vším zamyslel, pokýval hlavou, zahýkal a vydal se k domovu. Cestou ještě potkal spícího **d**udka a byl moc rád, že ten spí a nic mu neříká. Protože by měl z toho všeho zamotanou hlavu ještě víc.

Pokud použijeme doplňovačku, je vhodné děti upozornit na to, že tajenka nemusí mít vždy správně diakritiku.

Zadání

			černý zpěvný pták
			zkratka pro telefon
			Italsky tři
			jedovatý jehličnatý keř
			obyvatel z okolí Domažlicka

Řešení

K	O	S	černý zpěvný pták
T	E	L	zkratka pro telefon
T	R	E	Italsky tři
T	I	S	jedovatý jehličnatý keř
CH	O	D	obyvatel z okolí Domažlicka

Na internetu lze najít i stránky, které vám po zadání textu, jenž chcete zašifrovat, vyhotoví zakódovanou zprávu, stačí do vyhledávače zadat třeba slovo „šifrátor".

S oddílovými dětmi můžeme vyzkoušet i účast na nějaké šifrovací hře, kterou organizuje někdo jiný. Pokud máte chuť se zúčastnit nějaké takové hry, můžete vyhledat vhodnou právě pro vás v kalendáriu šifrovacích her www.sifrovacky.cz/kalendar/. Na takovou šifrovačku je třeba se pořádně připravit. Na webu www.sifrovacky.cz najde návštěvník informace, které se mohou hodit.

Pokud se chceme šifrováním více zabývat, je dobré si k tomu nastudovat různé materiály. Vhodný je například manuál Tmou, který vytvořili pro začátečníky pořadatelé stejnojmenné šifrovací hry.

Na tuto aktivitu navazuje v rámci pionýrských akcí a soutěží Pionýrská Stezka.

Tento metodický list pomáhá naplňovat Ideály Pionýra: Poznání a Překonání.

Přístup k dětem se specifickými vzdělávacími potřebami:

Dětem, které mají poruchu soustředění, umožníme luštit spíše zprávy, u kterých nezáleží na drobné nepozornosti, vhodné jsou například obrázkové šifry.

Dětem s potížemi ve čtení dopřejeme více času, případně text zkrátíme. U dětí, které mají potíže se psaním, dáváme pozor, aby si šifru špatně nepřepsaly.

Je vhodné, aby děti měly k dispozici papír na zápis, a to i tam, kde by toho nemuselo být zapotřebí.

Náročnost šifer přizpůsobujeme schopnostem dítěte tak, že uspět mohou i děti méně nadané.

Pozor na:

Jednoznačné zadání cílů ve zprávách. Nutno zajistit, aby děti nesešly z trasy, a pokud se to stane, tak je navést na správnou cestu (například doplňkovou šifrou, možností vzít si nápovědu).

Sadu úloh k luštění je nutné vždy nechat zkontrolovat více lidmi. Při kontrole ověřujeme, zda je zvolený způsob kódování jednoznačný (nelze vyluštit jiným způsobem a získat tak špatně další cíl cesty) a zda je kódování provedeno správně (nenachází se v zakódovaném textu chyba).

Moje poznámky: