

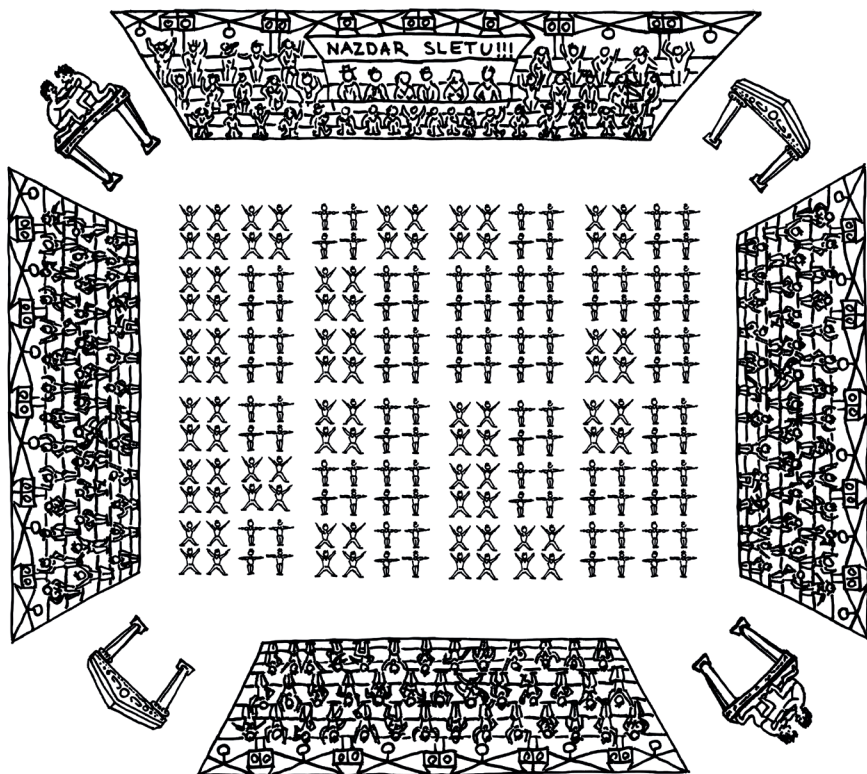
Červen 2025

METODICKÉ LISTY

Samostatná příloha časopisu Sokol

Jak na šifry

Kateřina Pohlová



Z OBSAHU

Úvodní slovo • Organizace šifrovacích her • Šifra • Pojmy a historie •
Abeceda a čísla • Šifry pomocí kódovacích systémů • Jak luštit •

ÚVODNÍ SLOVO

Letos v roce 2025 se bude již po jedenácté konat Noc sokoloven. Už několik let je tradicí, že má nějaké společné téma napříč republikou. V minulosti jsme vytvářeli z cviků písma, loni bylo tématem sto let od Šupčíkovy zlaté olympijské medaile, a proto jsme do programu zahrnuli lano a uzlování. Před několika lety jsme stavěli tzv. skupiny z lidí a v nedávné minulosti se téma točilo kolem hudby.

Vzdělávatelský odbor, který v rámci České obce sokolské Noc sokoloven pořádá, se letos usnesl, že tímto tématem bude šifrování. Tyto Metodické listy by vás mohly navést, jak lze se šiframi pracovat v dětských kolektivech. A nejen v nich, i dospělí mají rádi hádanky.

Já jsem se s prvními šiframi setkala jako malá na táborech a ve skautu. Text byl skryt skrze morseovku a polský kříž. Až teprve v dospělosti jsem se přes zážitkovou pedagogiku seznámila s lidmi, se kterými chodíme na šifrovačky. Pokud tyto hry neprobíhají v online prostředí, pak bývají celodenní nebo celonoční. Na prvním stanovišti je rozdána šifra, a kam jít dál, si už tým musí vyluštit. A mně se tak díky těmto šifrovacím hrám rozšířily zkušenosti a obzory, které bych vám na následujících několika stranách popsala. Příklady šifer, pokud není psáno jinak, jsou moje a lze je dál využít.

Třeba po přečtení těchto Metodických listů založíte v jednotě klub mladých šifrátorů či věrnou gardu luštitelů.

ORGANIZACE ŠIFROVACÍCH HER

Kde se dá šifrovačka hrát

Šifrovací hra se dá připravit v jedné místnosti, po sokolovně, v okolí sokolovny, jako výlet za pokladem, ale i jako celodenní nebo celonoční hra.

Hru můžou hrát buď jednotlivci, nebo týmy.

- V jedné místnosti jednotlivci nebo týmy soutěží mezi sebou, kdo dřív vyluští šifry.
- V prostorách sokolovny můžete hru spojit s orientákem tak, že rozdáte plány sokolovny (třeba použijte ty evakuační) a zakreslíte místa, kde hráči najdou zadání nebo nápovědu k šifrám atp.
- Kolem sokolovny lze rozmístit zadání šifer přímo v terénu.
- Při putování krajinou si hráči můžou nést zadání s sebou, nebo pokud máte dostatek organizátorů, je možné mít stanoviště, kde se šifry rozdávají.

Příklad: V šifrovací městské sokolské hře po Praze, která byla připravena ke sletu v roce 2018, si hráči nesli obálky se šiframi s sebou. Podle mapy znali jen první stanoviště, z šifry měli rozluštit další. Na tom dalším stanovišti se rozhlédli kolem sebe a podle fotky na obálce a předmětu v okolí věděli, jakou další obálku rozbalit. Bylo to například okno, zábradlí, celá budova, dveře atp. Pokud si chcete hlídat, aby týmy nepodváděly a rozbalovaly obálky popořadě, dejte jim navíc falešnou obálku – obálku s fotkou předmětu, který na cestě nepotkají – a chtějte pak vidět, že tuto obálku nerozlepily.

Pro všechny výše zmíněné varianty lze použít k šifrování předměty a prostory kolem sebe. V místnostech třeba nástěnky, v krajině a ve městě jiné prvky. Máte-li zkušenosti s únikovkami, lze takovou hru pro děti udělat i přímo v sokolovně.

Obtížnost

Vždy platí, že obtížnost by se měla přizpůsobit věku a zkušenostem. Chcete-li, aby si to děti užily, zvolte spíš lehčí šifry. Morseovka, Brailleovo písmo, semaforová abeceda nebo polský kříž (a i další) jsou velice lehké na vysvětlení a pochopení. A není vždy potřeba je nějak autorsky maskovat, děti si

užijí šifru, i když hned poznají princip jejího luštění. Děti brzy ztrácejí pozornost, proto je lepší dělat šifry s jednoduchým a kratším řešením. Pro mladší luštitelé je také dobré nastavit hru tak, aby nemuseli vyluštit všechny šifry, a vám to zase umožní, že do hry můžete zkusit dát nějakou těžší.

Nápovědy

Chcete-li zkusit těžší šifry, můžete využít systém nápověd. Pro motivaci hráčů je ovšem dobré, když některé šifry vyluští i bez nápovědy. Proto je dobré ty lehčí dát na začátek hry a pak občas i v průběhu. Nápověda by neměla být zadarmo, ale penalizována, aby hráči měli motivaci ji hned nepoužít. Zažila jsem i šifrovačky, kde bylo u jedné šifry nápověd víc. Ačkoli se to nezdá, napsat nápovědu tak, aby pomohla, ale zas neřekla postup řešení, je občas dost náročné. Kromě nápověd můžete do hry zakomponovat i získání postupu řešení, kde popíšete, jak šifru luštit. Anebo rovnou bez vysvětlování napíšete řešení, záleží na typu a obtížnosti šifry.

Příklad: Tým neví, co se šifrou. Jedná se o šifrovačku, kde řešením je, kam jít dál. Nejdříve si vezmou nápovědu, ta nepomůže, poté si vezmou postup řešení, ani ten nepomůže, nakonec řešení samotné. V tomto případě ale za šifru nedostanou žádný bod.

Dnes jsou velké šifrovačky řízeny skrze mobil (internet, aplikace), takže i přes něj si lze zažádat o nápovědu. Nejste-li technicky zdatní a jedná se hru pro několik sokolů a sokolek v okolí sokolovny, mohou si hráči například žádat o radu skrze SMS. Do úvodních materiálů pro hru je ale dobré dát formát, jak by tato SMS měla vypadat, abyste v ní měli vše, co potřebujete vědět (především číslo nebo název týmu a číslo nebo označení šifry). Nechcete, aby byly děti na telefonu? Pak můžete nápovědy napsat na papír a zabalit/zalepit ho tak dobře, že se pozná, že byl rozbalen. Na konci hry vám pak týmy budou nerozbalené nápovědy vracet a vy poznáte, kdo je využil a kdo ne. A pokud máte stanoviště s organizátory, mohou nápovědy sdělovat oni.

Co se při zašifrovávání i šifrování může hodit

- papír, tužka, čtverečkový papír, pravítko
- obálky a samolepicí papír, pastelky
- izolepa a lepidlo
- šifrovací tabulka

- při hledání řešení se spotřebuje i dost papíru, někdy je potřeba psát nebo kreslit přímo do zadání, pokud si ale nejste jisti správným postupem, je dobré psát přes fólii nebo slabý papír (pauzovací)

Chcete-li si se hrou pohrát, můžete zadání nechat ohořet nebo použít k zapečetění pečící vosk nebo vosk ze svíček. Děti to vtáhne více do dějové linky hry.

Testování šifer

Pokud si nejste jistí, zda úroveň šifer je opravdu ideální pro cílovou skupinu, nechte si je otestovat někým, kdo má podobné zkušenosti jako hráči. Ale pozor, nezvládne-li šifru dospělý, neznamená to vždy, že děti na ni nepřijdou. Stejně tak je záhodno si otestovat náročnější třeba celotáborové hry, ve kterých šifry používáte.

Doprovodné programy během šifrování

Luští-li šifry týmy, je dobré dát zadání šifry v několika kopiích, aby s ní mohlo naráz pracovat víc lidí. I tak je možné, že někoho luštění nebude bavit. Proto není od věci vymyslet doprovodné aktivity. Dá se to dobře skloubit třeba i s dáváním nápoděb – například tým dostane nápoděbu za složení básničky, nebo někam doběhne, něco udělá atp. Doprovodné aktivity nemusejí být jen na stanovišti, ale i po cestě při přesunu. Pokud je na stanovišti organizátor, lze vymyslet jakýkoli úkol, pokud není, můžete do zadání šifry vždy vypsát doplňkové úkoly, které jsou například spojeny se znalostmi o přírodě. Například úkol natrhej tu a tu rostlinu, najdi tu a tu šišku atp. Dobrým úkolem, který zabaví, je i rozdělení ohně. Ovšem jen pokud je během hry příhodné a legální místo na jeho rozdělení.

Příklad 1: Jednou jsme poprosili jednoho postaršího bratra sokola, aby na cestě, kudy chodí týmy, předstíral nevolnost. Speciální body navíc pak dostaly ty týmy, které mu samy od sebe pomohly.

Příklad 2: Na jedné hře jsem dostala špalek, ve kterém byla indicie. Naším úkolem bylo ji jakkoli během hry z toho špalku dostat. Některým hráčům se podařilo ho rozkopat silou, můj tým si poprosil o vypůjčení sekery u jednoho z domů.

Příklad 3: Zábavná varianta je, když jeden člen týmu má na zádech slovo, které jiné týmy nemají vidět, a naopak, ostatní týmy se snaží zjistit co nejvíce slov na cizích zádech. Týmy jsou pak ostražité, neshlukují se a mají o soutěživost navíc.

Zadání šifer

Při každé šifrovačce je dobré vysvětlit pravidla a říct, jakým způsobem luštit, zda se smí dohledávat na internetu atp. Důležité je zmínit, podle jaké abecedy se luští, v našich poměrech je to nejčastěji abeceda bez diakritiky v počtu 26 písmen. Může jich ale být i 27, pokud používáte ch. Vhodné je říct, o jaký druh šifer se jedná a co se v šifrách luští (zda slovo nebo umístění další šifry atp.). Šifry, na které se budeme v těchto listech zaměřovat, jsou šifry logické, ale i podle různých principů, jako je morseovka, Brailleovo písmo atd. Hráči jsou zvyklí, že si na tyto hry berou tzv. šifrovací tabulku. Takovou šifrovací tabulku si můžete také pro vaši hru „na míru“ vytvořit a dát do ní šifrovací systémy, které budou ve hře použity. Například když jsme dělali sokolskou městskou hru, do informací ke hře jsme dali morseovku a mapu trasy. Také nezapomeňte účastníkům hry napsat nebo říct, co všechno s sebou budou potřebovat.

Příklady: Šifra je napsána písmem, které je vidět jen při UV světle. Šifra je psána neviditelným písmem a je k přečtení, až když se zahřeje. Šifru nebo její část dostanete při přenosu skrze Bluetooth. V těchto případech nezapomeneme říct týmům, že potřebují UV baterku, sirky nebo zapalovač, telefon se zařízením Bluetooth.

Na co si dát pozor

Dejte si pozor na chyby, ty mohou zkazit dobrý pocit ze hry týmům i vám. Nechte si proto šifry několikrát otestovat. Šifry by měly odpovídat zkušenostem hráčů. Náročné šifry, které nevylušití ani jeden tým, také zkazí náladu hry. A nezapomínejte, že pro hráče jsou nápovědy sice dobré, ale i demotivační.

Hráči občas neodhadnou časovou náročnost hry, proto je někdy namístě jim nastavit tzv. časové brány – tedy dobu, do které by měli dojít na určité stanoviště. Vyřešit se to dá i automatickým posíláním nápověd a případně i řešení, pokud je tým dlouho na jedné šifře a nechce si nápovědu vzít sám od sebe.

Dobře udělaná šifra je taková, která svým vzhledem, grafickým zpracováním, textem, názvem atp. má navádět k řešení. Oproti tomu si dejte pozor, aby

součástí šifry nebyly prvky, které by na sebe strhávaly pozornost, ale přitom s řešením neměly nic společného. A pokud například opravdu trváte na nadbytečném zkrášení šifry, klidně do zadání napište, že to či ono není součástí řešení šifry.

Šifrovací tabulka

S rozvojem a rozšířením šifrovaček vznikly šifrovací tabulky. Někteří z organizátorů si je tvoří na míru pro danou hru. Pro Noc sokoloven a tyto Metodické listy jsme s Jiřím Braným také jednu tabulku udělali. Je to takový tahák pro hráče. Jednotám přihlášeným do Noci sokoloven jich několik zašleme. Pokud jste je nedostali nebo vám nestačí námi dodaný počet, je možné si je z webových stránek Sokola stáhnout, bude i v sokolské Canvě. Předpokládané využití je hlavně pro luštitel. Jen doporučuji je obeznámit s tím, že ve hře nejspíš nevyužijí všechny systémy, které jsou v tabulce zařazeny. A také upozornit hráče, že ne všechny šifry se luští s touto pomůckou (pokud tam tedy máte i šifry založené na znalostech a dedukci nebo googlení). Asi nemusím psát, že je dobré s šifrovací tabulkou hráče nejdříve seznámit a vysvětlit jim, co na ní všechno najdou a jak se s ní pracuje. Kromě té naší sokolské najdete jiné šifrovací tabulky na internetu.



QR kód s odkazem na šifrovací tabulku

ŠIFRA

Pojmy a historie

Šifra – způsob sdělení či předání zprávy, který má za cíl úmyslně znesnadnit, případně znemožnit její přečtení či pochopení někým, komu není určena.

Kryptografie neboli **šifrování** je nauka o metodách utajování smyslu zpráv převodem do podoby, která je čitelná jen se speciální znalostí. Zabývá se tedy tvorbou a vývojem šifer, klíčů, principů, metod atp.

Kryptoanalýza – protiklad kryptografie. Obecně jde o zkoumání skrytých a zašifrovaných zpráv, hledání metod k jejich rozkrytí, odhalení principů a klíčů.

Kryptologie – zahrnuje kryptografii a kryptoanalýzu. Jedná se tedy o pojem vyjadřující souhrnně kódování a dekodování zpráv.

Steganografie – je podobor kryptografie zabývající se ukrytím zprávy. Zpráva je ukryta tak, aby si pozorovatel neuvědomil, že komunikace vůbec probíhá. Síla této komunikace stojí a padá na jejím utajení, a zachycení skryté zprávy tak prakticky znamená její prolomení. Aby ani v tom případě nedošlo k prozrazení obsahu zprávy, zpravidla se kombinuje s dalšími metodami šifrování.

Zmínky o utajování obsahu písma se objevovaly již ve starém Egyptě, Mezopotámii a Indii.

Celé období kryptografie lze rozdělit do dvou částí. První je klasická kryptografie, která trvala zhruba do poloviny 20. století. První část se vyznačovala tím, že k šifrování stačila pouze tužka a papír, případně jiné jednoduché pomůcky. Během první poloviny 20. století ale začaly vznikat různé sofistikované přístroje, které umožňovaly složitější postup při šifrování. Tím přibližně začala druhá část, která se nazývá moderní kryptografie. V dnešní době se k šifrování zpravidla nepoužívají žádné zvlášť vytvářené přístroje, ale klasické počítače.

Šifry, o kterých pojednávají tyto Metodické listy, jsou tzv. herními šiframi. Kdybychom byli důslední, měli bychom používat spíše výrazu hádanka, rébus než šifra. Napsat text za použití morseovky nebo Brailleova písma není šifrování, ale jen přepsání do jiné abecedy. Nicméně s rozvojem šifrovacích her se význam slova šifrování rozšířil a používá se i pro šifry herní, tak jak si je budeme popisovat zde.

Abeceda a čísla

Základním kódováním jakékoli zprávy je abeceda. Můžete použít českou s háčky, ale nejčastěji se ve hrách používá anglická s 26 znaky. Pro některé případy, jako třeba polský kříž, lze využít i abecedu s písmenem ch. Občas se vyskytuje i abeceda s 25 písmeny, která se využívá v mřížkách. Nikdy nezapomeňte u zadání šifer napsat, jakou abecedou šifrujete.

Pro ukázky v těchto listech bude využita kromě polského kříže abeceda s 26 písmeny. Řešením je v herních šifrách často číslo, které odkazuje na dané pořadí písmene v abecedě. Šifru lze ztížit i počítáním odzadu či jinými variantami, na které by ale šifra sama měla navést.

Pokud jsou řešením šifry čísla a nedají se aplikovat na abecedu, pak podle jejich rozpětí, frekvence a dalších společných znaků (prvočísla) přichází v úvahu například pokusit se je dosadit do souřadnic, neboť výsledným heslem může být i název rybníka zobrazeného na mapě. Čísla mohou vést i k digitálnímu ciferníku.

Jednoduché substituce

Substituce nahrazuje jednotlivá písmena jinými písmeny či znaky. Pokud se písmena změni na prapodivné znaky, vzhledu šifry to přidá na zajímavosti (stejně funguje např. malý polský kříž).

K těmto substitucím je často potřeba klíč, který by hráči měli mít nebo nějakým způsobem získat.

Substituce, na které se dá přijít bez klíče

- pevný posun znaků v zadaném textu vždy o stejnou zadanou číselnou hodnotu v abecedě. Této šifře se říká Caesarova šifra, neboť ji používal

a v Zápiscích o válce galské popsal sám Julius Caesar. Jeho posun byl o tři písmena, ale název se zevšeobecnil na jakékoli posuny.

- převrácená abeceda (a→z, c→x...)
- pro dlouhé šifry se využívá frekvenční analýza, ta spočívá v porovnání frekvence jednotlivých znaků zašifrovaného textu se statistickými frekvencemi výskytu daných znaků v konkrétním jazyce

Substituce s klíčem

Klíč – mělo by se jednat o slovo, ve kterém se nevyskytují stejná písmena. Klíč se napíše jako první a doplní se zbylými písmeny abecedy v jejím pořadí bez písmen v klíči. Tak je zachován stejný počet písmen, ale oproti abecedě je jejich pořadí jiné.

Polyalfabetická substituce

Výše psané substituce jsou monoalfabetické a jejich nevýhodou je, že skrze frekvenční analýzu se dají prolomit. Proto vznikly složitější, ve kterých se používá několik šifrovacích abeced. Z vícefázových substitucí si popíšeme jen Vigenèrovu šifru, jež je založena na tzv. Vigenèrově čtverci, který také najdete na přiložené šifrovací tabulce. Vigenèrova šifra je založena na několika posunech v abecedách. Pro snadnější luštění jsou tyto posuny opět podle klíče. Zapišeme text zprávy a pod něj dokola opakujeme klíč. Tyto dva řádky „sečteme“ podle Vigenèrovy tabulky. Dešifruje se to opačným způsobem – šifrovaným textem a klíčem. Zajímavá je i varianta, že se klíč použije jen jednou a pak je místo klíče samotný text, který se zašifrovává. Při luštění se tak dekoduje nejdříve pomocí klíče a následně rozluštěnou částí textu.

Příklad s klíčem hovezi, velkými písmeny je výsledný zašifrovaný text.

s r a z n a c e l n i k u
h o v e z i h o v e z i h
ZFVDMIJSGRHSB

Transpoziční šifra

Transpoziční šifra je šifra, která je založena na změně pořadí písmen (nebo symbolů). To znamená, že písmena řešení jsou stejná jako písmena šifrované-

ho textu, ale musí se přijít na jejich správné pořadí. Často jsou založeny na určitém geometrickém postupu čtení písmen. Pro jejich zašifrování lze také použít klíče nebo se využívá čtvercová mřížka.

Příklad: Kyděn ot dej dujošeend.

Šifry luštitelné na základě všeobecných znalostí kulturního prostředí

V šifrách je častokrát potřeba doplnit slovo, znát hlášku, doplnit název nebo podle obrázku poznat osobnost, film... Většinou u těchto typů šifer platí, že víc hlav víc ví a dokážou se do nich zapojit všichni v týmu. Také si všimněte, zda v textu jsou číslovky. Mohou být přímo napsané, ale také ukryté ve slovech.

Příklad:

Vysoké napětí

Hluboké podvědomí

Auto osmiválec

Krutý vyjednaváč

Drahá elektřina

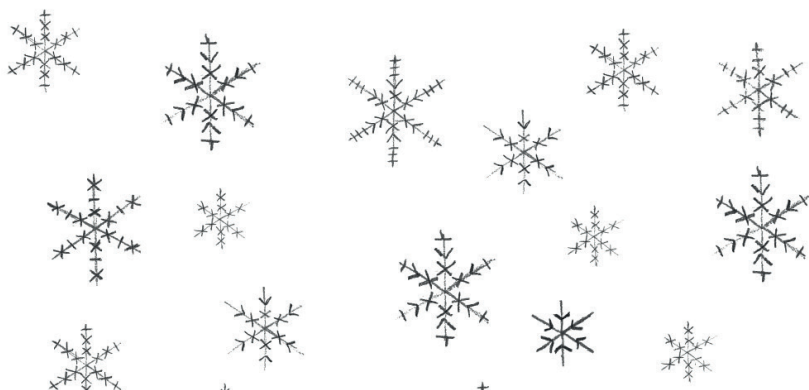
Využijete znalost:

- filmů, knih, herců, pohádek a večerníčků, jména postav, hlášek...
- bible, svatých a jejich atributů, přikázání, pověstí...
- králů, prezidentů, politiků, firem, značek aut, zkratek...
- státních svátků, významných dnů, kalendáře (zvláště šifry založené na jménech v kalendáři)
- pravidel her – karetých, domina, scrabble, pexesa, kvarteta, dobble...
- přísloví a rčení, pořekadel, pranostik...
- míchání barev, RGB, CMYK, barev duhy (ty jsou dobrou pomůckou při řazení písmen, jak se mají číst za sebou)
- římských číslic, chronogramu a ciferníku
- hudební nauky (noty, tóniny, akordy, notové osnovy, klíče...)
- melodií, písní, koled, žánrů, skladatelů, videoklipů, skupin, hudebních nástrojů...
- vzhledu starých mobilů a principu psaní na nich zpráv, vzhled klávesnice

Příklad 1: Podle obrázku je třeba poznat, o jaký film / pohádku se jedná. Společně mají, že se v názvu objevuje číslo, to pak určuje písmeno v názvu daného filmu / pohádky. (Ze hry Tápání 2024.)



Příklad 2: V následující šifře byla na zakreslení vložek použita římská čísla, ta byla převedena na abecedu. Podle četnosti stejných vložek se četlo výsledné pořadí písmen. Jedná se pouze o výřez ze zadání. (Ze hry Tápání 2024.)



Příklad 3: V následujícím příkladu využijete hned několika znalostí. Barvy duhy by vás měly navést, že se asi bude jednat o čísla, která se převedou na písmena, a ta se podle barvy budou řadit za sebou. Římské číslice jsou jasné, ale co ten rok? Tak zkuste ciferný součet.

Moje prabába viděla I. všesokolský slet 1882, moje bába cvičila na IX. všesokolském sletu v roce 1932 a já napsala jednu ze skladeb pro XVI. všesokolský slet 2018.

Příklad 4 ze sokolské městské hry v Praze: Obrázky mají navést na české a československé prezidenty.



5./11



2./13

30 x



6./10



2./20



1./11



1./14



10./11

ABCČDĎEFG

4./9



10./16



3./15



4./11

Šifry využívající znalostí z matematiky, geometrie, chemie, češtiny, zeměpisu

Šifry založené na znalostech ze školy se prolínají se šiframi na základě všeobecných znalostí. Ale není na škodu to oddělit. Sčítání, ciferný součet, ciferace (opakování ciferného součtu, dokud nevznikne jednociferné číslo) a další aritmetické operace nás při luštění nemohou překvapit. V šifrách se dá pracovat i s různými posloupnostmi, jako jsou prvočísla, Fibonacciho řada nebo třeba pí (ke všem těmto číselným řadám se dá např. přiřadit písmeno podle jejich pořadí v řadě). Využít se dají vzorce pro výpočet objemu, obsahu nebo představivost při skládání krychle.

Geometrie se využívá ke grafickým šifráům (viz níže). Řešením může být i změření nějaké délky, která opět odpovídá písmenu v abecedě. Setkala

jsm se i se šifrou, kde bylo na základě dvou bodů potřeba udělat přímku, která v jednom místě proťala právě jedno písmeno.

V chemii se dá na několik způsobů využít periodická tabulka prvků a třeba i koncovky k vytváření názvů oxidů (ný, natý, itý...).

Čeština se svými pády, slovními druhy, životností, videm, množným a jednotným číslem skýtá také nepřeberné množství, jak ji využít třeba v kombinaci s kódovacími systémy. Všimli jste si například, že jsou v zadání šifry často vyjmenovaná slova? Tak to také nebude náhoda.

Znalosti ze zeměpisu jsou dobré při poznávání známých míst, kontinentů, planet, hodí se znalost hlavních měst a vlajek atd.

Inspiraci bychom samozřejmě mohli hledat i v dalších ve škole povinných předmětech – biologii, dějepisu, ale třeba i tělocviku...

Příklad: Chemik na konci by měl napovědět, že se máme vydat do hlubin znalostí chemie. Zavalitý slizovitý závěrečný temný neurčitý spolkový a sebejistý chemik.

Grafické šifry

Grafické šifry jsou vhodné hlavně pro hry, neboť nedokážou obsáhnout delší text. Po vylustění takovéto šifry je řešení vykreslené, což mohou být písmena a čísla, ale také obrázek. Nápadů na takovéto šifry je mnoho a my si tady zkusíme popsat jen pár z nich. Často je řešení vykresleno pomocí mřížky, proto je dobré si na šifrovačky brát čtverečkový nebo milimetrový papír.

- udání počtu vybarvených a nevybarvených polí podle řádků
- udání počtu vybarvených polí – která to jsou, se musí zjistit
- vybraná písmena ze zprávy zakreslíme do mřížky, vytvoří tak obrázek
- různé typy bludišť, jejichž řešení opět kreslí písmeno nebo obrázek
- ve čtverečkové síti se dají využít i průsečíky
- někdy nás šifra navádí k použití kružítko a pravítka
- zadání šifry se dá rozstříhat a úkolem je složit ji
- různé hrátky s písmeny, aby na první pohled nebyla k přečtení
- na papíru jsou obrázky a některé z nich tematicky patří k sobě, při jejich spojení vznikne obrázek nebo písmena
- kreslení využívající směr světových stran, úhlů, semaforu

Digitální ciferník

V šifrovací tabulce naleznete digitální ciferník. Ten se skládá ze sedmi očíslovaných částí (vektorů). Toto číslování je ustálené. Pokud vám ze šifry vycházejí čísla do sedmi, zkuste je zakreslit jako digitální číslo. Vyjde vám z toho číslo, ale třeba i písmeno nebo obrázek. Očíslovány jsou i průsečíky vektorů.

Příklad: Po prvním rozkókání zjistíme, že se ve slovech vyskytují písmena, která dávají dohromady slovo stromek, vypíšeme si pořadí v tomto slově a vyjde nám 7, 5, 4, 2, 3; 3, 4, 5; 4, 7, 3, 6, 1; 5, 3, 7; 7, 3, 4, 5. Podle očíslovaného digitálního ciferníku zakreslíme čísla v podobě čar a čteme výsledné slovo. (Ze hry Tápání 2024.)

KMOTR ROM OKRES MRK KROM

Cviky

Pamatujete si ještě na Noc sokoloven, při které jsme cvičili písmena? I slovní popis cviků, které zobrazí slovo nebo číslo, se dá pokládat za grafickou šifru. Alžběta Pálková vám tenkrát sepsala cviky tvořící písmena se správným názvoslovím.

- A** vzpor na levé stojmo, paže v prodloužení trupu – předpažit dolů dovnitř, dlaň na koleno
- B** podřep – hluboký ohnutý předklon – předpažit vzhůru, prsty se dotýkají země – předklon hlavy
- C** sed (mírně) ohnutě – předpažit povýš – předklon hlavy
- D** klek rozkročný, náklon vzad prohnutě – zapažit, ruce na patách – záklon hlavy
- E** sed, předpažit pravou dolů, předpažit levou, předklon hlavy
- F** stoj – mírný úklon vpravo, předpažit pravou dolů, předpažit levou (dlaň dolů), úklon hlavy
- G** leh – přednožit – předpažit, dlaně sklopit
- H** klek na pravé, levá kolmo vlevo – vzpažit
- I** stoj
- J** leh ohnutě – přednožit – předklon hlavy – pokrčit připažmo, dlaně na stehna
- K** klek únožný levou, skrčit vzpažmo pravá, levá vzpažit zevnitř, dlaň vpřed

- L** sed – vzpažit
- M** vzpor vzadu sedmo skrčmo
- N** sed skrčmo, náklon vzad, pokrčít připažmo, dlaně (z boku) na stehnech
- O** leh na bříše prohnutě skrčmo, zapažit (uchopit za bérce)
- P** stoj, hluboký ohnutý předklon – předpažit dolů, prsty se dotýkají kolen – předklon hlavy
- Q** podpor na pravém předloktí ležmo prohnutě, břicho na základně, skrčmo – zapažit levou, uchopit špičky
- R** stoj přednožný – hluboký ohnutý předklon – předpažit dolů, prsty na levé koleno – předklon hlavy
- S** klek, ohnutý náklon vzad – předpažit vzhůru, dlaně sklopit – předklon hlavy
- T** stoj, rovný předklon – upažit
- U** leh ohnutě – přednožit – vzpažit vpřed – předklon hlavy
- V** leh – přednožit roznožmo
- W** leh – přednožit roznožmo, předpažit dovnitř, dlaně spojit
- X** stoj rozkročný, vzpažit zevnitř
- Y** stoj spatný, vzpažit zevnitř
- Z** klek, náklon vzad – předpažit poníž

Neviditelná písma

Jedná se o texty psané „neviditelným inkoustem“, skoro jako to známe z Harryho Pottera. Slouží k zapsání zprávy tak, aby nebyla vidět. Nejjednodušší „inkousty“ jsou ty, které zviditelníme teplem. Takto se dá použít šťáva z citronu či jiného ovoce, cibulová šťáva, ocet, roztok bílku s vodou v poměru 1:1, mléko, 20% roztok cukru či medu, moč. Britská tajná služba před sto lety najala i vlastního chemika, aby jí testoval a vymýšlel nové metody. A protože např. v SSSR byl nedostatek všeho, byli agenti instruováni, aby použili i to, co mají vždy po ruce – své sperma. Tuto látku (k nelibosti těch, kdo to po nich četli) opravdu používali.

Je potřeba si různé metody vyzkoušet včetně vhodného papíru. Může se stát, že někdy je text k přečtení i bez zahřátí, jindy se zase po něm nemusí čitelně objevit. Na psaní je asi nejlepší redispero. Pokud použijeme třeba štětec a papír se nám trochu zvlhčí a zkrabatí, můžeme to zamaskovat překrytím pomocí

„viditelného“ textu (ostatně tak to dělali i výše zmínění agenti – neboť dopis bez textu si o nežádoucí přečtení přímo říká). Pro zviditelnění je nejrychlejší použít svíčku nebo zapalovač, pro šetrnější a méně rizikové řešení je dobrá i žehlička. Pokud je šifra dělána pro děti, myslete i na variantu, že ji omylem spálí.

Šifry pomocí kódovacích systémů

Hlavním účelem kódování je převod mezi dvěma abecedami či obecněji mezi dvěma způsoby zápisu zprávy.

Morseova abeceda

Morseova abeceda se dá využít k velkému množství nápadů. Je velice rozšířená, neboť se s ní v dětském věku setká téměř každý. Lze ji zakódovat do čehokoli, u čeho se dají rozlišit tři hodnoty – čárka, tečka, oddělovač. V častých případech jsou písmena oddělena řádkem, takže stačí jen dvě hodnoty. Pokud morseovku neumíte z paměti, pomůže tzv. pavouk, kterého jsme také dali do šifrovací tabulky. Ten je rozdělen na dvě části, první začíná tečkou, druhá čárkou. Po pavouku se pohybujete podle daných znaků, až dojdete k hledanému písmenu. K naučení morseovky se používají pomocná slova, v češtině jsou to slova s krátkými a dlouhými samohláskami ve slabice, které napovídají tečku nebo čárku. Pomocná slova jsou s malými obměnami ustálená a také se mohou použít jako řešení šifry.

V šifrách se využívají převážně písmena, ale lze použít i čísla.

Příklady úpravy morseovky

- záměna znaků – výměna teček a čárek
- změna pořadí znaků – prohození tečky a čárky
- vynechání oddělovače – kódování není jednoznačné, ale má jen jedno srozumitelné řešení; vhodné pro starší děti s trpělivostí
- maskování – například ve slovech (samohláska, souhláska), peníze (kovové, papírové), čísla (lichá, sudá), noty (čtvrtové, půlové), dárky (tvrdé a měkké), atributy pohlaví (muž a žena), symbolika Sokola x Orla... fantazii se meze nekladou
- vzhledem k tomu, že morseovka se využívá v telegrafii, lze ji řešit i jinými smysly než zrakem – dobré jsou hry, kde se zpráva předává pomocí baterky, kouřových signálů, zvuků, ale třeba i čichu, hmatu a chutě.

Zkuste tak luštitelům nechávat čichnout ke smradlavým a voňavým věcem.

Příklad 1: Moje šifra, kterou naleznete u hry geocaching a jsou v ní skryté souřadnice k jedné ze sokolských keší vzniklých ke 100 letům naší republiky. Co takt, to číslo.



Příklad 2: Část šifry (3 písmena) ze sokolské městské hry v Praze.



Semaforová abeceda

Dalším oblíbeným kódovacím systémem je tzv. semafor. Jedná se o dohodnutou skupinu znaků vysílaných dvěma vlajkami jednou osobu, kdy jednomu znaku přísluší jeden signál. Dorozumívací systémy založené na předávání zpráv pomocí signálů dávaných pažemi, praporky či vlajkami byly vypracovány již koncem 17. století v námořní dopravě, v roce 1803 byl v Anglii systém standardizován a zejména menším plavidlům sloužil společně s vlajkovou abecedou až donedávna. Ve Francii byly pro rychlý přenos postaveny věže, které na sebe viděly. Skrz věže zpráva o 36 znacích urazila 200 km za cca půl hodiny. Později byl tento systém nahrazen telegrafem – morseovkou. Signály se používají v dopravě a jejím řízení, při práci v lomech, horolezectví.

Ačkoli byl tento systém využíván k vizuálnímu přenosu, v šifrách se dá použít často v souvislosti se světovými stranami, úhly, geometrií (spojování bodů) atp. Běžný je i slovní popis. Při luštění napoví, že se jedná o toto kódování, přítomnost tří bodů nebo osmi směrů.

Příklad 1: Pepa jede z Chomutova přes Prahu do Pardubic. (písmeno Y)

Jan jede z Českých Budějovic přes Prahu do Brna. (písmeno G)

Příklad 2: Ukázka tří písmen. Zadáním byly v jeden čas a den tři hvězdy. Řešením bylo, že se na mapách daného času a dne najde postavení hvězd na obloze, které dá písmeno semaforu. (Ze hry Tápání 2021.)

Datum	Čas	Odkud	Kudy	Kam
13.12.	23:50	Capella	Polaris	Deneb
15.12.	18:00	Deneb	Polaris	Vega
17.12.	06:15	Phecda	Polaris	Caph

13.12. 23:50 Capella -> Polaris -> Deneb



15.12. 18:00 Deneb -> Polaris -> Vega



17.12. 06:15 Phecda -> Polaris -> Caph



Námořní vlajková abeceda

Jedná se o soustavu využívanou k vizuálnímu dorozumívání na dálku. Vznikla před vynalezením rádiového spojení, především ke komunikaci z lodě na loď. Každému písmenu a číslici je přiřazena konkrétní vlajka. Vlajky mají viditelné kontrastní barvy – bílou, modrou, žlutou, červenou. Některé z vlajek signalizují konkrétní informaci nebo příkaz. Při složitějším zašifrování, aby nebylo hned znát, že se jedná o vlajkovou abecedu, lze využít jen barev nebo vzhledu vlajky (pruhy, puntík, dělení, křížení atd.).

Příklad: Křížení barevných hadů s částmi vzhledu vlajky napovídá, o kterou vlajku se jedná. (Ze hry Lost in Hvozd.)



Mřížky

Mřížky fungují na systému substituce, kdy dané písmeno je nahrazeno znakem. Asi nejznámější je velký polský kříž. Hezky v něm vychází rozložení písmen s písmenem ch. Ale i tak je vždy dobré říct v pravidlech hry, zda se používá polský kříž s ch, nebo bez něj. Písmeno je v šifře nahrazeno svým postavením v polském kříži, tedy okénkem, které ho obklopuje. Pozici písmene vyjadřuje tečka. Ta je buď vpravo, uprostřed, nebo vlevo. Pro zajímavější vzhled zápisu je pak možné použít malý polský kříž a hebrejský kříž. V těch jsou písmenka v okénku po jednom a tečka se používá jen pro danou sadu písmen. I tyto systémy se dají maskovat, aby nebylo hned zřejmé, jak se šifra luští. Třeba hebrejský kříž je pěkný sám o sobě a navozuje dojem „kabalského tajemství“. Než ho nějak „maskovat“ je lepší si spíš vyhrát se vzhledem šifry. Zkuste třeba opálený papír nebo i neviditelné písmo, třeba s využitím UV baterky na „dobrodružných“ místech.

Příklad: Zde je na ukázkou ve třech řádcích přepsáno slovo „vynálezce“; první řádek je polský kříž, druhý je hebrejský kříž a třetí řádek je malý polský kříž.



Brailleovo písmo

Brailleovo písmo vzniklo jako písmo pro nevidomé a písmena se čtou hmatem. Normální písmena nejsou vhodná ani pro prostorový tisk, ani pro hmatové rozpoznávání. Toto kódování vymyslel Francouz Louis Braille v první polovině 19. století. Písmena se skládají z kombinace teček umístěných v obdélníku 2×3. Tento systém lze tedy využít pro vytváření takto kódovaných slov a vět. A stejně jako u morseovky platí, že se fantazii meze nekladou. Protože se při zašifrování mohou smývat mezery mezi písmeny, vždy je dobré při luštění zbystřit, když je něčeho v počtu tří pod sebou (případně násobky tří) a dvou (a násobků dvou) vedle sebe. A protože se v Brailleově písmu stejně jako u morseovky vyskytují pouze dva znaky (pole s tečkou a bez tečky), lze využít podobných nápadů, jaké jsem nastínila výše.

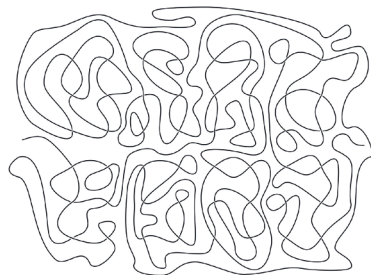
Příklad 1: Písmena v zadání napoví, jak dál řešit.

SSEPCE

SLPEEC

SLPEEC

Příklad 2: Po prvním rozkukání se zjistíme, že provázek je rozdělen na šest sektorů, ve kterých se kříží šestkrát, a křížení jsou navíc v osách. To nás navede na Brailleovo písmo. Podle toho, zda se kříží horem, nebo spodem, určíme písmeno. (Ze hry Tápání 2024.)



Dvojková (binární) soustava

S příchodem počítačů vznikla potřeba reprezentovat písmena digitálně. Kódování přiřazuje písmenům a dalším znakům jedničky a nuly. Prvním rozšířeným standardem se stalo kódování ASCII (American Standard Code for Information Interchange). Pro zakódování textu také vhodné.

*Příklad: **SOKOL SOKOL SOKOL SOKOL SOKOL SOKOL SOKOL SOKOL SOKOL SOKOL SOKOL***

JAK LUŠTIT

Při psaní těchto Metodických listů jsem myslela hlavně na sestry a bratry, kteří mají zálesácké kroužky nebo organizují i jiné než cvičící a sportovní aktivity. Obsahem má být stručný základní přehled různých druhů herních šifer, které jsou celkem lehce a jednoduše využitelné pro práci s dětmi, ale i k vytváření bojovek pro dospělé. Ale pokud vás to zaujalo natolik, že si vytvoříte tým a zaregistrujete se na nějakou šifrovačku, ať už terénní, nebo online, tak tady je pár tipů a rad, jak k šifrám přistupovat.

Všechno si spočítejte

Náhoda není v šifře náhoda a je podstatné, kolik čeho v šifrách je. Všechno si spočítejte a napište. Dávejte si pozor na čísla, jako je 26 – počet písmen v abecedě; na skupiny po jednom až čtyřech prvcích, které mohou být dvou druhů – morseovka; na tři body nebo osm směrů – semafor; na skupiny dvou prvků seřazené 2×3 – Brailleovo písmo; mocniny na druhou – čtverce; písmena N a E – souřadnice; čísla do 7 – digitální hodiny atd.

Analyzujte vzhled

Na šifře zpravidla bývá na první pohled něco vidět, šifra nějak vypadá. Než šifru začnete luštit, popište si její vzhled. Zvláště formátování textu. Zda jsou obrázky rozmístěny nahodile, nebo v liniích a čtvercích, jejich natočení, různá velikost a barevnost.

Všechno si pojmenujte

Pojmenujte si nejlépe nahlas, co v šifře vidíte, zejména pokud jsou tam obrázky. Pomůže, když si to zapíšete – až pak si třeba všimnete, že slova, která je označují, jsou stejně dlouhá nebo začínají na stejná písmena.

Brainstorming

První minuty luštění si vyhradte jen pro vymýšlení a střílení nápadů. Nebojte se skutečně říkat úplně vše, co vás napadne, i špatný nápad může vašemu spoluhráči asociovat správnou cestu k řešení. Nic zatím nehodnoťte, na to bude čas později.

Používejte šifrovací tabulku a internet

Kromě šifrovací tabulky existuje i šifrovací aplikace. Není na škodu, když je v týmu několik různých šifrovacích tabulek. Pokud to pravidla dovolují, používejte internet.

NOC SOKOLOVEN 2025 – ŠIFROVACÍ POMŮCKA



1	A	--	00001			A	0	----
2	B	----	00010			B	1	----
3	C	----	00011			C	2	----
4	D	--	00100			D	3	----
5	E	.	00101			E	4	----
6	F	----	00110			F	5	----
7	G	--	00111			G	6	----
8	H	----	01000			H	7	----
9	I	..	01001			I	8	----
10	J	----	01010			J	9	----
11	K	--	01011			K	10	
12	L	----	01100			L	11	
13	M	--	01101			M	12	
14	N	--	01110			N	13	
15	O	----	01111			O	14	
16	P	----	10000			P	15	
17	Q	----	10001			Q	16	
18	R	--	10010			R	17	
19	S	...	10011			S	18	
20	T	-	10100			T	19	
21	U	---	10101			U	20	
22	V	----	10110			V	21	
23	W	---	10111			W	22	
24	X	----	11000			X	23	
25	Y	----	11001			Y	24	
26	Z	----	11010			Z	25	

- Morseova abeceda
- | oddělení písmen || oddělení slov ||| oddělení vět
- 00001 Binární kód
- Mezinárodní námořní vlajková abeceda
- Semafor (praporeková abeceda)
- Braillovo slepecké písmo

Morseova abeceda v dešifrovací tabulce

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

Polský kříž

ABC	DEF	GHCh
IJK	LMN	OPQ
RST	UVW	XYZ

Pomocná slova pro morseovku

akát, blýskavice, cílovníci, dálava, erb, Filipíny, Grónská zem, hrachovina, chvátá k nám sám, ibis, jasmín bílý, krákorá, lupíneček, máva, národ, ó náš pán, papírníci, kvílí orkán, rarášek, sekera, tón, učený, vyučený, wagón klád, Xénokratés, ý se ztrácí, známá žena

Hebrejský kříž

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

Malý polský kříž

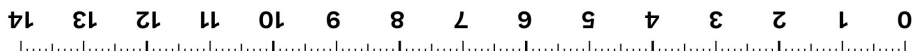
A	B	C	J	K	L	S	W
D	E	F	M	N	O	T	X
G	H	I	P	Q	R	U	Y
						V	Z

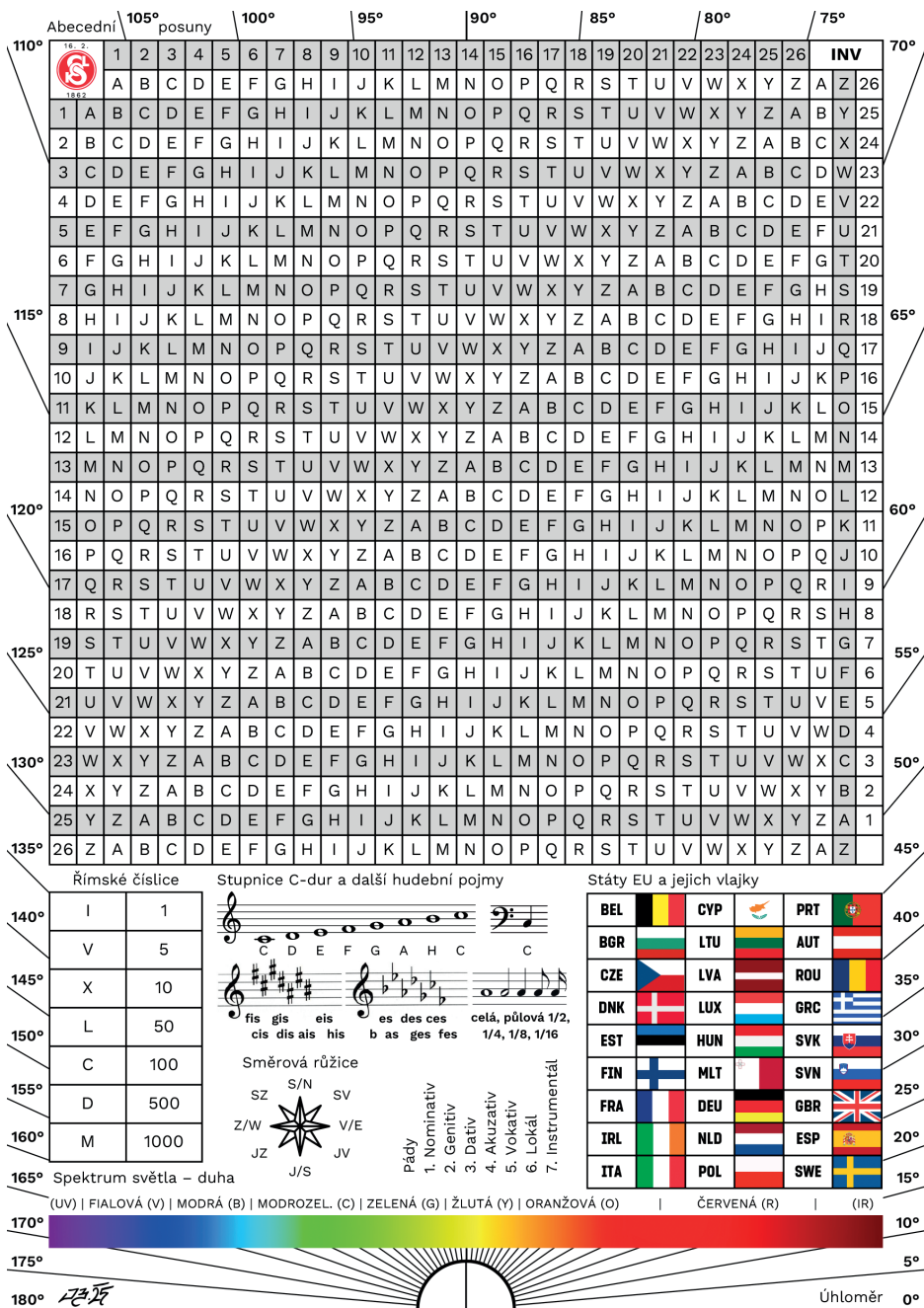
Telefonní klávesnice

1 .,?!	2 ABC	3 DEF
4 GHI	5 JKL	6 MNO
7 PQRS	8 TUV	9 WXYZ
*	0 MEZERA	#

Digitální segmenty

1	1	4
6		2
2	7	5
5		3
3	4	6





ZÁVĚR

Máte už hlavu plnou nápadů na vlastní šifry? Tak já nebudu zdržovat a napíšu jen pár posledních vět a poděkování.

Milí kryptologové, pokud byste mi chtěli cokoli sdělit nebo se na cokoli zeptat, tak pište na sokolský e-mail kpohlova@sokol.eu.

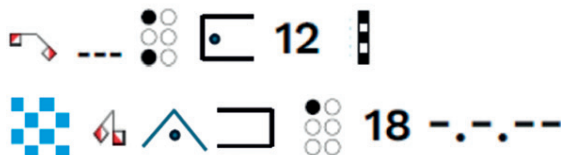
Chcete-li se přidat na nějakou hru se šiframi, navštivte stránky sifrovacky.cz. Tam najdete i další různé informace kolem organizování a hraní.

V těchto Metodických listech jsem vycházela hlavně ze své zkušenosti a občas se podívala do knihy od kolektivu autorů Šifry a hry s nimi, vydané v roce 2007.

Mezi ukázky jsem zařadila šifru ze hry Lost in Hvozd, což byla první šifrovačka, které jsem se kdy zúčastnila, a jak to tak bývá, „poprvé“ člověk jen tak nezapomene. Jedním z organizátorů této hry je Martin Hlinka z Rubicon Games, jemuž děkuji za konzultace. Martin nám také vymyslel šifry v roce 2018 pro sokolskou městskou hru v Praze. Další ukázky jsou ze hry Tápání, kterou připravuje spolek Technická přestávka. Tápání je šifrovací online vánoční kalendář vhodný i pro začátečníky. Děkuji tím všem zmíněným za možnost zveřejnění.

RUBICON
GAMES

Děkuji Milanu Pohlovi, že to po mně čte a opravuje chyby. A velký DÍK Jiřímu Branému za grafickou výpomoc s celou letošní Nocí sokoloven. Vytvořil šifrovací tabulku, dělá zajímavou grafiku šifer a sám některé vymýšlí. Jednu mnou vymyšlenou, ale Jirkou zpracovanou jsme dali na titulní stránku.



Kateřina Pohlová

This image shows a single sheet of white paper with horizontal ruling lines. The lines are evenly spaced and run across the width of the page. There are no margins, text, or other markings on the paper.



GENERÁLNÍ PARTNEŘI ČOS



**NÁRODNÍ
SPORTOVNÍ
AGENTURA**

PENNY.

Časopis SOKOL – Metodické listy – samostatná speciální příloha časopisu SOKOL, vydává Česká obec sokolská | Adresa redakce: ČOS, Újezd 450/40, 118 01 Praha 1 | Odpovědný redaktor: Martin Chlumský | Tisk: VH Print | Informace o časopisu podává a objednávky vyřizuje redakce. Nevyžádané rukopisy a fotografie se nevracejí. Za věcný obsah článků odpovídají autoři. Redakce si vyhrazuje právo příspěvky upravovat, krátit nebo komentovat | MK ČR E 17339, ISSN 0489-6718