Univerzita Hradec Králové

Pedagogická fakulta

Diplomová práce

2019 Václav Vlnas

Univerzita Hradec Králové

Pedagogická fakulta

Katedra kybernetiky Přírodovědecké fakulty

Historické a literární šifry jako téma v informatickém vzdělávání

Diplomová práce

Autor:	Václav Vlnas
Studijní program:	N7504 Učitelství pro střední školy
Studijní obor:	Učitelství pro střední školy - Informatika
	Učitelství pro střední školy - Dějepis
Vedoucí práce:	PhDr. Michal Musílek, Ph. D.

Hradec Králové 2019

Univerzita Hradec Králové
Pedagogická fakulta

Zadání diplomové práce

Autor:	**Václav Vlnas**
Studium:	P17P0628
Studijní program:	N7504 Učitelství pro střední školy
Studijní obor:	Učitelství pro střední školy - dějepis, Učitelství pro střední školy - informatika
Název diplomové práce:	**Historické a literární šifry jako téma v informatickém vzdělávání**
Název diplomové práce AJ:	Historical and literary ciphers as a topic of information science education

Anotace:

Klasické ruční šifry, které můžeme nalézt v archivech a v literárních dílech klasiků dobrodružné literatury, jsou součástí kultury lidstva stejně jako jsou ukázkou kódování informace do na první pohled nečitelné podoby v době před vznikem strojů na zpracování informací (počítačů). Hlavním cílem práce je využít silný motivační potenciál klasických ručních šifer jako téma v informatickém vzdělávání a ukázat žákům zejména středních škol, případně nadaným žákům 2. stupně základní školy, netradiční oblast zpracování informací, ať už klasickým způsobem tužka - papír, nebo prostřednictvím počítače, s využitím vhodného software. Cílem teoretické části práce bude podat stručný přehled faktorů motivace žáků, forem výuky a metod výuky a z nich vybrat ty, které jsou vhodné k výuce tématu historické a literární šifry. Obecně didaktický a oborově didaktický přehled bude doplněn vymezením základních kryptologických pojmů, základních typů šifer a posouzením, které z nich lze vhodně začlenit do informatického vzdělávání. Cílem praktické části práce bude vytipovat tři až pět konkrétních šifrových systémů, pro něž diplomant zpracuje pracovní listy pro žáky. Každý z pracovních listů bude obsahovat stručný historický úvod, definici šifrového systému a popis šifrování a dešifrování a, pokud je to přiměřené svou náročností, také odpovídající metody luštění. Následovat bude zadání založené na dobových historických pramenech, nebo na ukázce z konkrétního literárního díla. Za každým pracovním listem bude uvedeno autorské řešení šifry a metodické poznámky k možným variantám vedení vyučovací hodiny. Cílem empirické části práce bude ověřit jeden z vytvořených pracovních listů ve výuce a zhodnotit tuto výuku formou kvalitativního výzkumu sestávajícího z případové studie popisující výuku s využitím zvoleného pracovního listu a z dotazníkového šetření, ve kterém žáci odpoví na několik otevřených otázek vztahujících se k posouzení atraktivity, názornosti a srozumitelnosti výuky a k jejímu přínosu pro osobní rozvoj respondentů.

Garantující pracoviště:	Katedra informatiky, Přírodovědecká fakulta
Vedoucí práce:	PhDr. Michal Musílek, Ph.D.
Oponent:	doc. RNDr. Štěpán Hubálovský, Ph.D.

Datum zadání závěrečné práce: 7.10.2017

Prohlášení

Prohlašuji, že tato diplomová práce je mým původním autorským dílem a že jsem práci vypracoval (pod vedením vedoucího diplomové práce) samostatně. Všechny zdroje, prameny a literaturu, které jsem při vypracování používal, nebo z nich čerpal, jsem v práci řádně uvedl.

V Hradci Králové dne

Poděkování

Rád bych poděkoval PhDr. Michalu Musílkovi, Ph. D., za velký zájem, za vedení, cenné rady a čas, kterým přispěl k vypracování této diplomové práce. V neposlední řadě bych chtěl poděkovat svým blízkým a rodině za pomoc a podporu.

Anotace

VLNAS, Václav. *Historické a literární šifry jako téma v informatickém vzdělávání*. Hradec Králové: Pedagogická fakulta Univerzity Hradec Králové, 2019. 125 s. Diplomová práce.

Klasické ruční šifry, které můžeme nalézt v archivech a v literárních dílech klasiků dobrodružné literatury, jsou součástí kultury lidstva, stejně jako jsou ukázkou kódování informace do na první pohled nečitelné podoby v době před vznikem strojů na zpracování informací (počítačů). Hlavním cílem práce bylo využít silný motivační potenciál klasických ručních šifer jako téma v informatickém vzdělávání a ukázat žákům zejména středních škol, případně nadaným žákům 2. stupně základní školy, netradiční oblast zpracování informací, ať už klasickým způsobem tužka - papír, nebo prostřednictvím počítače, s využitím vhodného software. Cílem teoretické části práce bylo podat stručný přehled faktorů motivace žáků, forem výuky a metod výuky a z nich vybrat ty, které jsou vhodné k výuce tématu historické a literární šifry. Obecně didaktický a oborově didaktický přehled byl doplněn vymezením základních kryptologických pojmů, základních typů šifer a posouzením, které z nich bylo možné vhodně začlenit do informatického vzdělávání. Cílem praktické části práce bylo vytipovat tři konkrétní šifrové systémy, pro něž byly zpracovány pracovní listy pro žáky. Každý z pracovních listů obsahoval stručný historický úvod, definici šifrového systému a popis šifrování a dešifrování, a pokud to bylo přiměřené svou náročností, také odpovídající metody luštění. Následovalo zadání založené na dobových historických pramenech, nebo na ukázce z konkrétního literárního díla. Za každým pracovním listem bylo uvedeno autorské řešení šifry a metodické poznámky k možným variantám vedení vyučovací hodiny. Cílem empirické části práce bylo ověřit jeden z vytvořených pracovních listů ve výuce a zhodnotit tuto výuku formou kvalitativního výzkumu sestávajícího z případové studie popisující výuku s využitím zvoleného pracovního listu a z dotazníkového šetření, ve kterém žáci odpověděli na několik otevřených otázek vztahujících se k posouzení atraktivity, názornosti a srozumitelnosti výuky a k jejímu přínosu pro osobní rozvoj respondentů.

Klíčová slova

Šifry, výuka, pracovní listy, případová studie, motivace, atraktivita

Annonation

VLNAS, Václav. *Historical and literary ciphers as a topic of information science education.* Hradec Králové: Faculty of Education, University of Hradec Králové, 2017. 125 p. Diploma Thesis.

Classical hand ciphers, which could be found in the archives and literary works, are part of human culture as well as being a show case of information encryption before the emergence of information processing machines (computers). The main goal of thesis was to use the strong motivational potential of classic ciphers as a topic in informatics education and to show, to pupils of high school, alternatively to gifted pupils of secondary school, either, the traditional way - hand-written, or using the computers with proper software. The aim of the theoretical part of the thesis was to outline a brief overview of the motivation factors of pupils, forms of teaching and teaching method itself, and to choose the ones that are suitable for teaching the topic of historical and literary cipher. The didactic and general didactic overview includes the definition of basic cryptological concepts, basic types of ciphers and the assessment of which ones could be appropriately integrated into informatics education. The goal of the practical part of the thesis was to select three specific cipher systems, for which worksheets for pupils were processed. Each worksheet contained brief historical introduction, cryptographic system definition and a description of encryption and decryption methods, and, if appropriate, the corresponding methods of decay. This was followed by an assignment based on historical sources, or an example from a particular literary work. For each worksheet, there was an authoring solution to the cipher and methodological notes on possible variations of the lesson. The aim of the empirical part of the thesis was to verify one of the proposed worksheets in the classroom and to evaluate this method of teaching in the form of a qualitative research consisting of a case study describing teaching using the selected worksheet and a questionnaire survey in which pupils answered several open questions related to the attractiveness and clarity of teaching and its contribution to the personal development of respondents.

Keywords

Ciphers, education, worksheets, case study, motivation, attractivity

Obsah

Úvod

Diplomová práce se zabývá využitím klasických a literárních šifer ve výuce. Hlavním cílem práce je využít silný motivační potenciál klasických ručních šifer jako téma v informatickém vzdělávání a ukázat žákům zejména středních škol, případně nadaným žákům 2. stupně základní školy, netradiční oblast zpracování informací, ať už klasickým způsobem tužka - papír, nebo prostřednictvím počítače, s využitím vhodného software. V práci jsou obsaženy okomentované pracovní listy, včetně případové studie a dotazníkového šetření, jejichž pomocí je možné vyhodnotit cíle práce.

Práce je členěna do tří hlavních částí, které jsou dále děleny na kapitoly a podkapitoly. První tematický celek je teoretická část, která se dělí na 5 kapitol. První kapitola se zabývá motivací obecně, tak i konkrétně. Tato kapitola se věnuje také rozdělení motivace na vnitřní a vnější, dále pak na motivující a demotivující činitele výuky. V této kapitole můžeme také nalézt metody rozvíjející motivaci nebo současné kognitivní teorie motivace.

Druhá kapitola se věnuje klíčovým kompetencím, které jsou pro další průběh práce naprosto nezbytné a které obsahují všechny kompetence, i ty, které nejsou pracovním listem a výukou rozvíjeny.

Třetí kapitola se zabývá formami a metodami výuky. V této kapitole jsou rozepsány podle různých kritérií a členění tak, aby byly přehledně seřazeny. Položky těchto kritérií jsou ve větší míře popsané, či vysvětlené. Celá tato kapitola je rozdělena na dvě základní části, jak už název napovídá, na formy a metody výuky.

Čtvrtá kapitola teoretické části se věnuje odlišné problematice, než předchozí kapitoly, a to kryptologickým pojmům. Tato kapitola obsahuje obecný úvod a seznam kryptologických pojmů, které jsou vysvětleny, či popsány.

Poslední kapitolou teoretické části jsou základní typy šifer. Tato část obsahuje obecný úvod a vysvětlení substituční šifry. K tomuto vysvětlení jsou přidány i různé typy substitučních šifer. Kapitola se dále zmiňuje o šifře transpoziční a o kódové knize, které však nejsou obsahem této práce a z tohoto důvodu nejsou dále rozvíjeny do širších souvislostí.

Druhým tematickým celkem je praktická část. Tato část práce je nejobsáhlejší částí a dělí se na tři hlavní kapitoly, které mají kapitoly. Tento celek začíná obecným úvodem, který následuje první kapitola, která se věnuje prvnímu pracovnímu listu. V této kapitole je možno nalézt devět konkrétních podkapitol, které korespondují s vypracovaným pracovním listem a které jsou náležitě a podrobně popsány. Pracovní list obsahuje titulní stranu, úvod, definici šifrového systému, popis šifrování a dešifrování, metody luštění, zadání pracovního listu, prostor pro luštění, řešení, metodické poznámky a zdroje. Tento konkrétní pracovní list obsahuje historickou substituční šifru, která byla vytvořena pro potřeby výuky.

Druhá kapitola druhého tematického celku se zabývá taktéž pracovním listem, který je však vypracován podrobněji a obsahuje šifru, která je taktéž substituční. Šifra v tomto pracovním listu je o něco složitější na vypracování. Tato kapitola má stejnou strukturu, jako předchozí kapitola. Všechny podkapitoly jsou rozebrány a okomentovány.

Třetí kapitola se věnuje třetímu pracovnímu listu a sdílí s předchozími dvěma kapitolami stejnou strukturu. Tento list taktéž obsahuje šifru, nikoliv písmennou, ale znakovou. Avšak stále se jedná o substituční šifru. Tento pracovní list je na rozdíl do dvou předchozích složitější na vypracování a to především díky této šifře. Kapitola je členěna na podkapitoly, jak již bylo zmíněno, a tyto podkapitoly jsou rozčleněny na určité celky, které jsou náležitě okomentovány.

Třetí tematický celek je empirická část, která se věnuje kvalitativnímu výzkumu. tato kapitola se rozdělena na tři hlavní kapitoly, které se dále dělí na podkapitoly. První kapitolou je kvalitativní výzkum, který obsahuje obecný úvod a několik podkapitol a to především cíl výzkumu, formulaci výzkumných otázek a hypotéz, metodologii, charakteristiku místa šetření a charakteristiku výzkumného vzorku.

Druhá kapitola se zabývá především analýzou dat a je členěna do čtyř podkapitol. První podkapitola je věnována případové studii, následuje analýza prvního a druhého dotazníkového šetření. Poslední podkapitol je věnována testování stanovených hypotéz.

Poslední kapitola empirické práce představuje výsledky výzkumného šetření. Tato shrnující a vyhodnocující kapitola je členěna na dvě podkapitoly. První podkapitolou jsou odpovědi na výzkumné otázky, které jsou podloženy daty z případové studie a z dotazníkového šetření. Druhou a poslední podkapitolou je vyhodnocení stanovených

hypotéz, jejichž stanovisko taktéž vychází ze získaných dat, které byly získány případovou studií a dotazníkovým šetřením.

1 Teoretická část

1.1 Motivace

Motivace, dnes velmi často využívané slovo ve školství, je základní podmínkou lepších výkonů ve vzdělávání a ve školství vůbec. Kapitola nese název motivace, protože se práce zabývá využitím šifer v informatické výuce (nikoliv jen v informatice), kde je velmi podstatné, aby žáci byli motivovaní, protože šifry samotné mohou být obtížné a jejich řešení si může vyžádat delší čas a pozornost. Z tohoto důvodu je nutné žáky více motivovat, jelikož více motivovaní žáci lépe rozvíjejí své klíčové kompetence, které jsou stěžejní pro rozvoj osobnosti.

Podle Čapka je největším problémem s motivací ve školství to, že žáci jsou učeni stylem - udělej to, dostaneš toto. Tento způsob „úplatků“ učí žáky korupčnímu jednání. Nicméně když se člověk na tuto problematiku zaměří více dopodrobna, tak zjistí, že onen úplatek není tak docela úplatek, ale ohodnocení žáka, které může žákovi zvýšit sebehodnocení a zároveň motivovanost. (Čapek, 2014, s. 114–115)

Jako základní pilíř motivace studentů Čapek uvádí hodnocení a to už jak slovní, tak školní známky. (Čapek, 2014, s. 116–117) „*Učitel, který ve vyučování uplatňuje adekvátní způsoby vnější i vnitřní motivace, klade pevné základy pozitivního rozvoje osobnosti žáka.*“. (Lokšová, 2006, s. 9) Motivace samotná se musí přizpůsobovat cíli, obsahu vyučování a věků žáků. Problematika motivace spočívá v tom, že přesahuje i do mimoškolního prostředí, které ji utváří, následně na to může učitel svým špatným výběrem motivačních metod žáka v motivaci brzdit anebo dokonce způsobit nezájem nebo odpor. (Lokšová, 2006, s. 9)

Vysvětlit pojem motivace je velmi problematické, protože se sama řadí mezi hypotetické konstrukty, které nemají fyzickou podobu a má několik funkcí. Jednou z těch funkcí je to, že je dynamizující, která se zabývá tím, že někdo něco dělá. Další aktivizující, ta se ptá proč to tak je. Poslední je usměrňující, která má dohlížet na to, aby to budoucnu žák dělal, nebo nedělal. K motivaci existuje řada teorií, které jí zabývají. Tyto teorie můžeme rozdělit podle toho, zdali se více soustřeďují na obsahovou stránku (co člověka motivuje), nebo na stránku procesuální (jak to na něj působí). (Lokšová, 2006, s. 10)

Jak již bylo výše zmíněno, existuje více teorií, jak lze k motivaci přistupovat. Jednou z nich je behaviorální teorie. „*Behaviorální teorie vidí jako zdroj motivace úsilí dosáhnout příjemných důsledků určitého chování nebo snahu vyhnout se důsledkům*

nepříjemným. Hlavním motivačním činitelem je zpevnění vnější odměnou." (Lokšová, 2006, s. 10)

Další teorií je humanistická. Ta klade důraz na to, že žák musí překonávat sám sebe, skrze svoje vývojové možnosti - více a více se zdokonaluje. Aby mu bylo umožněno patřičné zdokonalení, musí učitel žákovi vytvořit patřičné prostředí, které je založeno na vřelém vztahu žáka a učitel, na bezpečí a bezpodmínečném přijetí každého jedince. Tato teorie má v praxi vést žáka k vyšší a vyšší autonomii, nicméně má i negativní důsledek a to ten, že pokud žákovi bude dávána vysoká autonomie dříve, než je na to připraven, tak to žáka velmi zatíží a výsledek bude opačný. (Lokšová, 2006, s. 11)

Následující teorií je kognitivní. *„Kognitivní (poznávací) přístup klade důraz na význam poznávacích (kognitivních) procesů pro chování člověka. Vychází z předpokladu, že člověk je především „zpracovatelem" informací a „institucí činící rozhodování". Zpracování informací je tedy logickým výsledkem shromáždění nutných poznatků a výsledného rozhodnutí člověka."*(Lokšová, 2006, s. 11) Ze všech výše zmíněných teorií je tato teorie nejvíce zastoupena v pedagogické literatuře 90. let.

1.1.1 Vnitřní a vnější motivace

Motivaci jde rozdělit podle různých kritérií, ale základní rozdělení je na vnější a vnitřní. Vnitřní motivace se od vnější liší tím, že pochází z člověka samého. Jedinec dělá určitou činnost z vlastní vůle a nečeká, že za to dostane nějakou odměnu. (Lokšová, 2006, s. 15)

Vnější motivace je spojená s nějakým tlakem, stihnout něco za nějaký čas a za to dostane žák odměnu. Tuto činnost žák nedělá z vlastního zájmu, ale vždy je spojeno s odměnou, proto se tomuto způsobu říká instrumentální - nástrojem pro dosažení cíle. Vnější činitelé, které ovlivňují vnější motivaci, by neměli ve struktuře motivačních činitelů převládat, jinak hrozí snížení výkonu žáků. (Lokšová, 2006, s. 15)

Vzhledem k tomu, že vnější motivace je jedna z těch, které učitel může přímo ovlivnit (myšleno v jedné konkrétní hodině, nikoliv soustavně), můžeme rozdělit tuto motivaci na čtyři druhy a regulace chování.

1. Externí regulace – *„vztahuje se k chování, které je iniciované výlučně externími motivačními činiteli, např. odměnou nebo hrozbou trestu. Žák, který vykonává činnost, protože mu učitel za ni dá známku, nebo proto, že se chce vyhnout konfrontaci s rodiči, je motivován vnějšími motivačními činiteli a jeho chování je externě regulované. Externí regulace představuje*

tu formu vnější motivace, která vychází z vnitřních zdrojů osobnosti žáka nejméně.“ (Lokšová, 2006, s. 16)

2. Regulace pasivně převzatá – „*základem pro tento typ externí motivace je zvenku převzatá, ale vnitřně neakceptovaná regulace chování. Vychází z internalizovaných pravidel chování podmíněných nějakou sankcí (pocit viny) nebo odměnou (sociální ocenění). Příkladem je žák, který dbá na včasný příchod do třídy proto, aby se subjektivně necítil jako „špatný“. Tento žák se neidentifikoval s tímto vnějším motivačním činitelem (stanovený čas začátku vyučování), takže přesnost příchodu do školy není jeho vlastním vnitřním motivem chování*.“ (Lokšová, 2006, s. 16)
3. Identifikovaná regulace – „*vzniká tehdy, když žák přijme danou hodnotu za svou a identifikuje se s požadovaným chováním, takže danou činnost vykonává mnohem ochotněji. Identifikace žákovi umožňuje pochopit smysl vykonávání učební činnosti. Příkladem je student, který se ochotně učí matematiku i doma, neboť ví, že je to důležité pro jeho úspěch v tomto předmětu. Tato motivace je vnější proto, že student k vykonávání činnosti motivován především snahou dosáhnout dobrých výsledků a známek z matematiky, a ne v první řadě svým vlastním zájmem o tento předmět. Navzdory tomu je už toto chování více regulované zevnitř, protože student jedná ochotně, ne pouze pod vnějším tlakem*.“ (Lokšová, 2006, s. 16)
4. Integrovaná regulace – „*představuje vývojově vyšší formu vnější motivace. Je již plně integrována do osobnosti žáka, příslušný vnější motivační činitel je asimilován s ostatními zájmy, hodnotami a potřebami jedince. Např. žák může mít dvě výrazné motivace - být dobrým studentem a zároveň být dobrým sportovcem. Je reálné, že tyto dva odlišné motivy mohou být v konfliktu a vyvolávat v žákovi tenzi, přičemž jsou oba stejně důležité. Pouze v případě, kdy se tyto motivy stanou vzájemně integrovanými a harmonickými s celou osobností žáka, je regulační proces integrován a chování je výrazem celé osobnosti žáka. Takovéto chování se objevuje u člověka až během dospělosti. Vnitřní motivace a integrovaná motivace mají obsahovat odlišnosti. Vnitřní motivace charakterizuje zájem o činnost samotnou, zatímco pro integrovanou vnější regulaci je typické, že činnost je pro danou osobnost důležitá z hlediska vysokého hodnocení potenciálních*

výsledků (Deci, Vallerand, Pelletier, Ryan, 1991).“ (Lokšová, 2006, s. 16–17)

Zároveň vnější motivace má velký význam v celkové motivaci a to především díky působení odměn a trestů. V procesu učení mají funkci informační a motivační. (Lokšová, 2006, s. 19)

1.1.2 Motivující a demotivující činitelé výuky

Činitelé výuky už neodmyslitelně patří do výuky, ale ne každý činitel vede k úspěšné motivaci a zvýšení výkonu žáků. V rozdělení (níže) je patrné, že činitelů je celá řada a i když jsou to činitelé v zásadě motivující, může jejich špatné využití mít efekt naprosto opačný. Jak už nadpis napoví, existují i činitelé demotivující, kteří se ve škole objevují. Jejich funkce, na rozdíl od motivujících činitelů, je v tom, že i když člověk sebe líp použije demotivující činitel, nikdy se z něj v konečném důsledku nemůže stát činitel motivující.

Podle Lokšové (2006, s. 18) tyto činitele můžeme rozdělit na vnitřní a vnější.

1. Vnitřní činitelé
    a. poznávací potřeby a zájmy
    b. potřeby výkonu
    c. potřeby vyhnutí se neúspěchu a dosažení úspěchu
    d. sociální potřeby, tj. potřeba pozitivního vztahu a potřeba prestiže
2. Vnější činitelé
    a. školní známky
    b. odměna a trest
    c. vztah žáka k jiným lidem
3. Demotivující činitel
    a. autokratický styl vyučování
    b. rigidita a strnulost vyučovacích metod
    c. malé zaměření na tvořivost
    d. velké množství informací
    e. důraz na školní známky
    f. zdůrazňování soutěží

1.1.3 Metody rozvíjející motivaci

Jak už bylo výše zmíněno, motivace je zásadní na rozvoj žáků, na jejich výkon a potřeby. Učitel by právě kvůli tomuto měl dbát na to, aby tyto aspekty byly rozvíjeny. K tomuto mu mohou pomoci metody rozvíjení motivace. Loksošová ve své knize (2006) nabízí desítky zajímavých možností, jak toho dosáhnout, které častou souvisí s formou a metodou výuky.

1. Problémové vyučování
2. Vyučování hrou
3. Dramatizace činností
4. Soutěže
5. Odměna a trest
6. Rozmanitost ve vyučování
7. Imaginace
8. Kooperativní vyučování
9. Tvořivost
10. Aktuálnost

1.1.4 Současné kognitivní teorie motivace

V dnešní době se klade důraz na vnitřní zpracování žákových zkušeností a to buď vědomě, nebo nevědomě. Všechny tyto aspekty souvisí s kognitivním paradigmatem, které je klíčové pro psychologii. Podle Lokšové (2006, s. 22) jsou k této problematice důležité určité pojmy, kterými se zabývá.

1. **Kognitivní disonance** - podle tohoto by měl být motivačním činitelem rozpor mezi žákovými předsvědčeními, tento rozpor vede žáka k myšlenkové činnosti (právě díky motivaci) a cílem této činnosti je znovu nastolení rovnováhy. (Lokšová, 2006, s. 22–23)
2. **Očekávání úspěchu** - podle teorie Atkinsona (1964) lze rozdělit žáky na dva typy. První typ bere potřebu úspěchu víc, než strach ze selhání, proto se třeba častěji hlásí. Pro druhý typ žáka je zásadní vyhnout se selhání důležitější věcí, než dosáhnout úspěchu. Hlavní u výkonové motivace je její stabilita, proto čím vyšší je hodnota cíle, nebo šance ho dosáhnout, tím jsou žáci více motivovaní. (Lokšová, 2006, s. 23)

3. **Atribuční procesy** - podle těchto procesů mají žáci tendenci vše si vysvětlovat a dávat tomu smysl. Problémem toto procesu je to, že když žák několikrát zažije neúspěch, má pak tendenci svůj neúspěch vysvětlovat stylem, že on sám za to nemůže, ale může za to a ono. Pokud tento problém zajde dále, žák se, ani u složitějších úloh, nesnaží najít alternativní řešení, protože má pocit, že neexistuje. (Lokšová, 2006, s. 24)
4. **Sebeúcta a sebepojetí** - učitel se k žákům musí stavět jako k lidským bytostem a bez jakýchkoliv rozdílů a pomocí motivace u nich budovat kladné sebepojetí a sebeocenění (Lokšová, 2006, s. 24)
5. **Vnímaná osobní zdatnost** - Lokšová zde zmiňuje Bandurovu teorii sociálního učení (1973), podle které by měl žák dostávat na pozitivní zpětnou vazbu za své úspěchy. Když žák nedostává patřičnou zpětnou vazbu, může to vést k tomu, že nabude pocitu, že žádný výkon nebo úspěch nepodává.
6. **Cíle akcentující kompetence, výkon nebo vztahy** - učitel má za úkol odvést žáky od cílů vedoucích k úspěchu a nasměrovat je k cílům, které u žáků rozvíjejí klíčové kompetence (Lokšová, 2006, s. 24)

1.2 Klíčové kompetence

„*Klíčové kompetence představují souhrn vědomostí, dovedností, schopností, postojů a hodnot důležitých pro osobní rozvoj a uplatnění každého člena společnosti*“ (Belz, 2001, s. 27)

Klíčové kompetence jsou rozděleny podle jejich zaměření na konkrétní rozvoj žáka.

RVP pro gymnázia [online, cit. 21. 4. 2019], Národní ústav pro vzdělávání. Dostupné z WWW: < http://www.nuv.cz/t/rvp-pro-gymnazia>

1. **Kompetence k učení**

   Žák:

   a. své učení a pracovní činnost si sám plánuje a organizuje, využívá je jako prostředku pro seberealizaci a osobní rozvoj
   b. efektivně využívá různé strategie učení k získání a zpracování poznatků a informací, hledá a rozvíjí účinné postupy ve svém učení, reflektuje proces vlastního učení a myšlení

c. kriticky přistupuje ke zdrojům informací, informace tvořivě zpracovává a využívá při svém studiu a praxi
d. kriticky hodnotí pokrok při dosahování cílů svého učení a práce, přijímá ocenění, radu i kritiku ze strany druhých, z vlastních úspěchů i chyb čerpá poučení pro další práci

2. Kompetence k řešení problému

Žák:

a. rozpozná problém, objasní jeho podstatu, rozčlení ho na části
b. vytváří hypotézy, navrhuje postupné kroky, zvažuje využití různých postupů při řešení problému nebo ověřování hypotézy
c. uplatňuje při řešení problémů vhodné metody a dříve získané vědomosti a dovednosti, kromě analytického a kritického myšlení využívá i myšlení tvořivé s použitím představivosti a intuice
d. kriticky interpretuje získané poznatky a zjištění a ověřuje je, pro své tvrzení nachází argumenty a důkazy, formuluje a obhajuje podložené závěry
e. je otevřený k využití různých postupů při řešení problémů, nahlíží problém z různých stran
f. zvažuje možné klady a zápory jednotlivých variant řešení, včetně posouzení jejich rizik a důsledků

3. Kompetence komunikativní

Žák:

a. s ohledem na situaci a účastníky komunikace efektivně využívá dostupné prostředky komunikace, verbální i neverbální, včetně symbolických a grafických vyjádření informací různého typu
b. používá s porozuměním odborný jazyk a symbolická a grafická vyjádření informací různého typu
c. efektivně využívá moderní informační technologie
d. vyjadřuje se v mluvených i psaných projevech jasně, srozumitelně a přiměřeně tomu, komu, co a jak chce sdělit, s jakým záměrem a v jaké situaci komunikuje; je citlivý k míře zkušeností a znalostí a k možným pocitům partnerů v komunikaci
e. prezentuje vhodným způsobem svou práci i sám sebe před známým i neznámým publikem

f. rozumí sdělením různého typu v různých komunikačních situacích, správně interpretuje přijímaná sdělení a věcně argumentuje; v nejasných nebo sporných komunikačních situacích pomáhá dosáhnout porozumění

4. Kompetence sociální a personální

Žák:

a. posuzuje reálně své fyzické a duševní možnosti, je schopen sebereflexe
b. stanovuje si cíle a priority s ohledem na své osobní schopnosti, zájmovou orientaci i životní podmínky
c. odhaduje důsledky vlastního jednání a chování v nejrůznějších situacích, své jednání a chování podle toho koriguje
d. přizpůsobuje se měnícím se životním a pracovním podmínkám a podle svých schopností a možností je aktivně a tvořivě ovlivňuje
e. aktivně spolupracuje při stanovování a dosahování společných cílů
f. přispívá k vytváření a udržování hodnotných mezilidských vztahů založených na vzájemné úctě, toleranci a empatii
g. projevuje zodpovědný vztah k vlastnímu zdraví a k zdraví druhých
h. rozhoduje se na základě vlastního úsudku, odolává společenským i mediálním tlakům

5. Kompetence občanská

Žák:

a. informovaně zvažuje vztahy mezi svými zájmy osobními, zájmy širší skupiny, do níž patří, a zájmy veřejnými, rozhoduje se a jedná vyváženě;
b. o chodu společnosti a civilizace uvažuje z hlediska udržitelnosti života, rozhoduje se a jedná tak, aby neohrožoval a nepoškozoval přírodu a životní prostředí ani kulturu;
c. respektuje různorodost hodnot, názorů, postojů a schopností ostatních lidí
d. rozšiřuje své poznání a chápání kulturních a duchovních hodnot, spoluvytváří je a chrání
e. promýšlí souvislosti mezi svými právy, povinnostmi a zodpovědností; k plnění svých povinností přistupuje zodpovědně

a tvořivě, hájí svá práva i práva jiných, vystupuje proti jejich potlačování a spoluvytváří podmínky pro jejich naplňování;

f. chová se informovaně a zodpovědně v krizových situacích a v situacích ohrožujících život a zdraví, poskytne ostatním pomoc;
g. posuzuje události a vývoj veřejného života, sleduje, co se děje v jeho bydlišti a okolí, zaujímá a obhajuje informovaná stanoviska a jedná k obecnému prospěchu podle nejlepšího svědomí.

6. Kompetence k podnikavosti

Žák

a. cílevědomě, zodpovědně a s ohledem na své potřeby, osobní předpoklady a možnosti se rozhoduje o dalším vzdělávání a budoucím profesním zaměření;
b. rozvíjí svůj osobní i odborný potenciál, rozpoznává a využívá příležitosti pro svůj rozvoj v osobním a profesním životě;
c. uplatňuje proaktivní přístup, vlastní iniciativu a tvořivost, vítá a podporuje inovace;
d. získává a kriticky vyhodnocuje informace o vzdělávacích a pracovních příležitostech, využívá dostupné zdroje a informace při plánování a realizaci aktivit;
e. usiluje o dosažení stanovených cílů, průběžně reviduje a kriticky hodnotí dosažené výsledky, koriguje další činnost s ohledem na stanovený cíl; dokončuje zahájené aktivity, motivuje se k dosahování úspěchu;
f. posuzuje a kriticky hodnotí rizika související s rozhodováním v reálných životních situacích a v případě nezbytnosti je připraven tato rizika nést;
g. chápe podstatu a principy podnikání, zvažuje jeho možná rizika, vyhledává a kriticky posuzuje příležitosti k uskutečnění podnikatelského záměru s ohledem na své předpoklady, realitu tržního prostředí a další faktory.

1.3 Formy a metody výuky

Tato část představuje několik možností, forem a metod výuky, které jsou ve školství uplatnitelné a které představují nedílnou součást vyučování kteréhokoliv učitele.

Protože ale kritérií, forem a metod je velmi mnoho, je tato kapitola kvůli přehlednosti rozdělena na dvě podkapitoly.

1.3.1 Formy výuky

Organizační uspořádání vnějších podmínek, za kterých se prostřednictvím adekvátních vyučovacích metod a prostředků realizují cíle výuky. Formy výuky můžeme třídit podle určitých kritérií.

1. **Specifičnosti didaktické interakce**
   a) **individuální vyučování** (Vališová, 2011, s. 180)
      - nejstarší forma vyučování
      - dnes se využívá především jako individuální studijní plán pro žáky s uměleckým, nebo sportovním zaměřením
      - nízká produktivita práce učitele
   b) **skupinové vyučování** (Vališová, 2011, s. 180)
      - jedná se o kooperativní výuku
      - činnosti pro skupinovou práci
      - významný sociální aspekt
   c) **hromadné vyučování** (Nelešovská, 2005, s. 32)
      - obvykle jedna třída ve stejné věkové i mentální úrovni
      - vysoká produktivita učitele - řídí celou hodinu
   d) **další vyučovací formy**
      - individualizovaná - důraz na svobodu v pracovním tempu i způsobu práce žáka (Zormanová, 2014, s. 106)
      - projektová - žáci jsou zapojeni do různých projektů (Zormanová, 2012, s. 95)
      - diferencovaná - žáci jsou rozděleni do skupin podle určitého kritéria (Zormanová, 2012, s. 89)
      - týmová - spolupráce více učitelů v rámci flexibilních žákovských skupin (Vališová, 2011, s. 182)

2. **Časové jednotky**

   Formy výuky [online, cit. 11. 7. 2019], Metodický portál RVP. Dostupné z WWW: <https://wiki.rvp.cz/Knihovna/1.Pedagogick%C3%BD_lexikon/F/Formy_v%C3%BDuky>

   a) **vyučovací hodina /den**
   b) **týden /čtvrtletí /pololetí**
   c) **školní rok**

3. **Prostorové jednotky**

   a) **mimotřídní formy** (Vališová, 2011, s. 181–182)
      - domácí úkol
      - exkurzní vyučování - probíhá při odborné exkurzi
      - odborná exkurze - prezentace, přímé pozorování
      - kulturně osvětový vzdělávací program - film, divadlo, atd.

   b) **mimoškolní formy** (Vališová, 2011, s. 181–182)
      - různé kurzy, sportovní dny

Formy výuky, které jsou vhodné pro k výuce tématu historické a literární šifry jsou, dle mého názoru, především skupinová výuka nebo projektová výuka. Skupinová výuka nabízí možnost práce ve dvojicích, která je pro luštění šifer mnohem praktičtější, protože se na to mohou v jeden moment soustředit dva žáci, nebo si mohou lépe rozvrhnout práci při luštění. Samozřejmě je zde možnost i větší skupiny, avšak jsem toho názoru, že v tomto případě je možnost poklesu produktivity žáků, protože by se na pracovní list soustředilo pouze několik jedinců. Vhodná by pro šifry byla i projektová výuka, která nabízí větší časovou dotaci, tudíž by žáci měli více času na samotné luštění šifry, v tomto případě i složitější. Avšak v běžné výuce (myšleno jedna, či dvě vyučovací hodiny) je nejlépe uplatnitelná práce ve dvojicích, či trojicích.

1.3.2 Metody výuky

1. **Klasické výukové metody** (Maňák, 2003, 53–105)

   a. **metody slovní**
      - vyprávění
      - vysvětlování (výklad)

- přednáška
- práce s textem
- výukový rozhovor

b. metody názorně demonstrační

- předvádění a pozorování
- práce s obrazem (ikonickým textem)
- práce se schématy, přehledy a myšlenkovými mapami

c. metody dovednostně-praktické

2. **Aktivizující metody** (Zormanová, 2012, s. 15)

a. aktivizační metody diskusní

- diskuse o určitém tématu
- argumentace
- přijetí názoru druhého

b. aktivizační metody k řešení problémů

- samostatné tvořivé myšlení žáků

c. aktivizující situační metody

- řešení problémového případu vycházejícího z reálné situace

d. aktivizující inscenační metody

- žáci sami předvádějí určitou situaci
- hraní rolí

3. **Komplexní výukové metody** (Maňák, 2003, 131–195)

a. frontální výuka

b. skupinová a kooperativní výuka

c. individuální a individualizovaná výuka

d. kritické myšlení

e. projektová výuka

f. učení v životních situacích

g. projektová výuka

Metody, které by byly vhodné pro informatické vzdělávání k výuce tématu historické a literární šifry, je hned několik. Dle mého názoru to jsou určitě metody slovní, které pedagog používá neustále, dále pak metody názorně demonstrační a metody dovednostně-praktické. Při této výuce by neměly chybět metody aktivizační, konkrétně diskusní, k řešení problému.

1.4 Kryptologické pojmy

Tato část práce obsahuje seznam kryptologických pojmů, které jsou nezbytné k pochopení problematiky kryptografie a jejího významu v práci. Dále tato část pomůže k lepší orientaci v práci samotné, především v pracovních listech praktické části.

Samotná kryptologie zastřešuje několik vědních disciplín, které již pracují s šiframi. První z těchto vědních disciplín je kryptografie, která se snaží otevřený text zašifrovat, aby ho nemohl rozluštit nikdo jiný, než určený cíl/adresát. (Vondruška, 2006, s. 8–9) Druhou je kryptoanalýza, která se naproti tomu, zabývá dešifrováním pomocí nejrůznějších metod. (Janeček, 1994, s. 15), (Vondruška, 2006, s. 9) Třetí disciplínou je steganografie, která má za úkol ukrýt zašifrovanou zprávu tak, aby nikdo nevěděl, že vůbec existuje. (Singh, 2009, s. 5–7), (Singh, 2009, s. 19–21)

Následuje seznam pojmů:

- **Bigram, Trigram, Polygram** - jedná se o dvě, tři, nebo neurčitý počet písmen jdoucích po sobě v textu (Vondruška, 2006, s. 13).
- **Dešifrování** - proces, při kterém dochází k přeměně šifrovaného textu zpět, na text otevřený.
- **Šifrovací klíč** - je to pomůcka, ve které je přesný postup na zašifrování otevřeného textu a jeho následné dešifrování - může obsahovat heslo (Vondruška, 2006, s. 15).
- **Heslo** - je to často slovo, více slov, číslo, nebo nějaká číselná posloupnost, která složí k rozluštění šifrovaného textu - často je součástí šifrovacího klíče (Piper, 2006, s. 16).
- **Homofony** - bývají to skupiny znaků šifrové abecedy, které nahrazují jeden znak v otevřeném textu, aby bylo obtížnější jejich dešifrování; často to bývají samohlásky, které se frekventovaně používají (Vondruška, 2006, s. 32).
- **Klamač** - může to být cokoliv, co je v šifře nadbytečné, protože jeho funkcí je zmást člověka a udělat šifru hůře prolomitelnou (Vondruška, 2006, s. 12).
- **Kód** - je to nějaký šifrový znak, který nahrazuje v šifrovaném textu slovo, sloveso, spojky atd., které se často používají (Vondruška, 2006, s. 16–17).
- **Nomenklátor** - systém šifrování, který kombinuje klamače, kódy a homofony (Singh, 2009, s. 25).

- **Otevřený text** - je text, který ještě neprošel procesem šifrování a je ho možné přečíst.
- **Substituce** - systém šifrování, kde je jeden znak otevřeného textu nahrazen jedním znakem šifrové abecedy (Janeček, 1994, s. 73–76).
- **Šifrová abeceda** - je to skupina znaků, která slouží k zašifrování otevřeného textu, mohou to být písmena otevřeného textu, čísla, nebo obrazce.
- **Šifrování** - proces, při kterém dochází k přeměně otevřeného textu do textu šifrovaného pomocí šifrového systému.
- **Šifrový text** - je text, který prošel procesem šifrování a obsahuje určitý systém šifrování.
- **Transpozice** - systém šifrování, při kterém dochází k posunu písmen abecedy o určitý počet pozic (tzn., když máme posun +3, tak se A změní na D - takto to platí pro všechna písmena otevřeného textu) - posun může být doprava (+X), nebo doleva (-X)
  (Vondruška, 2006, s. 30), (Janeček, 1994, s. 25–29).

1.5 Základní typy šifer

V kryptografii existuje několik základních typů šifer, kterými je možné zašifrovat text. Některé, z těchto typů šifer, jsou obsaženy v pracovních listech praktické části. Ty zbývající jsou zde začleněny pro přehlednost a lepší orientaci v problematice šifrování.

- **Substituční šifra** - je to šifra, u které je písmeno otevřeného textu nahrazeno znakem šifrové abecedy - tato šifra je také využívána ne vždy jako šifra, nýbrž pomůcka - Morseova abeceda, Braillovo písmo. (Vondruška, 2006, s. 29), (Janeček, 1994, s. 73–76)
  - ❖ **Monoalfabetická šifra** - tento druh substituční šifry využívá jednoduchou záměnu písmena otevřeného textu, za jeden symbol, znak, nebo číslici šifrové abecedy - tato šifra je velmi lehce prolomitelná díky metodě frekvenční analýzy znaků (Vondruška, 2006, s. 31).
  - ❖ **Homofonní šifra** - tento způsob šifrování je velmi podobný monoalfabetické šifře, jen s tím rozdílem, že pro jeden znak otevřeného textu může být několik znaků šifrové abecedy - využití homofonů sice ztíží prolomení šifry, nicméně za využití frekvenční analýzy znaků na větším

množství šifrovaného textu je pravděpodobnost dešifrování vysoká (Vondruška, 2006, s. 32).

- **Polyalfabetická šifra** - *„tato šifra je postavena tak, že každé písmeno je zvlášť zašifrováno jednoduchou substitucí, ovšem střídají se různé substituce (typicky posuvné šifry) buď podle periodického hesla, nebo s využitím autoklávu. Tento způsob byl vyvinut na základě toho, aby již nebylo možné dešifrovat text na základě frekvenční analýzy znaků. Nicméně slabinou tohoto důmyslného systému je fakt, že jde luštit „na základě analýzy vzdálenosti mezi opakováními řetězců šifrovaných znaků“, jak uvádí Vondruška.(2006, s. 32–33)“* (Vlnas, 2017, s. 17).
- **Bigramová šifra** - šifra, ve které se využívají bigramy, nebo pak trigramy - dochází k záměně bigramů v šifrované abecedě textu za bigramy v otevřeném textu (Vlnas, 2017, s. 17–18).
- **Digrafická substituční šifra** - tato šifra je velmi podobná monoalfabetické šifře, jen s tím rozdílem, že jednomu znaku otevřeného textu odpovídají dva znaky šifrové abecedy - často využívána číselná kombinace (Vondruška, 2006, s. 35).

- **Transpoziční šifra** - tato šifra je založena na jednoduchém posunu písmen otevřeného textu a to buď doprava, nebo doleva (viz. Transpozice) - tato šifra je velmi lehce prolomitelná (Vondruška, 2006, s. 30), (Janeček, 1994, s. 25–29).
- **Kódová kniha** - jak už název napovídá, jedná se o knihu, která obsahuje slova, ke kterým je přidělen nějaký kód - tento způsob šifrování byl poměrně lehce rozluštitelný a také velmi zdlouhavý (Vondruška, 2006, s. 30–31), (Janeček, 1994, s. 132).

Do informatického vzdělávání bych osobně začlenil substituční šifry, jejichž variabilitou možných znaků lze docílit vyššího či nižšího stupně obtížnosti, zároveň tyto šifry jsou z hlediska časové náročnosti lépe využitelné v krátkém časovém úseku (jedna nebo dvě vyučovací hodiny). Samozřejmě je zde možnost začlenit do informatické výuky i úplně jiné typy šifer, nebo různé typy substituční šifry, avšak tyto šifry jsou časově poměrně náročné a komplikované na luštění.

2 Praktická část

Praktická část práce obsahuje tři různé pracovní listy, které byly navrženy tak, aby využitelné ve výuce nejen informatiky, ale například matematiky, historie, atd. Zmíněné pracovní listy obsahují substituční šifry, avšak pokaždé s jinou znakovou sadou a v práci jsou seřazeny podle obtížnosti.

Pracovní listy neobsahují pouze samotné šifry, ale obsahují také úvod, kde je literárních šifer stručně zmíněn autor díla a jeho život a následně dílo samotné. U historické šifry, která má rovněž svého autora, je zmíněn původ šifry. Za úvodem následuje definice šifrového systému, kde je popsán sytém, jak šifra funguje. Po definici následuje popis šifrování a dešifrování, který je doplněn metodami luštění. Konečně následuje zadání pracovního listu, kde je uvedena samotná šifra a prostor k jejímu dešifrování. Pro ověření správnosti pracovní list obsahuje také řešení, metodické poznámky pro učitele a zdroje. Všechny pracovní listy mají naprosto stejnou strukturu, liší se pouze designem, šifrou, metodickými poznámkami a samozřejmě zdroji.

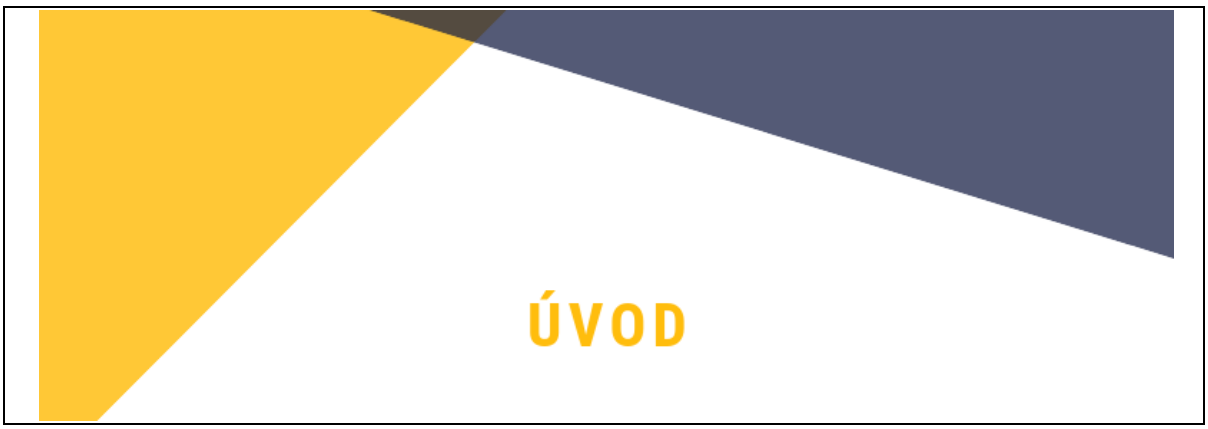
Praktická část je členěna na podkapitoly, které obsahují části pracovních listů, které jsou okomentovány a popsány. Všechny pracovní listy jsou vytvořeny na webové platformě https://www.canva.com/, odkud je možné je exportovat. Celková práce s touto platformou je velmi intuitivní a nabízí uživateli volnou ruku na tvorbu designu, avšak funkce této platformy jsou částečně limitovány. Nutno podotknout, že využívání této platformy je zdarma a je zde na výběr velké množství využitelného materiálu, který si může uživatel, dle libosti, upravovat.

2.1 Pracovní list – 1 „Caesarova šifra“

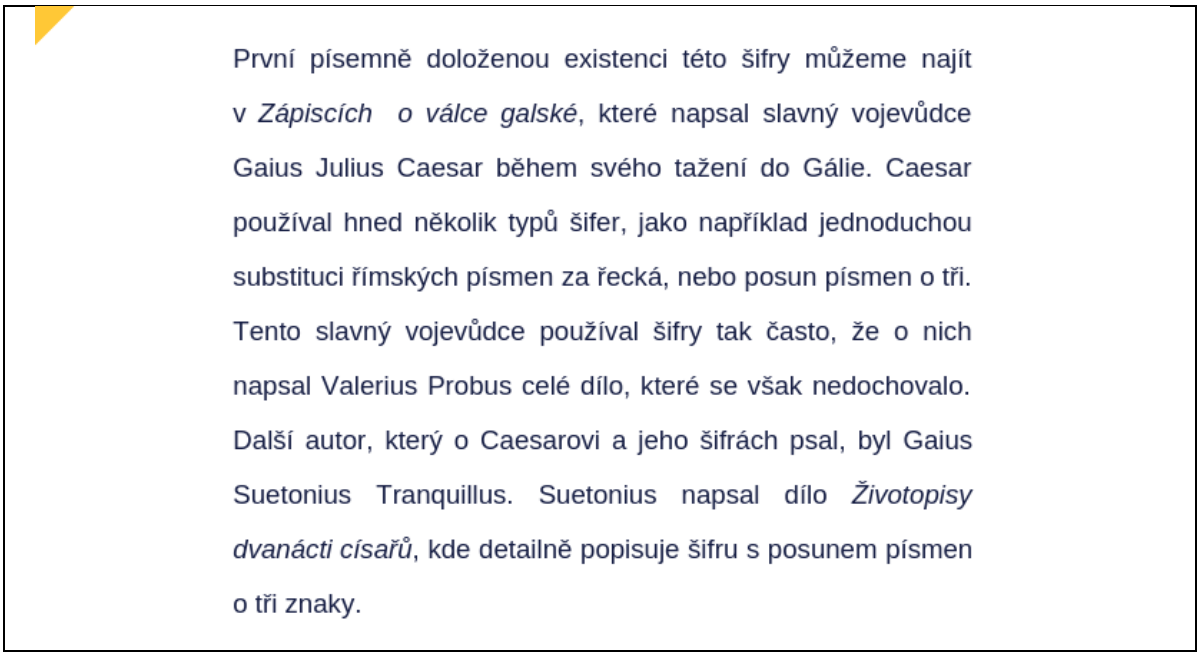
2.1.1 Titulní strana

Titulní strana je jedna z nejdůležitějších stran celého pracovního listu, jejíž funkce je především upoutat žáka. Barvy a design jsou u této strany nejzásadnější, jelikož tato strana rozhoduje o tom, zda se pracovní list zalíbí, či nikoliv. První strana obsahuje její název, což je i název samotného pracovního listu, popis, že se jedná o pracovní list a v neposlední řadě také obsah. Tento design sem zvolil, protože má žáka upoutat a zároveň být jednoduchý. Proto jsem vybral geometrické obrazce, které se částečně překrývají a dodávají pracovnímu listu určitou eleganci. V tomto pracovním listu mají i barvy svůj význam, ač možná pro mnoho lidí, skrytý. Žlutá, až oranžová barva, má symbolizovat středomoří, kde je hodně slunce a které je taktéž Caesarovým domovem. Šedá barva je barva kovu, zbrojí a mečů, tedy jeho legií.

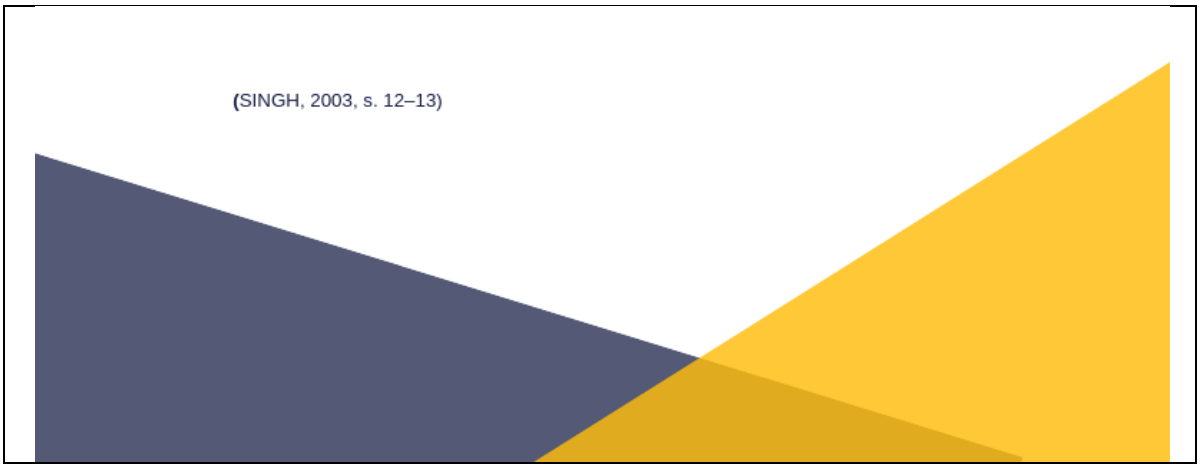
2.1.2 Úvod



Úvodní strana je z grafické stránky v podobném duchu jako titulní strana, avšak na této, i na následujících stránkách, jsem trojúhelníky nepoužil vertikálně, ale horizontálně. Tato změna umožnila více prostoru uprostřed pracovního listu a zároveň působí lepším dojmem. Tento list obsahuje stručný historický úvod o původu šifry a zdroj, odkud bylo čerpáno.



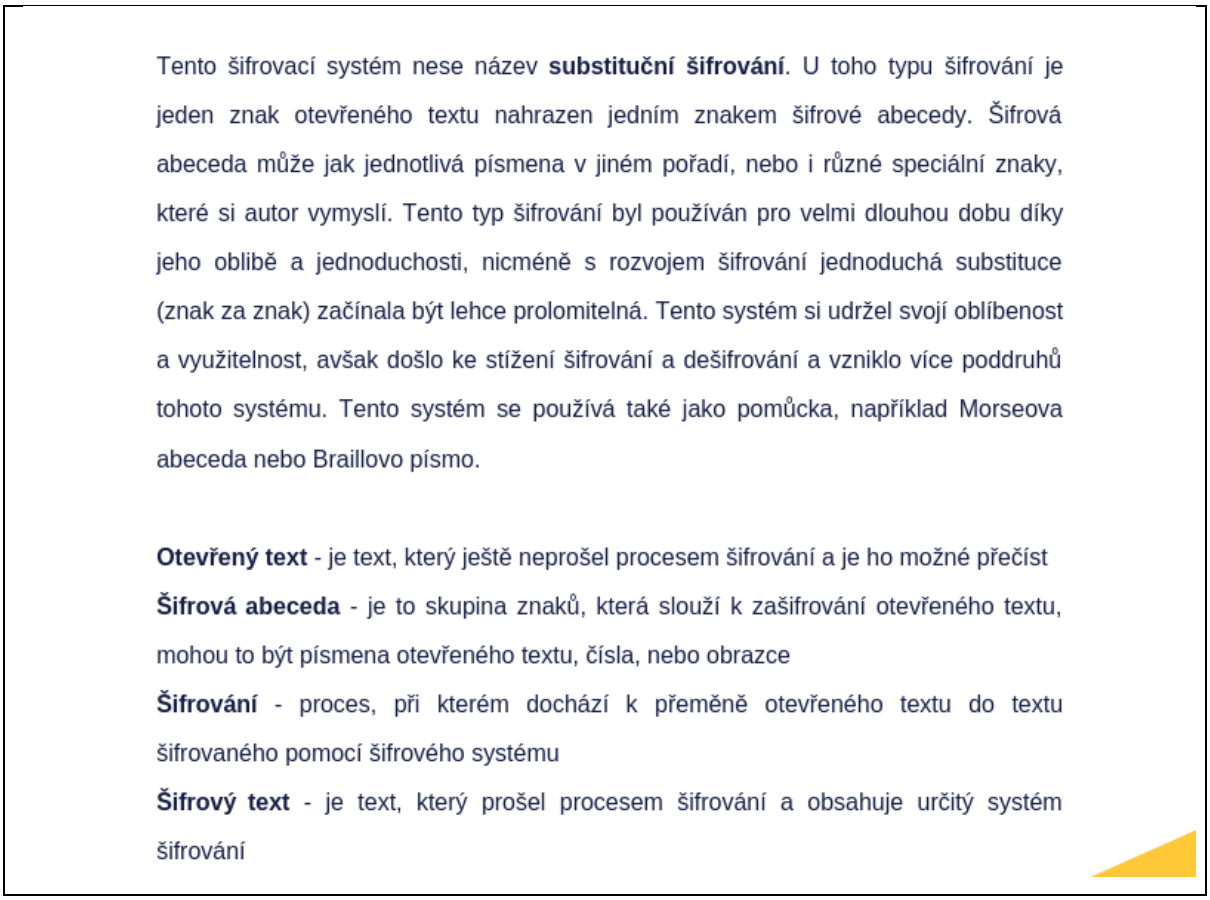
Celkově je úvod jednou z nejdůležitějších částí celého pracovního listu. V této části jsem popsal, kdo a kdy o Caesarově šifře psal. Díla autorů jsem napsal kurzívou, aby v samotném textu vynikla. Samotný úvod je poměrně stručný, nicméně jsem zvolil kratší variantu úvodu, protože jsem toho názoru, že žáci více ocení času na luštění šifry, než číst dlouhý úvod.



Třetí částí úvodu je odkaz na zdroj na knihu od autora, jehož publikace je velmi dobrým zdrojem informací o kryptografii a zároveň hodnotným zdrojem vývoje šifer. Nejspodnější část zabírají trojúhelníky, které si drží motiv předchozí strany.

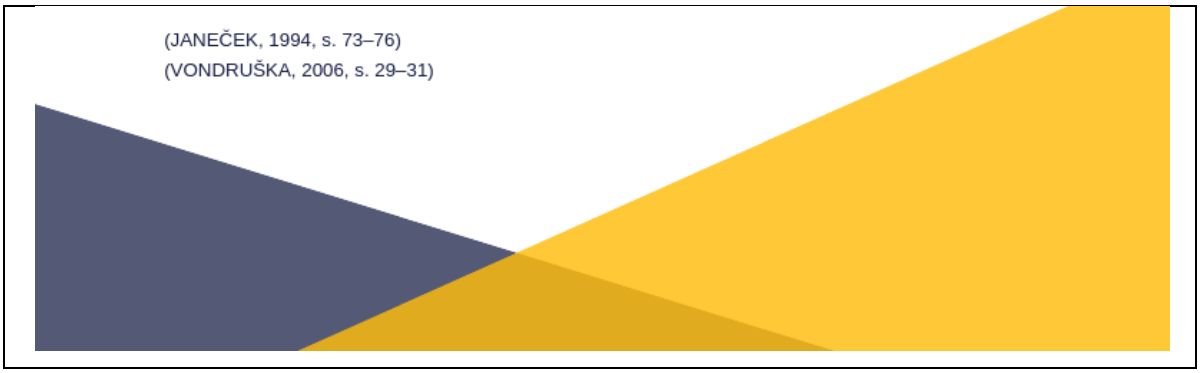
2.1.3 Definice šifrového systému

Třetí strana pracovního listu popisuje samotný šifrovací systém a používá cizích slov, která jsou pod textem vysvětlena. Stejně jako na předchozí straně, geometrické tvary sdílejí stejný význam, avšak zde jsou posunuty, aby pracovní list nepůsobil jednotvárně.



Samotný text definice jsem se snažil napsat velmi jednoduše, aby byl pro žáky co nejvíce pochopitelný, zároveň jsem se snažil, aby byl text co nejvíce stručný. Nicméně aby mohl být text stručný, musel jsem použít několik slovních spojení, které žáci neznají, kromě těch, co se už někdy věnovali kryptografii. Celý text je tedy rozdělen na dvě hlavní části, kdy v té první je definice a v té druhé jsou pojmy, které jsem použil v definici a které

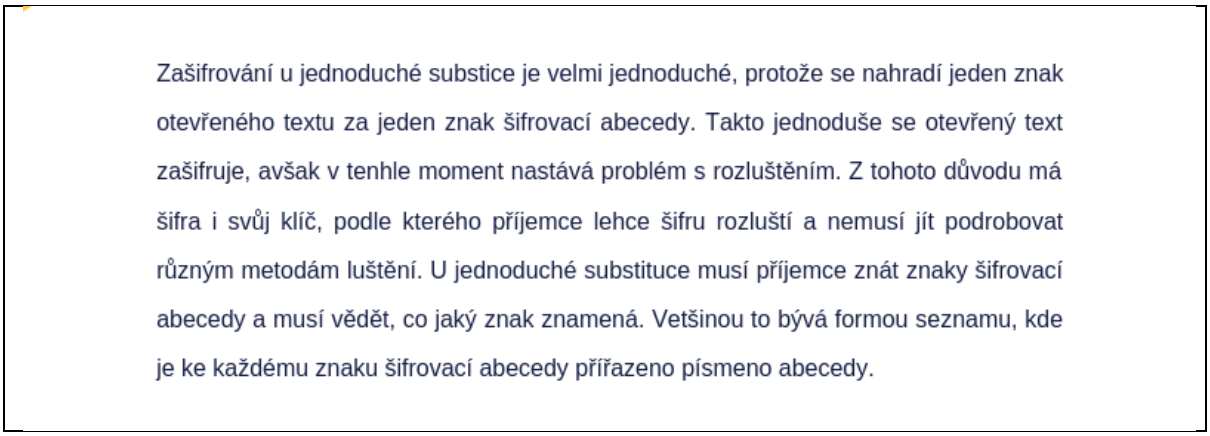
jsou vysvětleny. Zároveň jsem důležité pojmy zvýraznil, aby se upřednostnil jejich význam.



Poslední část této stránky obsahuje odkaz na zdroje, ze kterých jsem čerpal a které mohou být hodnotnými zdroji žákům pro další vzdělávání a získání informací o kryptografii. Nejspodnější část této strany je tvořena překrývajícími se trojúhelníky, které si udržují hlavní motiv, avšak styl překrytí je jiný, aby se narušila monotónnost pracovního listu a udržela jeho atraktivita.

2.1.4 Popis šifrování a dešifrování

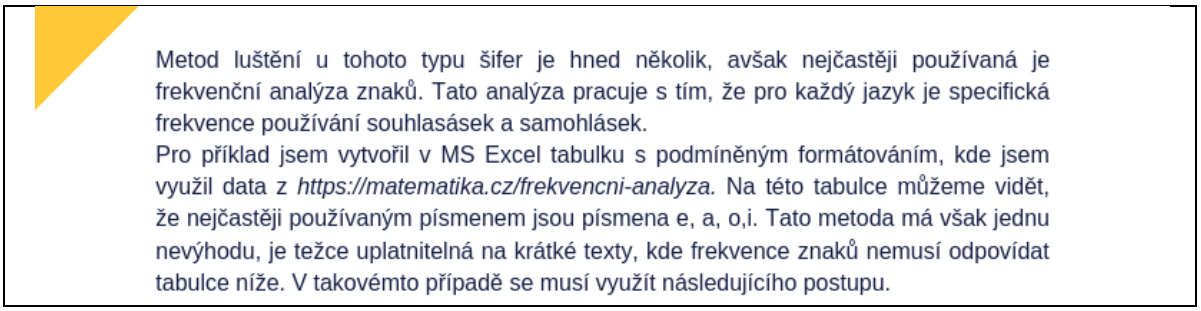
Pro mnoho žáků je mnoho textu unavující a pracovní list má být lehký pro žáky atraktivní, proto jsem zvolil popis šifrování a dešifrování stručnou formou. Snažil jsem se tento proces sepsat tak, aby byl co nejvíce pochopitelný a aby žákům nebyl na překážku.



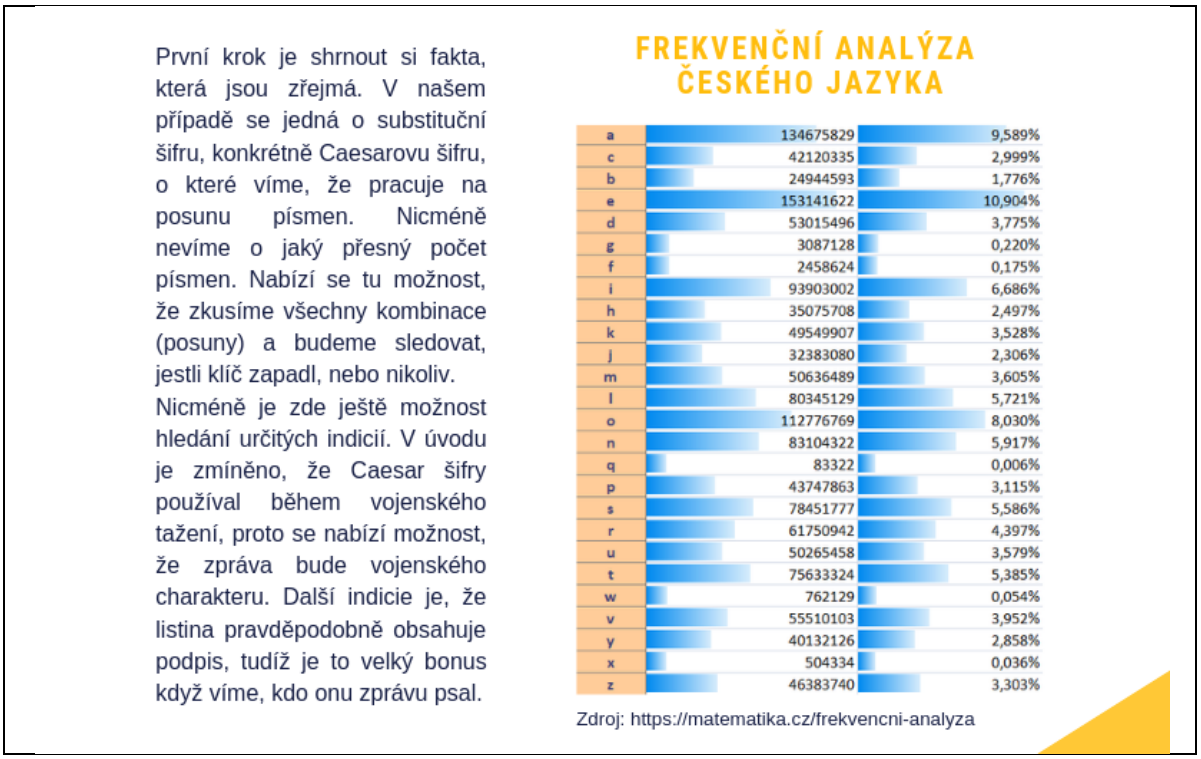
Samotný text je velmi krátký a neobsahuje žádné odborné pojmy, ani žádné jiné těžce pochopitelné výrazy. Je to z důvodu, aby žáci nad textem tolik neztráceli čas.

2.1.5 Metody luštění

Metody luštění je jedna z důležitých listů pracovního listu. Tuto stránku jsem rozdělil na dvě, kromě nadpisu, hlavní části, jelikož každá je o něčem trochu jiném.



Tato část popisuje metodu frekvenční analýzy, kdy jsem se ji snažil popsat co nejvíce jednoduše. V této části je taktéž zmíněn MS Excel, který v luštění šifer může hodně pomoci, nicméně není nutný, pokud člověk nepotřebuje rozluštit větší množství textu.

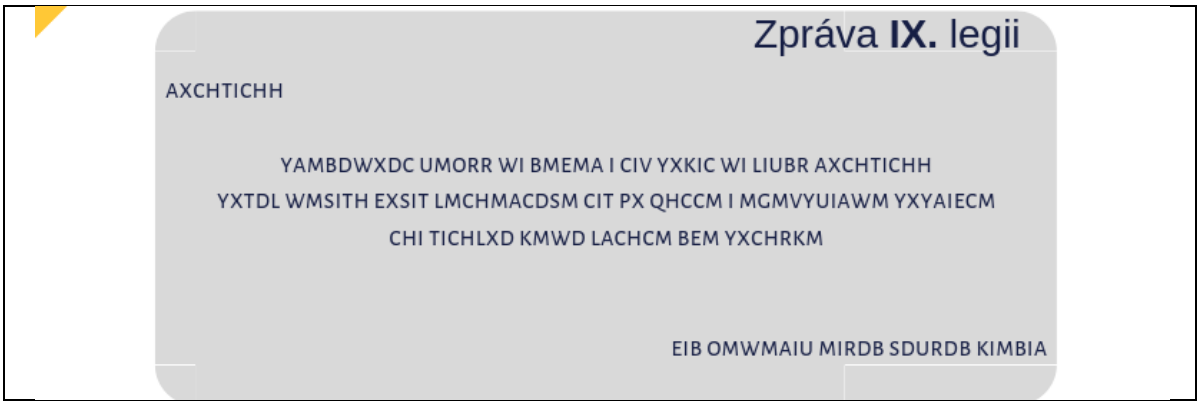


V této části se žáci dozvědí asi nejvíce informací potřebných k rozluštění šifry. Nachází se zde jak popis, jak k samotné šifře (obecně) postupovat, tak i postup, jakým je šifra zašifrována, taktéž žáci jenom potřebují vědět, o kolik políček je abeceda posunuta. Zároveň jsem zde zmínil nevýhody této šifry, protože když sem vymýšlel zadání této šifry, tak metoda frekvenční analýzy moc nekorespondovala, avšak ne ve všech směrech. K tomuto popisu jsem přidal graf frekvenční analýzy českého jazyka, kterou jsem vytvořil v MS Excel a na kterou jsem použil podmíněné formátování, které udělalo graf velmi přehledným. Data pro tento graf jsem využil z webu matematika.cz, který je uveden pod grafem.

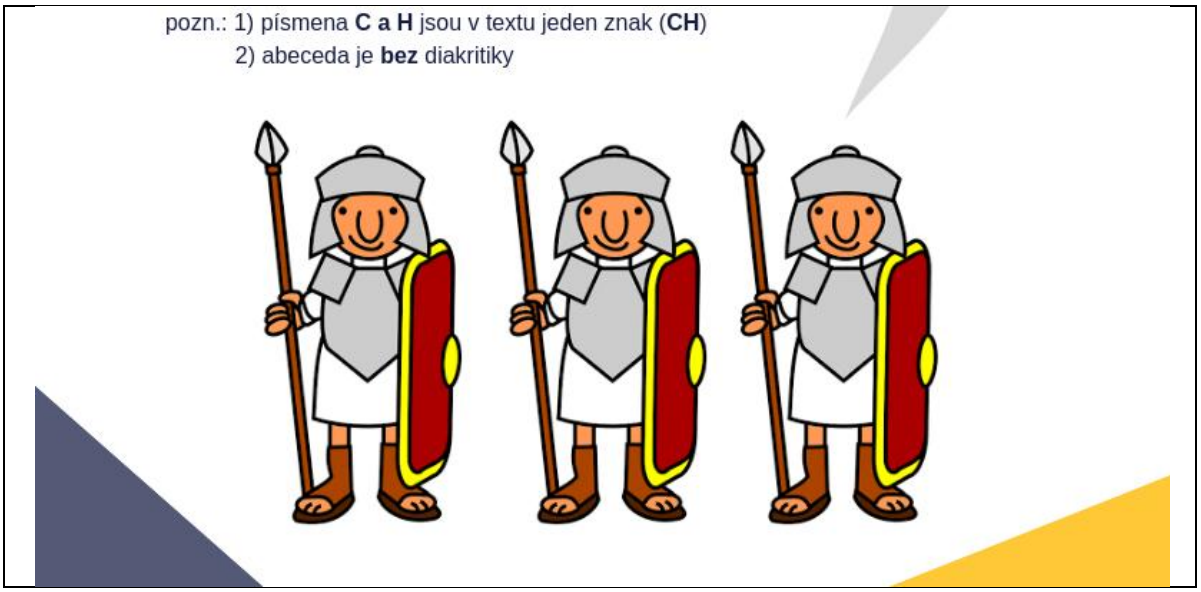
2.1.6 Zadání pracovního listu

Pro žáky asi nejvíce atraktivní část pracovního listu, kdy se po mnoha textech dostali konečně k samotné šifře. Tato konkrétní šifra (myšleno v tomto znění) není v žádné

publikaci, ani nikde na internetu. Tuto stránku jsem rozdělil na dvě hlavní části, na část se šifrou a na část poznámkami a přidaným grafickým prvkem.



Část se šifrou obsahuje mnou vymyšlený text, který se snaží držet si dobový ráz, jedná se totiž o vojenské rozkazy, to je jeden z důvodů, proč není šifra na luštění složitá. Samotnou šifru jsem dal do šedého obdélníku s kulatými rohy. Původně jsem chtěl použít jako pozadí pro šifru papyrus, ale z důvodu úspory barvy při tisku jsem zvolil jednodušší provedení, které se však drží motivu pracovního listu.



V této části můžeme nalézt poznámky k šifře. Jsou dvě a nejdůležitější části jsou zvýrazněny tučně, aby se předešlo přehlédnutí. Hned pod nimi jsou obrázky tří legionářů, které mají šifře dodat ten správný význam a mají narušit opakující se motivy, které klesají na atraktivitě. Tyto obrázky jsem získal na webu clcker.com, kde si může libovolný uživatel internetu stáhnout nabízené obrázky, aniž by se musel registrovat, či vyplňovat nějaké ověřovací formuláře (http://www.clker.com/clipart-roman-soldier.html).

Stránka, která následuje po zadání šifry je určena pro poznámky k řešení šifry. Zvolil jsem obdélník, který je vyplněn tečkami seřazenými do řádků, avšak ničím jsem ho neohraničoval, protože by pak místo pro psaní vypadalo velmi uzavřeně vzhledem k bílé ploše kolem tohoto pole.

2.1.7 Řešení

ŘEŠENÍ

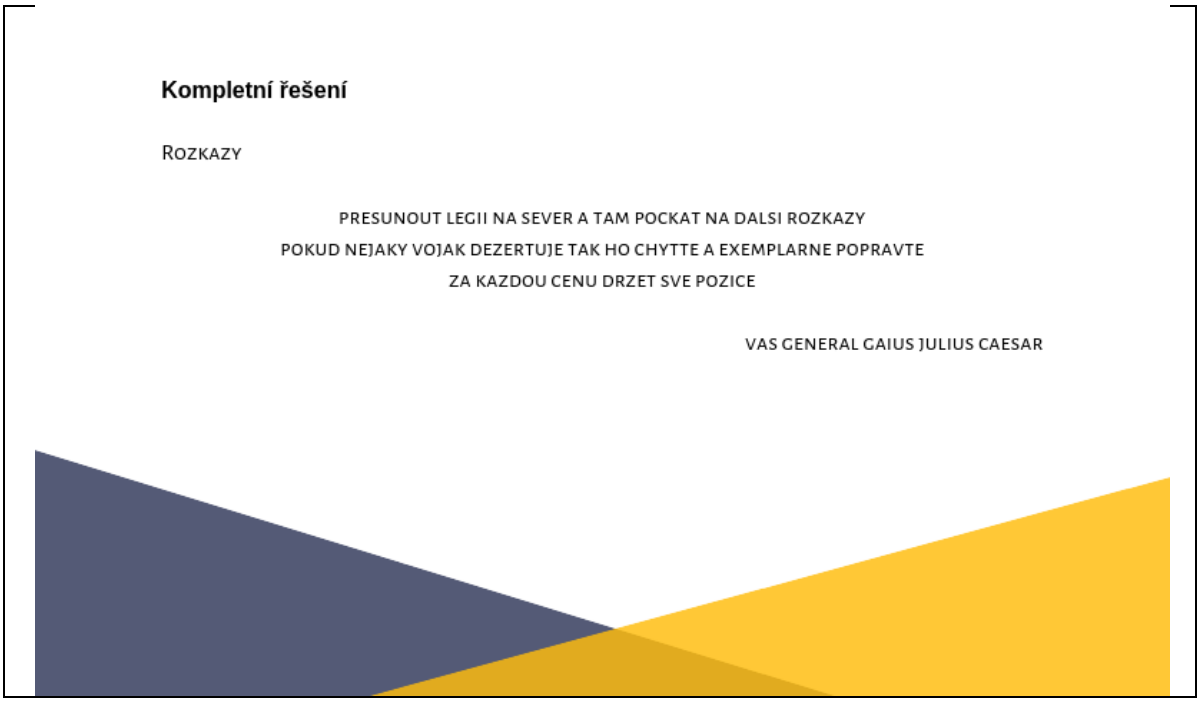
Následující řešení je pomocí tabulky, která je zároveň klíčem k šifře výše. Pod tabulkou je přepsaný celý text.

1	2	3	4	5	6	7	8	9	10
a	b	c	d	e	f	g	h	ch	i
i	j	k	l	m	n	o	p	q	r

11	12	13	14	15	16	17	18	19	20
j	k	l	m	n	o	p	q	r	s
s	t	u	v	w	x	y	z	a	b

21	22	23	24	25	26	27
t	u	v	w	x	y	z
c	d	e	f	g	h	ch

Stránku s řešením jsem rozdělil na dvě hlavní části. První část obsahuje tabulku s klíčem, kde jsem v MS Excel vytvořil tabulku s abecedou a abecedu posunutou o devět políček (šifra). Tabulku jsem zvýraznil a přeměnil tak, aby byla dobře čitelná. Po tabulce následuje kompletní řešení šifry.



Kompletní řešení

ROZKAZY

PRESUNOUT LEGII NA SEVER A TAM POCKAT NA DALSI ROZKAZY
POKUD NEJAKY VOJAK DEZERTUJE TAK HO CHYTTE A EXEMPLARNE POPRAVTE
ZA KAZDOU CENU DRZET SVE POZICE

VAS GENERAL GAIUS JULIUS CAESAR

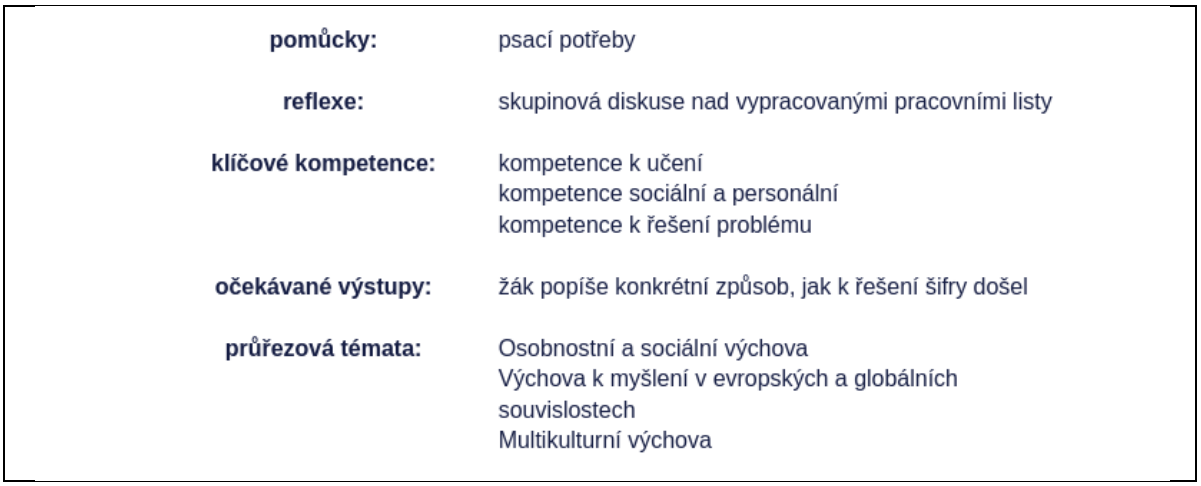
Kompletní řešení šifry obsahuje přepis samotné šifry. Celá šifra je bez diakritiky, jak již bylo zmíněno v zadání. Při přepisu jsem zanechal řádky i mezery naprosto identicky

s šifrou a díky tomu je pak kontrola správnosti velmi rychlá. Celá stránka obsahuje, stejně jako předchozí stránky, překrývající se trojúhelníky, jak v hlavičce strany, tak i v patičce. Tyto trojúhelníky mění tvar svého překrytí, aby pracovní list nevypadal jednotvárně.

2.1.8 Metodické poznámky

Metodické poznámky, asi nejdůležitější list pro učitele. Tato stránka obsahuje, mimo nadpisu a grafického zpracování hlavičky a patičky, seznam věcí, které jsou nezbytné pro správné fungování a zařazení pracovního listu.

První položkou seznamu jsou cíle. Cíl je nejdůležitější věcí celého seznamu, protože bez něj by nebylo možné s pracovním listem pracovat a taktéž bez cíle by neměl žádný smysl, byl by to jen text a to by bylo všechno. Další položkou je věková skupina, která je taktéž velmi důležitá, protože pokud by byl pracovní list dán skupině žáků nad doporučený věk, vyřešili by ho velmi jednoduše, naopak pro žáky mladší by byl téměř neřešitelný. Následuje organizace činnosti, která je spíš doporučením, než pravidlem, protože pro práci s šiframi se nabízí práce ve skupině, která je další diskusi mnohem lepší, a také rozvíjí více klíčových kompetencí. Čas potřebný ke zpracování je taktéž orientační, protože může být třída, která zvládne šifru vyřešit za 30 minut a druhá ani ne za 45 minut, nicméně záleží na věkové skupině a celkové připravenosti třídy.



pomůcky:	psací potřeby
reflexe:	skupinová diskuse nad vypracovanými pracovními listy
klíčové kompetence:	kompetence k učení kompetence sociální a personální kompetence k řešení problému
očekávané výstupy:	žák popíše konkrétní způsob, jak k řešení šifry došel
průřezová témata:	Osobnostní a sociální výchova Výchova k myšlení v evropských a globálních souvislostech Multikulturní výchova

Pomůcky pro tuto šifru stačí pouze psací potřeby, protože šifra je tak jednoduchá, že není potřeba mobilních telefonů, nebo jiných zařízení. Důležitou položkou jsou reflexe. Reflexe by měla vždy proběhnout na konci této aktivity a měla by shrnout vše, co pracovní list měl sdělit, taktéž je vhodnou formou shrnutí diskuse. Nedílnou součástí je seznam klíčových kompetencí, které jsou u žáků rozvíjeny a bez kterých by nebyl pracovní list hodnotný pro osobní rozvoj žáků. Následují očekávané výstupy, kde je popsáno, co žák zvládne po splnění pracovního listu vysvětlit, nebo popsat. Poslední položkou je seznam průřezových témat, do kterých pracovní list zasahuje a které by si žáci měli osvojovat.

2.1.9 Zdroje

ZDROJE

SEZNAM LITERATURY

JANEČEK, Jiří. *Rozluštěná tajemství: luštitelé, dešifranti, kódy a odhalení.* Praha: XYZ, 2006, 268 s. ISBN 80-86864-54-5.

SINGH, Simon. *Kniha kódů a šifer: tajná komunikace od starého Egypta po kvantovou kryptografii.* 2. vyd. v českém jazyce. Přeloţil Dita ECKHARDTOVÁ, přeloţil Petr KOUBSKÝ. Praha: Dokořán, 2009, 382 s. Aliter. ISBN 978-80-7363-268-7.

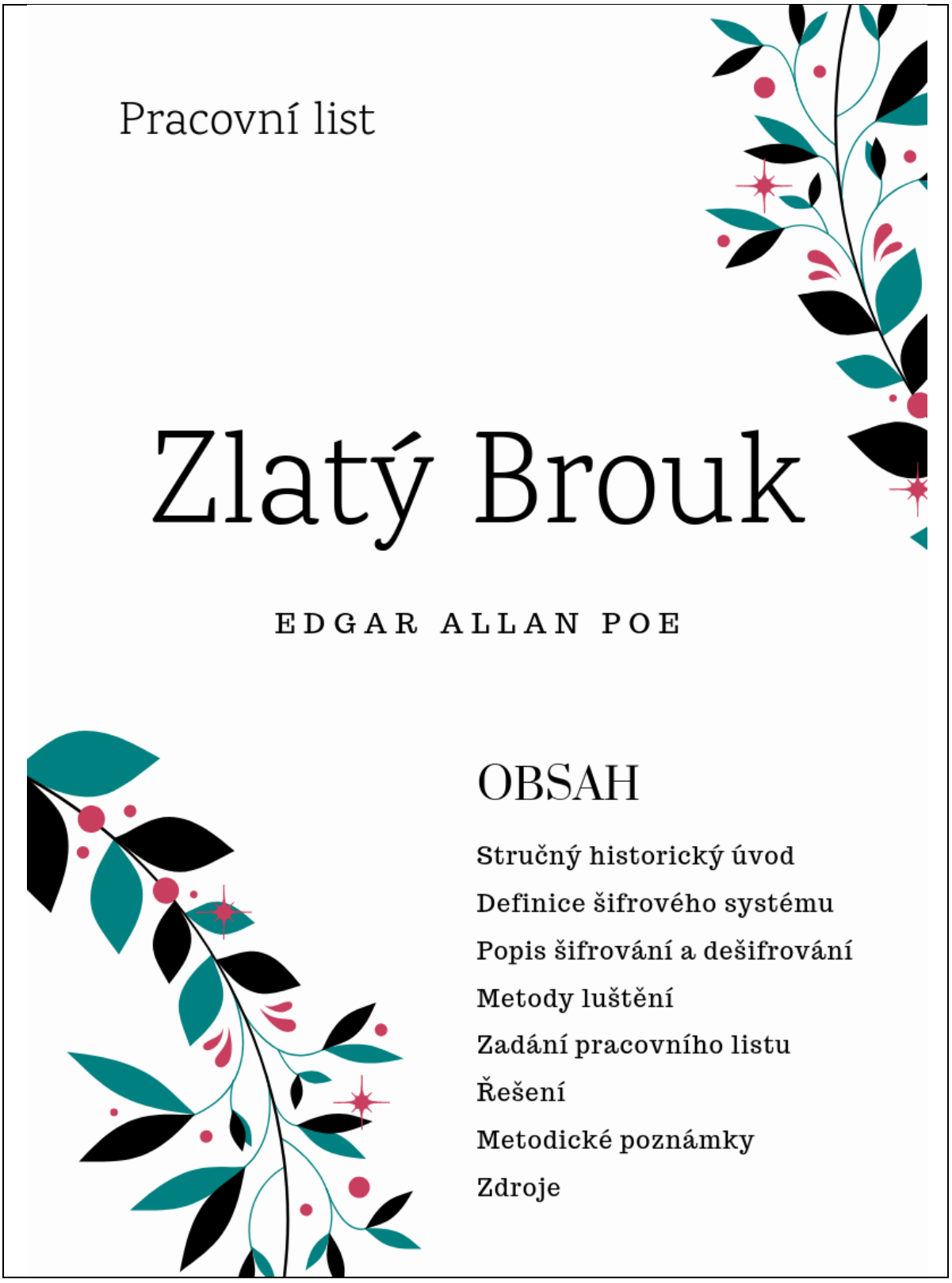
VONDRUŠKA, Pavel. *Kryptologie, šifrování a tajná písma.* Praha: Albatros, 2006, 340 s. Oko. ISBN 80-00-01888-8.

Poslední stranou pracovního listu jsou zdroje. Tato stránka obsahuje, kromě nadpisu a grafického zpracování hlavičky a patičky, také seznam literatury. Seznam literatury je napsán v souladu s platnou citační normou a abecedně seřazen. Tento seznam slouží jednak jako odkaz na zdroje, taktéž jako případná opora pro žáky, kteří by chtěli

dále rozvíjet svoje znalosti a dovednosti v oblasti kryptografie. Seznam literatury neobsahuje žádné internetové zdroje, protože jsem je v práci nepoužil.

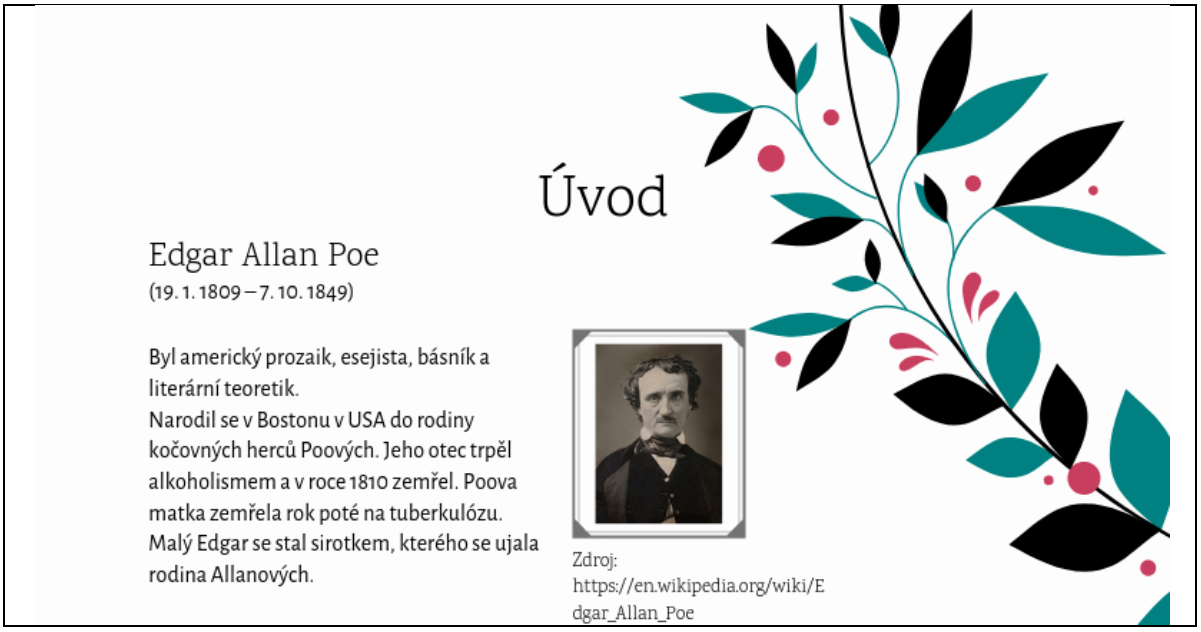
2.2 Pracovní list – 2 „Zlatý Brouk“

2.2.1 Titulní strana

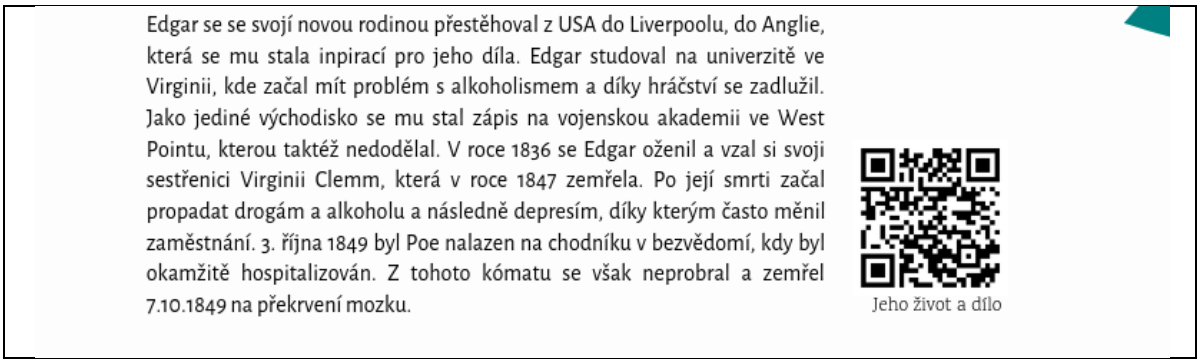


Hlavním cílem pracovního listu je žáka zaujmout, proto si myslím, že titulní strana je hlavním spouštěčem toho, jak žák bude pracovní list na první pohled vnímat. Titulní strana nese velkým písmem název a to „Zlatý Brouk“, podle povídky, kterou napsal Edgar Allan Poe. Jméno autora se nachází hned pod názvem díla. V hlavičce „titulky“ je taktéž označení, že se jedná o pracovní list. V druhé polovině titulní strany se nachází obsah pracovního listu, kde jsou pojmenovány konkrétní stránky. Z grafické stránky je jak titulní strana, tak i celý pracovní list, doplněn barevnými ornamenty, které mají zvýšit atraktivitu pracovního listu. Tyto ornamenty jsou v pravém horním a levém dolním rohu. Pracovní list je navržen tak, aby ho bylo možné tisknout černobíle a byla zároveň zachována jeho atraktivita a vzhled, zároveň je šetrný na barvu do tiskáren.

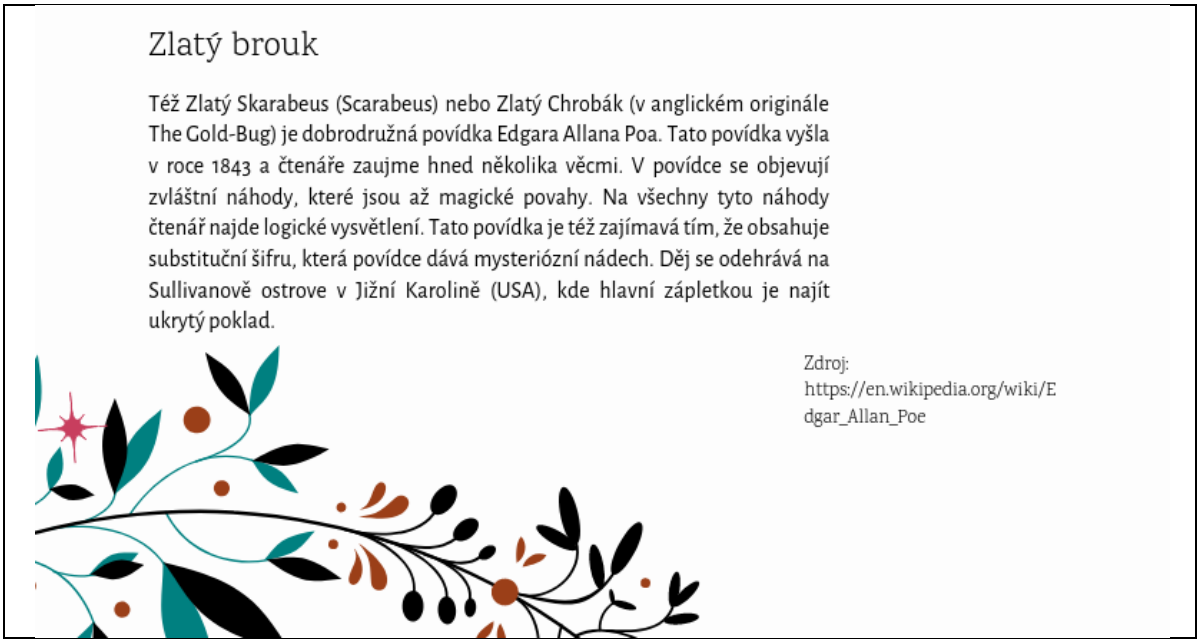
2.2.2 Úvod



Jednou z nejdůležitějších stran pracovního listu je úvod. Úvod má za cíl žáka vnést do pracovního listu a nastínit mu, co ho čeká v následujících listech. Tato stránka je rozdělena tematicky na několik pomyslných částí. První část, která obsahuje název „Úvod“, je samotném autorovi. Obsahuje jeho jméno, datum narození a úmrtí a samozřejmě také stručně jeho život. Samozřejmě tato část obsahuje také autorovu fotku a zdroj. Podobně jako titulní strana, má i tato část ornamentální dekoraci v pravém horním rohu, avšak trochu jinou, aby se narušila případná monotónnost pracovního listu.

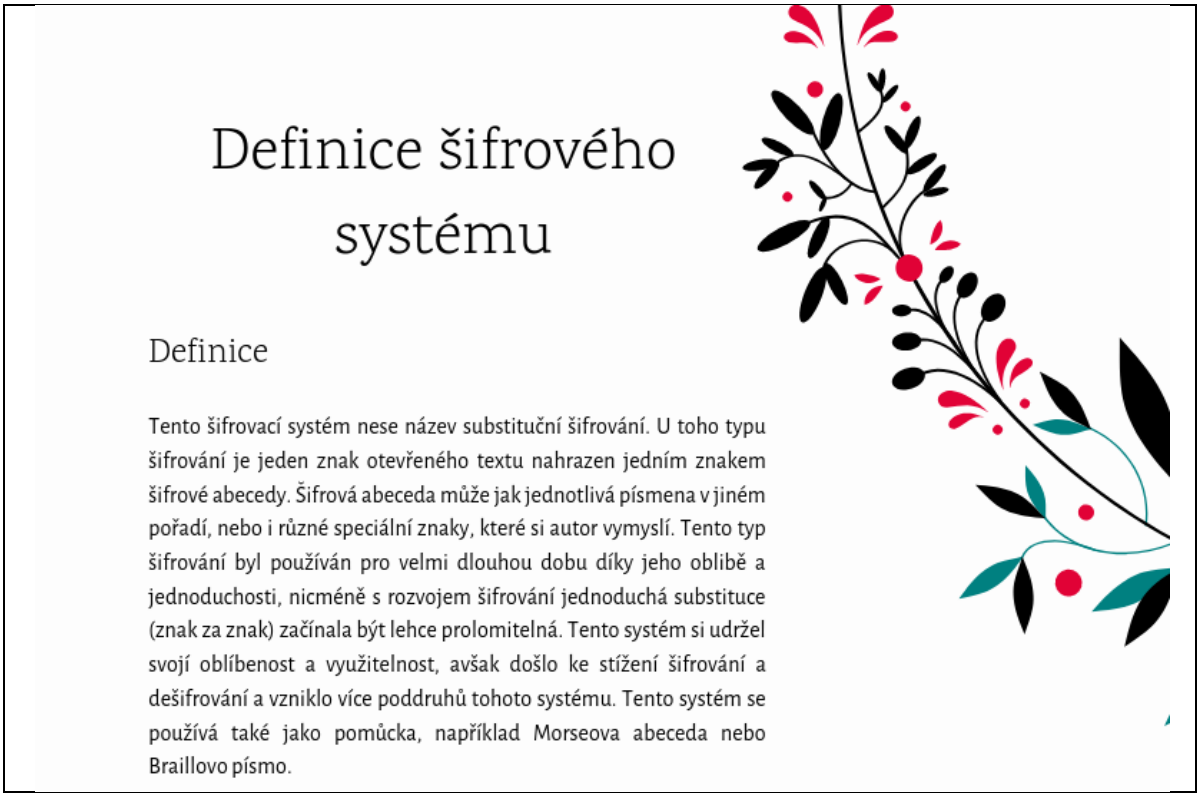


Protože by tak krátký odstaveček nebyl adekvátním shrnutím tak významného autora, je tato strana doplněna širším, avšak taktéž stručným popisem jeho života. Pro žáky, kteří by se více zajímali o jeho život, jsem přidal QR kód, který jsem vytvořil na webu QR generátor (https://www.qrgenerator.cz/). Následuje autorovo dílo, ve kterém se šifra nachází.



Tato závěrečná část úvodní strany obsahuje stručný popis díla „Zlatý Brouk“, informaci, že v tomto díle se objevuje šifra. Patička stránky je doplněna dekorativními ornamenty, které se liší od předchozích (tvarem nebo barvou), a zdrojem.

2.2.3 Definice šifrového systému

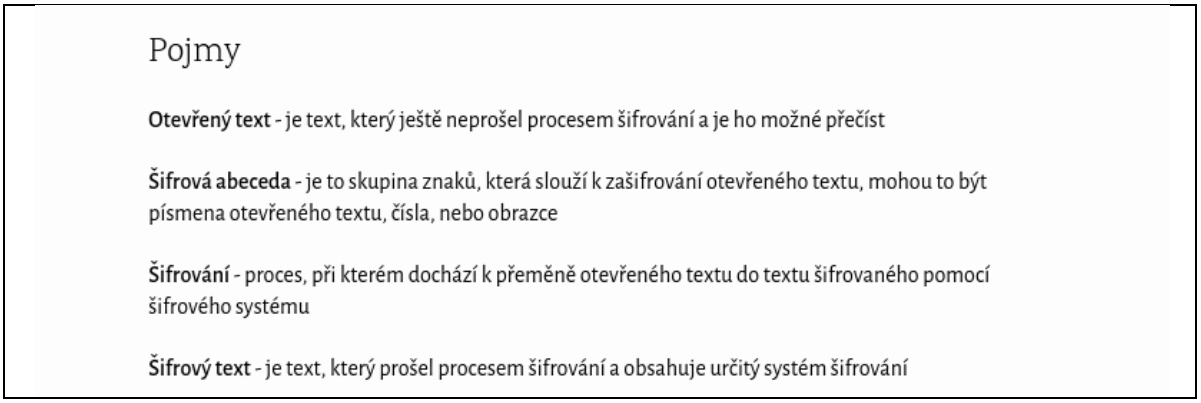


Definice šifrového systému

Definice

Tento šifrovací systém nese název substituční šifrování. U toho typu šifrování je jeden znak otevřeného textu nahrazen jedním znakem šifrové abecedy. Šifrová abeceda může jak jednotlivá písmena v jiném pořadí, nebo i různé speciální znaky, které si autor vymyslí. Tento typ šifrování byl používán pro velmi dlouhou dobu díky jeho oblibě a jednoduchosti, nicméně s rozvojem šifrování jednoduchá substituce (znak za znak) začínala být lehce prolomitelná. Tento systém si udržel svojí oblíbenost a využitelnost, avšak došlo ke stížení šifrování a dešifrování a vzniklo více poddruhů tohoto systému. Tento systém se používá také jako pomůcka, například Morseova abeceda nebo Braillovo písmo.

Slovo definice u žáků často vzbuzuje obavy, nebo pocit, že je to složité. Tuto stránku pracovního listu jsem rozdělil na dvě části a ta první obsahuje samotnou definice. Protože sám vím, že definice nebývají obvykle každému hned jasné, rozhodl jsem se jí parafrázovat tak, aby byla pro žáky napsána „lidsky“ a stručně, pokud možno. Díky tomu se mi podařilo definici shrnout do jednoho odstavce, kde jsem však byl nucen použít několik slovních spojení, u kterých nemusí být na první pohled zřejmý význam. Samotná hlavička stránky je vyzdobena dekorativními ornamenty, které mají narušit svým měnícím se vzhledem pocit, že je žák zaplavován texty.



Pojmy

Otevřený text - je text, který ještě neprošel procesem šifrování a je ho možné přečíst

Šifrová abeceda - je to skupina znaků, která slouží k zašifrování otevřeného textu, mohou to být písmena otevřeného textu, čísla, nebo obrazce

Šifrování - proces, při kterém dochází k přeměně otevřeného textu do textu šifrovaného pomocí šifrového systému

Šifrový text - je text, který prošel procesem šifrování a obsahuje určitý systém šifrování

Jak jsem již výše zmínil, použil jsem v textu několik výrazů, které žáci pravděpodobně znát nebudou, pokud se již nezajímali o něco z kryptografie. Proto jsem

druhou část této strany nazval „Pojmy“ a zde sem ty nejdůležitější vysvětlil. Pro lepší přehlednost jsem zmíněné pojmy zvýraznil tučně a nechal mezi nimi větší mezery, například pro žáky se specifickými poruchami učení.

Patička stránky obsahuje opět dekorativní ornament, který je poměrně výrazný a má vzbudit pocit lehkosti, protože je na něm modrá a zelená v kombinaci s černou. Zároveň tato část obsahuje odkaz na zdroje, odkud jsem čerpal a odkud mohou případně žáci čerpat, pokud je toto téma bude do budoucna zajímat.

2.2.4 Popis šifrování a dešifrování

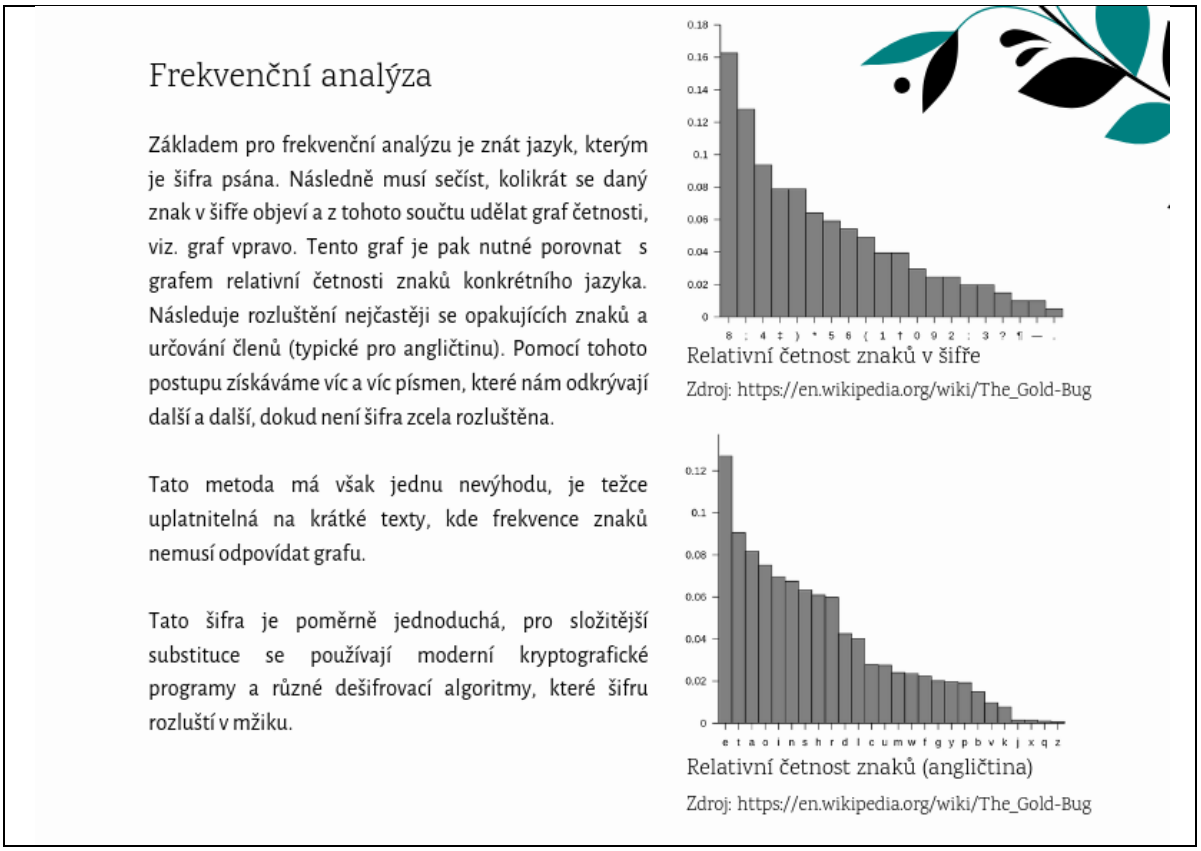
Tento list se jeví jako nejdůležitější z celého pracovního listu, avšak pro úspěšné zvládnutí rozluštění šifry je podstatné pochopit definici, proces jakým se šifruje a dešifruje, tak i metody, které následují. Stránka je rozdělena na dvě hlavní části. První částí je horní

polovina strany, která obsahuje název a podnadpis (šifrování). Následuje popis procesu šifrování substituční šifry, kdy jsem se snažil jednoduše tento proces popsat, aby jej žáci snadněji pochopili.

Druhou polovinou strany je část dešifrování, která taktéž popisuje proces šifrování, jen opačným způsobem. Zároveň tato část obsahuje odkaz na zdroje, pokud by chtěli zapálení žáci zjistit více informací o tomto tématu. A v neposlední řadě strana obsahuje dekorativní ornament, který má trochu jiný motiv a jiné barvy, než ten na předešlé straně - je to z důvodu, aby žákům nepřišly stránky všechny stejné a pracovní list je nenudil.

2.2.5 Metody luštění

Metody luštění - jeden z nejdůležitějších listů k získání řešení samotné šifry. Tuto stránku jsem rozdělil na dva hlavní celky. Prvním z nich je definice, kde je popsána metoda, jakou se substituční šifra luští. Samotná definice je velmi stručná, jednoduchá a pokračuje názorným popisem a grafy níže.

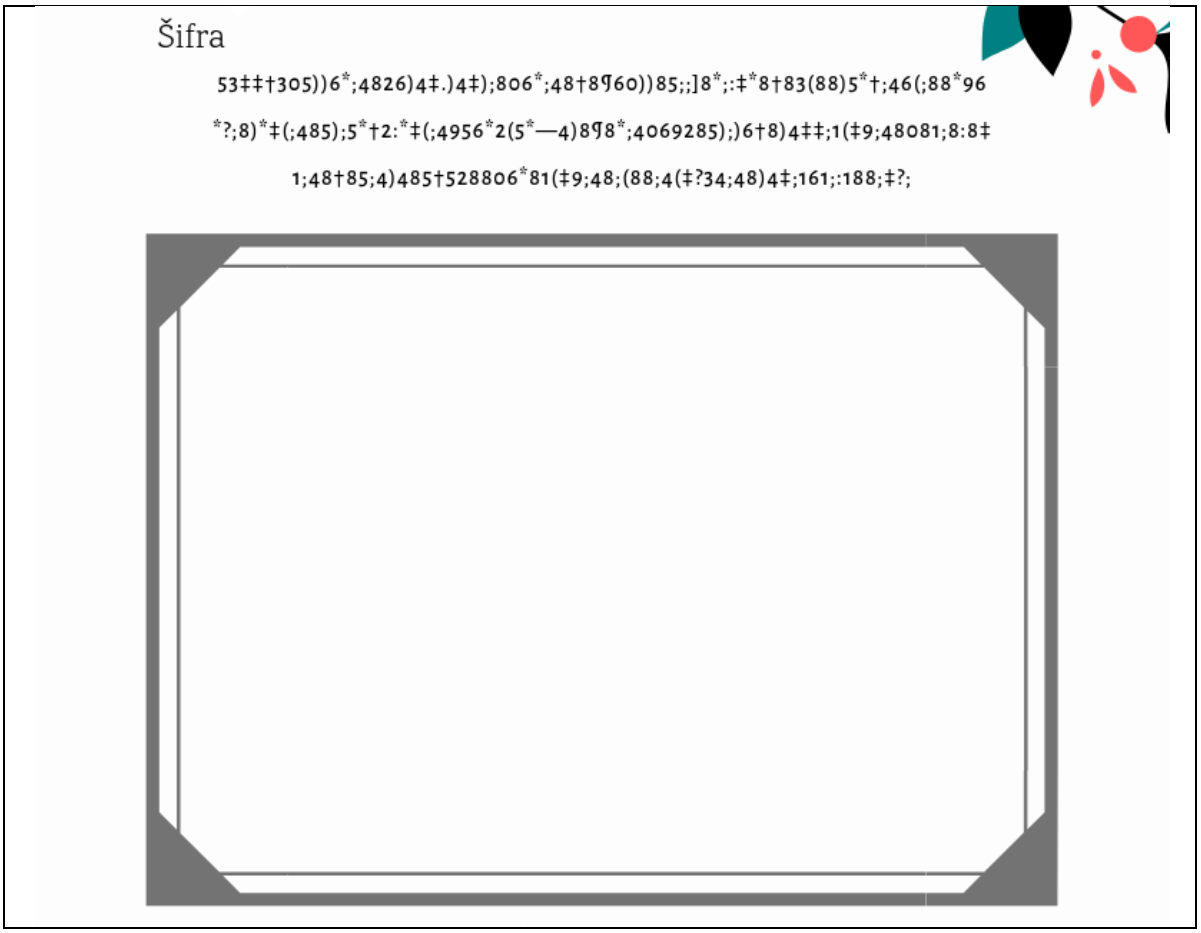


Jak již název napovídá, tento celek se zabývá frekvenční analýzou. Žákům je zde napsán postup, jak si s touto metodou počínat a aby to žáci měli o něco jednodušší, přiložil sem k této části dva grafy. První graf ukazuje relativní četnost znaků v samotné šifře, tudíž žákům stačí jen ho porovnat s grafem níže, což je relativní četnost znaků anglického jazyka

(šifra je psána anglicky). U obou grafů je uveden zdroj. I když se toto může jevit, že se jedná o samotné řešení, tak to tak vůbec být nemusí, protože jak je uvedeno v pracovním listu, graf relativní četnosti je spolehlivý na dlouhý text. Stejně jako předchozí listy, i tento je doplněn o dekorativní ornamenty, které se liší tvarem a barvou od předchozích.

2.2.6 Zadání pracovního listu

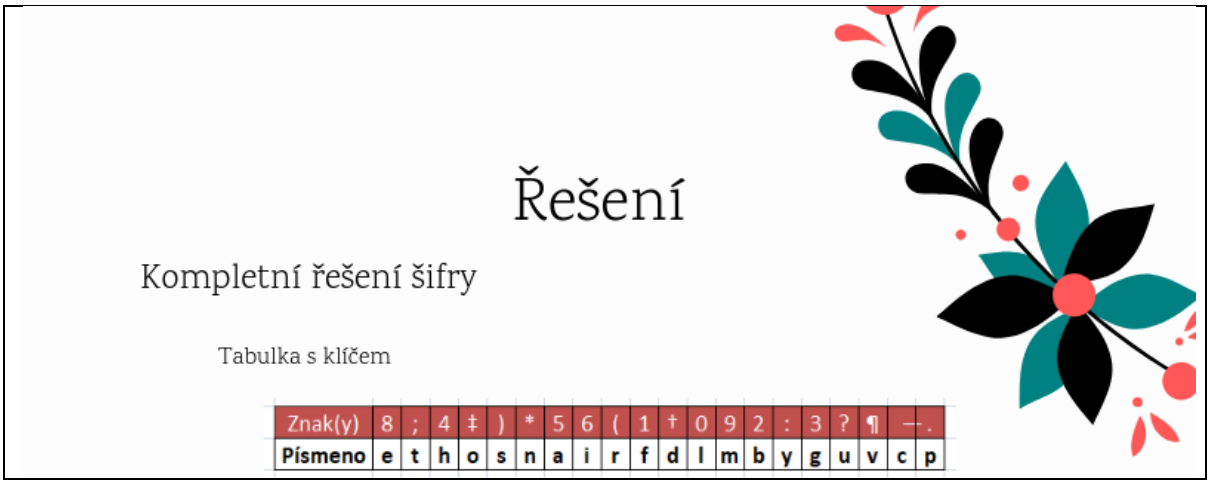
Pro žáky asi nejvíce atraktivní list. Už jen hlavička tohoto listu je zvláštní jedním prvkem a to je zlatý brouk. Hlavička je též doplněna zdobnými ornamenty, avšak bez zmíněného zlatého brouka by již tento vzor ztrácel na atraktivitě. Tento list je rozdělen na dvě hlavní části, na hlavičku, která je popsána výše, na zadání samotné šifry a na patičku.



Zadání samotné šifry může působit trochu chaoticky a neorganizovaně, avšak pokud žáci použijí metodu frekvenční analýzy, kde mají dokonce graf relativní četnosti znaků v šifře, tak jim luštění půjde poměrně rychle. Aby tato část působila uceleně, doplnil jsem do pracovního listu zdobený obdélník, do kterého mohou žáci zapisovat postup při řešení šifry. Tento obdélník obsahuje i následující strana, která poskytuje prostor pro další zápisky a která je v příloze (Příloha – A02), kde je přiložen kompletní pracovní list.

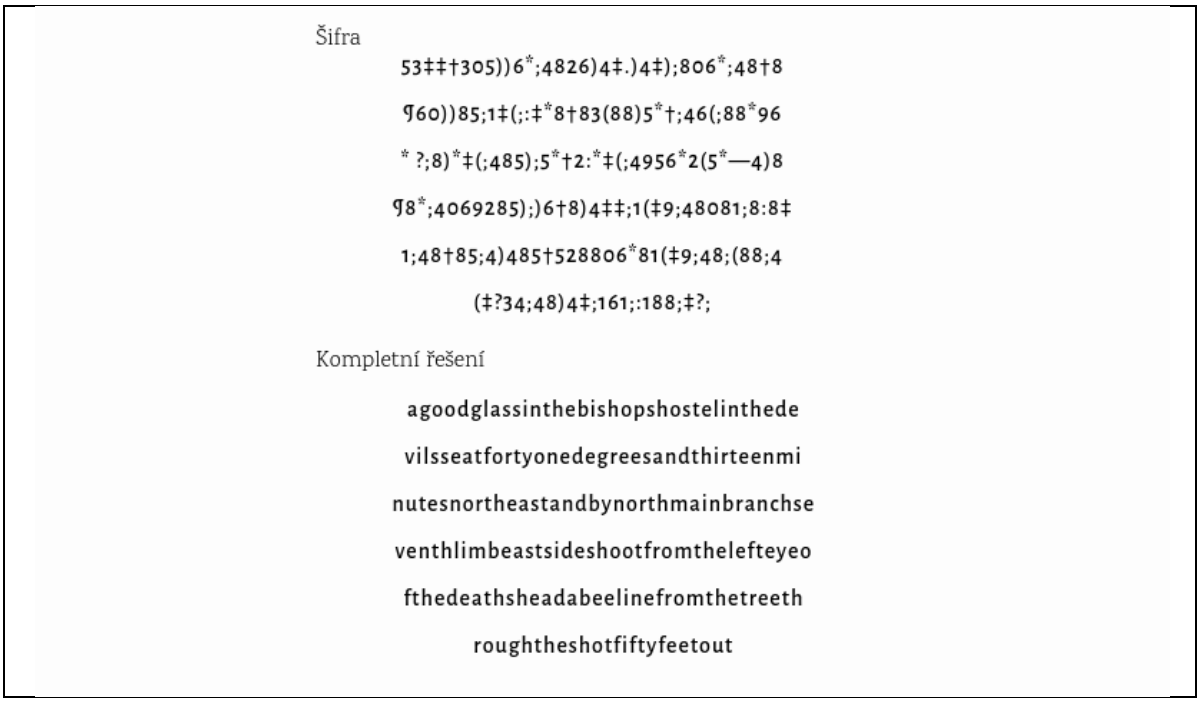
Patička zadání pracovní listu je taktéž zvláštní, oproti ostatním listům, a to především tím, že obsahuje dva zlaté brouky, mimo dekorativní ornamenty, které jsou na každé straně. Tito brouci jsou schválně jeden větší a jeden menší a to z důvodu, aby žákům přišel list, že se mění, že to není duplikát, kterému se mění text. U obrázků brouků jsem nedával zdroj, protože obrázek brouka pochází z webu Pinterest (https://cz.pinterest.com).Tato část taktéž obsahuje zdroj šifry.

2.2.7 Řešení

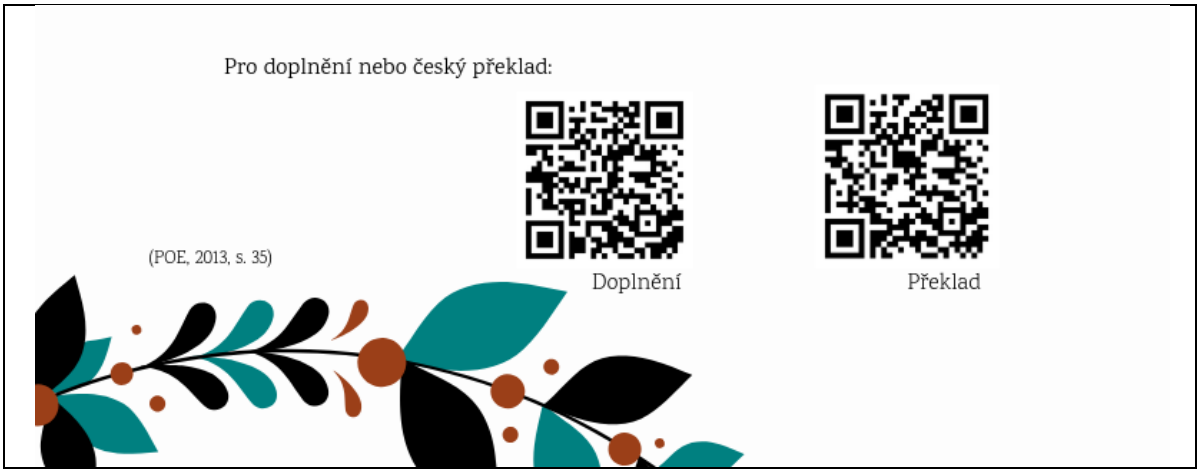


Samotný list řešení jsem rozdělil na tři části. První částí je hlavička, s dekorativním ornamentem, nadpisem, podnadpisem a tabulkou, která je klíčem k šifře. Tuto tabulku

vytvořil v MS Excel, kterou jsem naformátoval tak, aby ladila s designem pracovního listu. Zároveň je tato tabulka klíčem k rozluštění šifry. V následující části je přepis šifry.



V této části je samotná šifra, u které jsem nejdříve napsal přepis šifry nerozluštěné a následně hned pod to dodal kompletní řešení, tzn. celý přepis šifry. Pro lepší kontrolu jsem zanechal řádky u obou přepisů stejně, aby následná kontrola byla rychlejší.



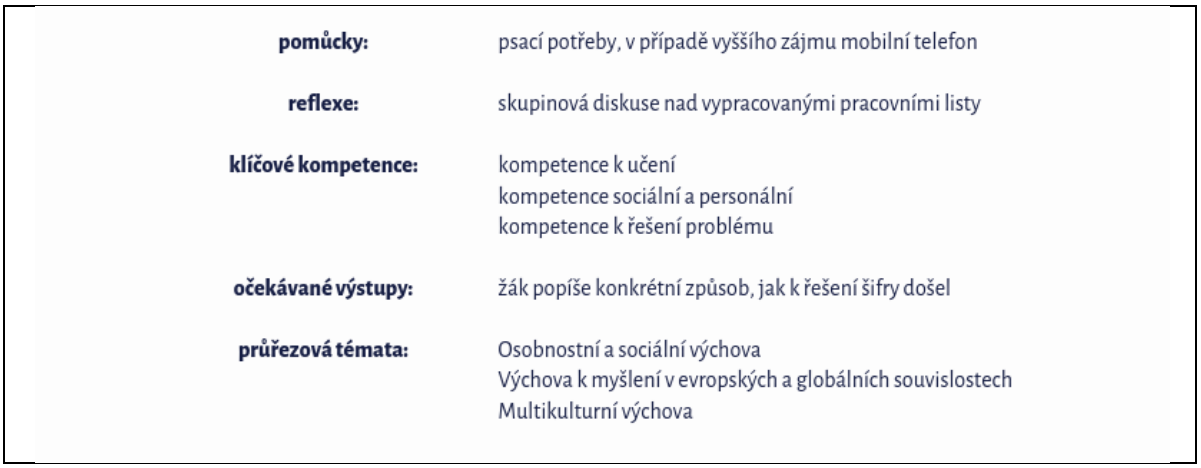
Patičku této části tvoří především dva QR kódy, které jsem vygeneroval na webu QR generátor (https://www.qrgenerator.cz/). První QR kód, který se jmenuje doplnění, odkazuje na život a povídku, kterou napsal Edgar Allan Poe. Druhý QR kód odkazuje na jeho povídku, kde je český překlad šifry, pokud by žáci nerozuměli anglické verzi šifry. Spolu s QR kódy je zde odkaz na knihu a konkrétní stranu, kde lze šifru nalézt.

Nejspodnější část je doplněna dekorativními ornamenty, které jsou opět jiné, než na předchozí straně.

2.2.8 Metodické poznámky

Metodické poznámky, asi nejdůležitější list pro učitele. Tento list jsem rozdělil na dvě hlavní části a to především kvůli přehlednosti popisu.

První a nejdůležitější věc v těchto poznámkách je cíl. Cíl je naprosto stěžejní, protože bez něj by nebylo možné s pracovním listem pracovat a neměl by žádný smysl. Další důležitou položkou je věková skupina, která je taktéž dost zásadní. Důležitá je proto, že pokud se dá žákům, nad hranici, bude pro ně velmi jednoduchá, naopak, pokud se dá žákům pod hranici, bude pro ně téměř neřešitelná. Následuje organizace činnosti, ve které jsem popsal ideální zadání pracovních listů v hodině, kdy je vhodné využít skupinovou práci. Avšak tato část není povinná a může si jí pedagog upravit podle libosti. Čas potřebný ke zpracování je taktéž orientační, protože může mít pedagog třídu, která zvládne šifru za 30 minut, nebo třídu, která nestihne šifru vyluštit ani za 45 minut.

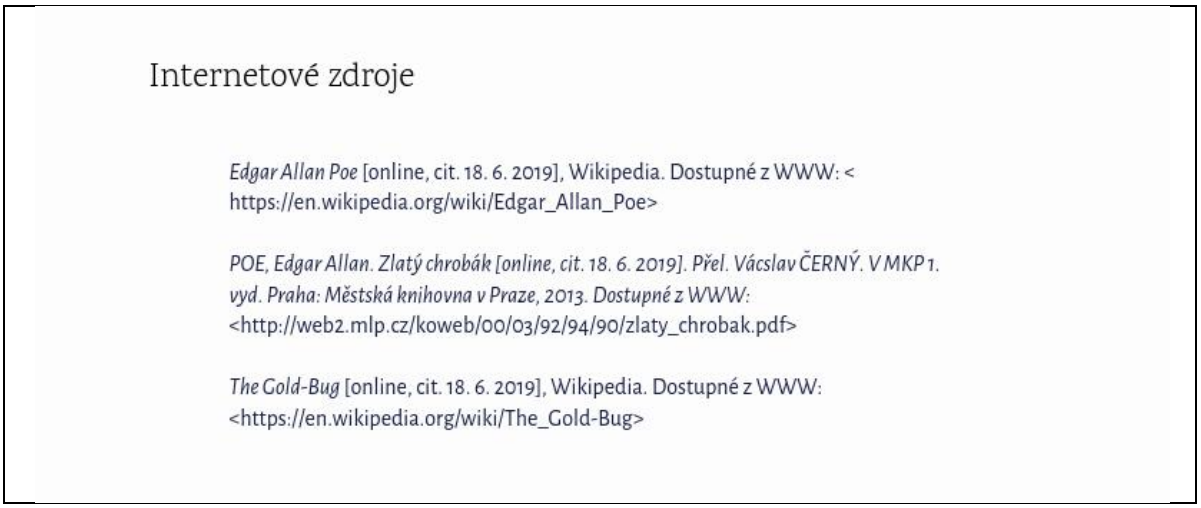


pomůcky:	psací potřeby, v případě vyššího zájmu mobilní telefon
reflexe:	skupinová diskuse nad vypracovanými pracovními listy
klíčové kompetence:	kompetence k učení kompetence sociální a personální kompetence k řešení problému
očekávané výstupy:	žák popíše konkrétní způsob, jak k řešení šifry došel
průřezová témata:	Osobnostní a sociální výchova Výchova k myšlení v evropských a globálních souvislostech Multikulturní výchova

Další položkou jsou pomůcky, kdy žákům stačí pouze psací potřeby a mobilní telefon jen pokud se budou o šifru, či pracovní list, více zajímat. Důležitou věcí je reflexe, kdy učitel diskutuje s žáky o pracovním listu a s žáky si sděluje pozitiva, negativa, dílčí úspěchy, apod. Pracovní list by nesplňoval všechny úlohy, kdyby nerozvíjel klíčové kompetence, které jsou v poznámkách taktéž vypsány. Následují očekávané výstupy, kde je popsáno, co žák zvládne po splnění pracovního listu vysvětlit, nebo popsat. Poslední položkou je seznam průřezových témat, do kterých pracovní list zasahuje a které by si žáci měli osvojovat.

2.2.9 Zdroje

Posledním stranou pracovního listu jsou zdroje. Tuto stránku jsem kvůli lepšímu popisu rozdělil na dvě části. První část obsahuje nadpis „Zdroje“ a podnadpis „Seznam literatury“, který obsahuje knihy, ze kterých jsem čerpal a které mohou být zdrojem dalších informací pro žáky, které šifra zaujme.



Internetové zdroje

Edgar Allan Poe [online, cit. 18. 6. 2019], Wikipedia. Dostupné z WWW: < https://en.wikipedia.org/wiki/Edgar_Allan_Poe>

POE, Edgar Allan. Zlatý chrobák [online, cit. 18. 6. 2019]. Přel. Vácslav ČERNÝ. V MKP 1. vyd. Praha: Městská knihovna v Praze, 2013. Dostupné z WWW: <http://web2.mlp.cz/koweb/00/03/92/94/90/zlaty_chrobak.pdf>

The Gold-Bug [online, cit. 18. 6. 2019], Wikipedia. Dostupné z WWW: <https://en.wikipedia.org/wiki/The_Gold-Bug>

Druhou částí jsou „Internetové zdroje“, kde jsou odkazy na webové stránky, ze kterých jsem čerpal. Na některé z těchto odkazů je možné se dostat skrze výše zmíněné QR kódy. Samotné dílo „Zlatý Brouk“ jsem vybral z dostupných online zdrojů, protože si pak každý se žáků bude moci povídku přečíst, aniž by musel v knihovně čekat na výpůjčku.

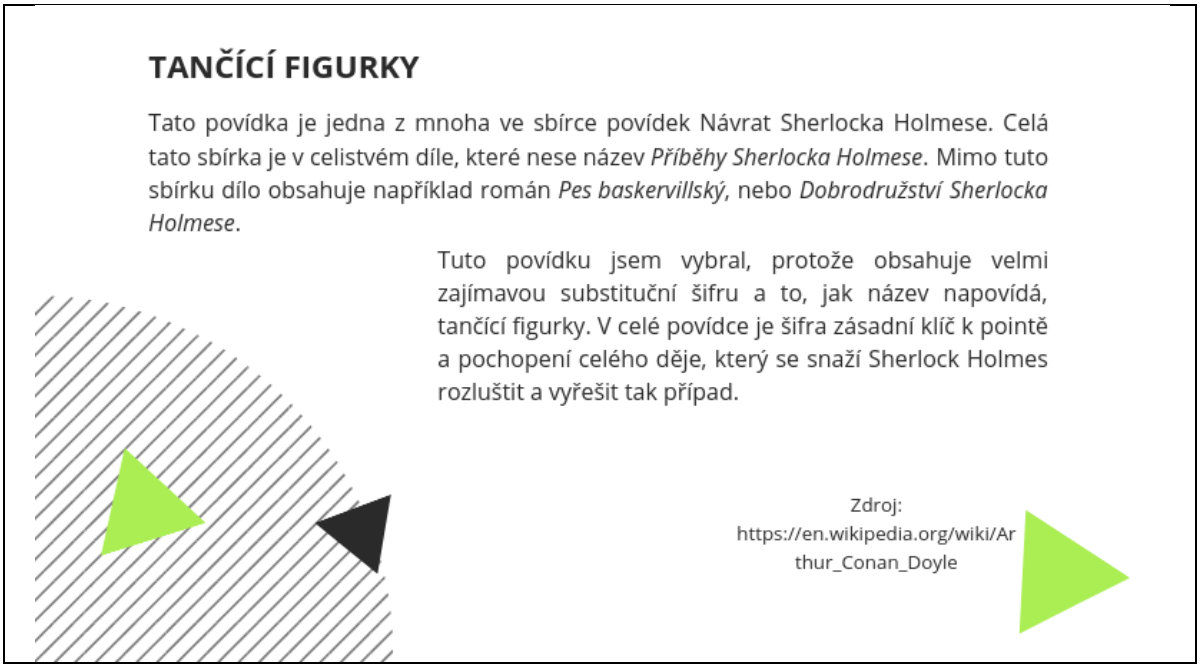
2.3 Pracovní list – 3 „Tančící figurky“

2.3.1 Titulní strana

Titulní strana je jednou z nejdůležitějších stran pracovního listu, jelikož ta rozhodne o tom, zda bude atraktivní, nebo nikoliv. Tato titulní strana pracovního listu „Tančící figurky“ má v sobě hned několik motivů. Avšak nejdříve bych popsal, co strana obsahuje. Stejně jako předchozí pracovní listy, tato strana obsahuje název šifry, potažmo díla a název autora. Tyto informace jsou v horní části stránky, stejně jako označení, že se jedná o pracovní list. Tento text je vsazen do tmavého čtverce, který je spojen se čtvercem druhým, který sděluje obsah pracovního listu. Levý horní roh a dolní pravý roh jsou vyplněny pruhy, které tvoří kruh a mají symbolizovat taneční parket. Avšak co by byl parket bez tanečníků, proto je list doplněn o trojúhelníky zelené a tmavé barvy. Tyto dva prvky se snaží převést název díla do prostoru. Jak jsem již výše zmiňoval pruhy, jež obsahuje pravý dolní roh, tak ty mají i jednu praktickou funkci a to, že pokud zadavatel tiskne pracovní listy, může je lehce roztřídit, jelikož pouze titulní strana obsahuje toto pole s pruhy vpravo dole. Tento pracovní list je navržen tak, aby byl dobře čitelný a barevně nenáročný, jak v černé, tak i v barevné podobě.

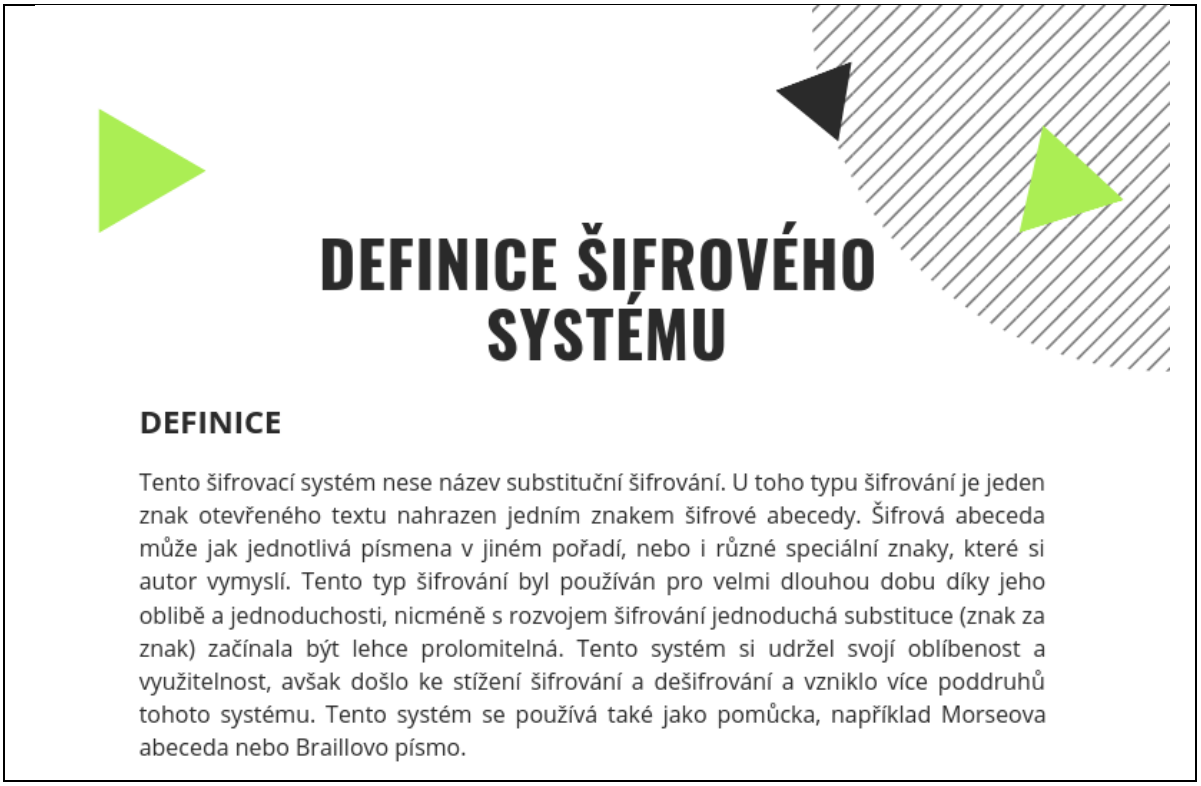
2.3.2 Úvod

Úvodní strana je jedna z nejdůležitějších, dle mého názoru, stran z celého pracovního listu, protože na této stránce najde žák informace, které ho vnesou do života autora a jeho myšlení. Celý úvod je rozdělen na dvě části, na život autora a na dílo, ve kterém je šifra. Život autora je zestručněn, jak jen je to možné, a to z důvodu časové náročnosti celého pracovního listu. První část úvodu obsahuje též autorovu fotografii s uvedeným zdrojem.

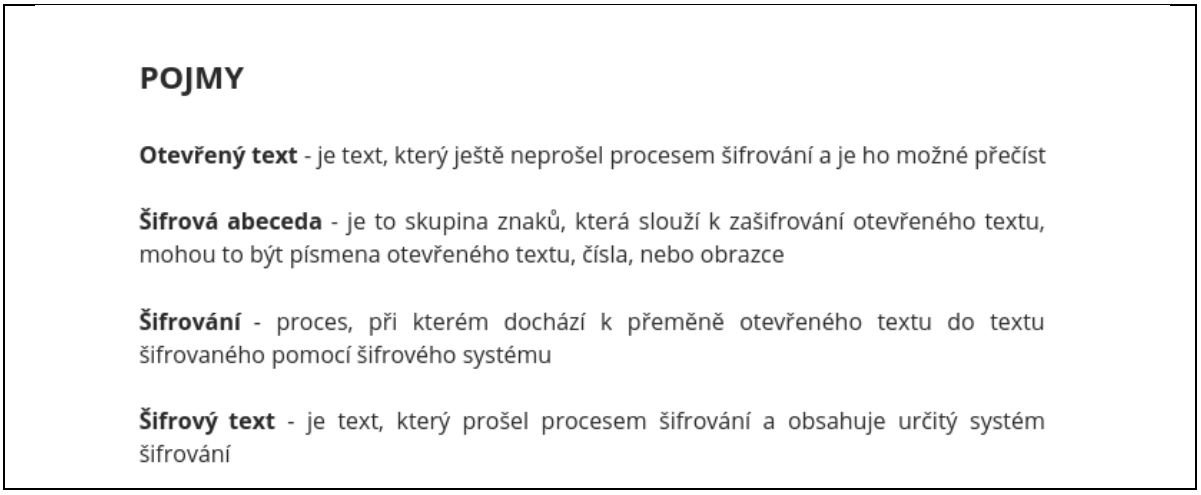


Druhá část úvodu je věnována samotné povídce „Tančící figurky“. Tuto část jsem zahrnul do pracovního listu, protože si myslím, že je důležité, aby tam byla. Jsem toho názoru, že pokud šifra žáka zaujme, může v něm vzbudit zájem buď o samotné šifry, jejich původ, vývoj apod., tak i literaturu celkově. Pro některé žáky může být tato povídka motivací k dalšímu rozvoji v oblasti kryptografie v informatice. Celý úvod je doplněn zdrojem a samozřejmě je doprovázen grafickými doplňky, stejně jako úvodní strana, avšak pruhované pruhy jsou v opačných rozích.

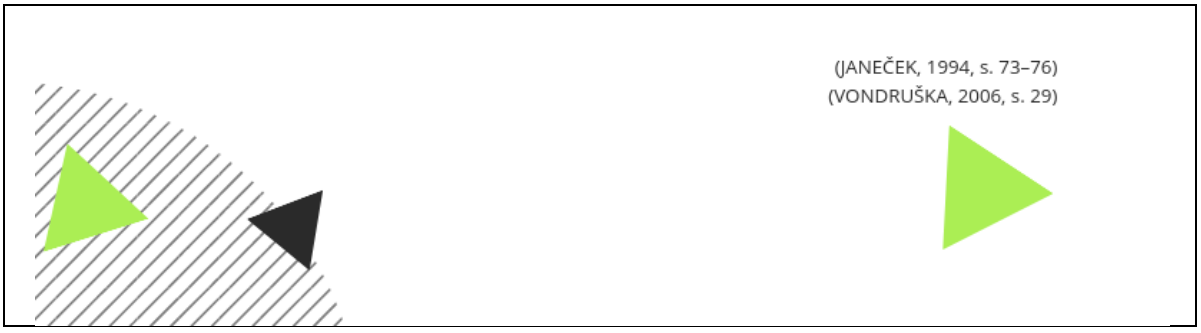
2.3.3 Definice šifrového systému



Často nejméně oblíbená část pracovních listů, nudná a pro některé zbytečná teorie. Nemůžu než souhlasit, avšak pokoušel jsem se napsat definici tak, aby byla lehce pochopitelná a aby se v ní žáci neztráceli. Proto jsem zvolil kratší variantu, kdy definice je jen na několik řádků, ale je v ní v podstatě vše, co žák potřebuje vědět k pochopení, co konkrétní šifrový systém obsahuje. Nicméně abych mohl definici napsat takto krátkou, bylo zapotřebí použít několik slov, kterým by žáci nemuseli rozumět, nebo si je odvodit. Z tohoto důvodu jsem rozdělil tuto stránku na dvě části, kdy první část se věnuje samotné definici a druhá pojmům.



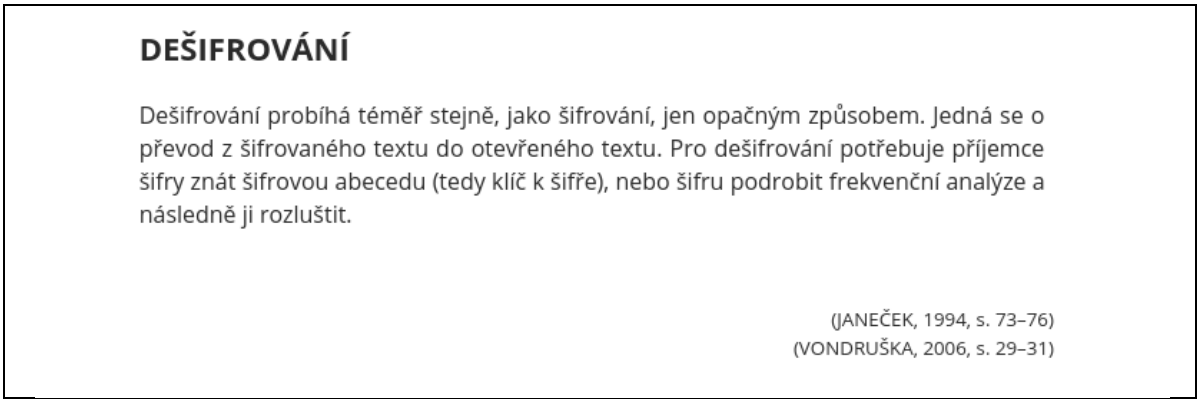
K definicím patří pojmy, což muselo být i zde. Myslím si však, že vysvětlit čtyři pojmy, které jsem se pokusil napsat opět tak, aby byly co nejlépe pochopitelné, nebude mít za následek nepochopení definice, kde jsou pojmy použity. Názvy pojmů jsem pro lepší přehlednost zvýraznil tučně a udělal mezi nimi větší mezeru, aby se žákům, kteří mají nějakou specifickou poruchu učení, dobře četli.



Poslední část této stránky není v hodině tak moc důležitá, ale protože žákům pracovní listy zůstávají (záleží však na učiteli), tak si mohou nějaké informace dohledat v knihách, které jsou zde uvedeny. Jedná se o dvě publikace s tématem kryptografie, které jsou velmi dobře zpracovány a žákům, kteří by projevovali o toto téma zájem, by doplnily informace, které pracovní list postrádá.

2.3.4 Popis šifrování a dešifrování

Popis šifrování a dešifrování - tento list se jeví jako nejdůležitější z celého pracovního listu, avšak pro úspěšné zvládnutí rozluštění šifry je podstatné pochopit definici, proces jakým se šifruje a dešifruje, tak i metody, které následují. Celá stránka je rozdělena na dvě části, ta první nese název šifrování, kde jsem se snažil opět velmi jednoduše vysvětlit proces šifrování. Druhá část nese název dešifrování.



Tato část je velmi podobná předchozí, protože jde v podstatě o obrácený postup. Stejně jako předchozí list, i tato stránka obsahuje odkaz na zdroje, kde si může žák dodatečně dohledat potřebné informace ke konkrétnému šifrovacímu systému a mnohem víc, pokud ho tyto publikace zaujmou.

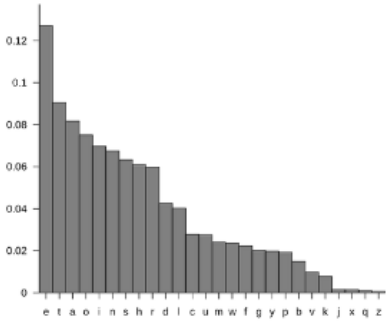
2.3.5 Metody luštění

Metody luštění, tato stránka je, na rozdíl od dvou předchozích, hodně konkrétní, protože vysvětluje postup, jakým se zvolená šifra (substituční) luští. U těchto metod jsem byl trochu limitován prostorem, protože jsem nechtěl na popis využít více stran, jelikož si z vlastní zkušenosti pamatuji na obsáhlé pracovní listy a následné nízké nasazení spolužáků a to je z důvodu, že v pracovním listu bylo mnoho informací. Proto jsem se chtěl poučit a zkusit jinou variantu a to, co nejméně textu. Stránku jsem rozdělil na dvě části.

V té první, která nese název definice je jen velice stručně popsaná metoda frekvenční analýzy.

FREKVENČNÍ ANALÝZA

Základem pro frekvenční analýzu je znát jazyk, kterým je šifra psána. Následně musí sečíst, kolikrát se daný znak v šifře objeví a z tohoto součtu udělat graf četnosti, viz. graf vpravo. Tento graf je pak nutné porovnat s grafem relativní četnosti znaků konkrétního jazyka. Následuje rozluštění nejčastěji se opakujících znaků a určování členů (typické pro angličtinu). Pomocí tohoto postupu získáváme víc a víc písmen, které nám odkrývají další a další, dokud není šifra zcela rozluštěna.



Relativní četnost znaků (angličtina)

Zdroj:
https://en.wikipedia.org/wiki/The_Gold-Bug

Tato metoda má však jednu nevýhodu, je těžce uplatnitelná na krátké texty, kde frekvence znaků nemusí odpovídat grafu.

Tato šifra je poměrně jednoduchá, pro složitější substituce se používají moderní kryptografické programy a různé dešifrovací algoritmy, které šifru rozluští v mžiku.

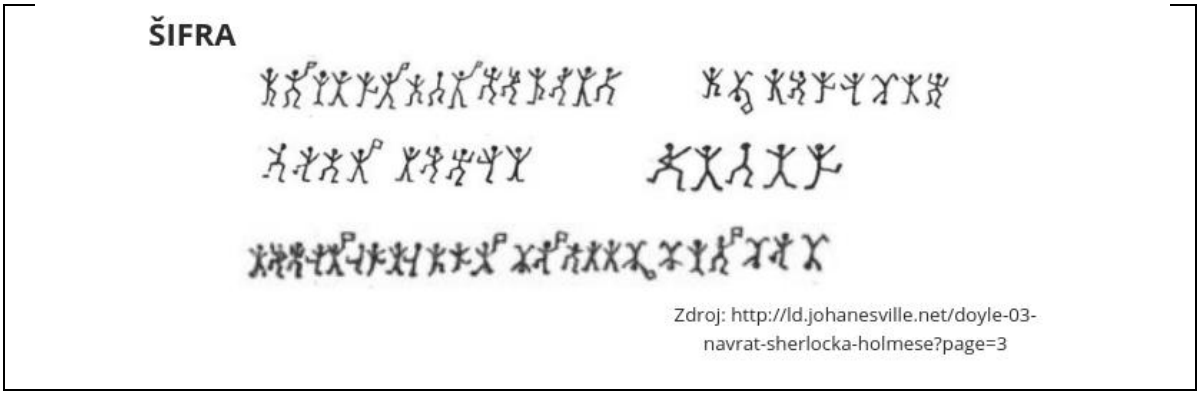
(JANEČEK, 1994, s. 73–76)
(VONDRUŠKA, 2006, s. 29–31)

Nejdůležitější část samotného pracovního listu s názvem frekvenční analýza představuje konkrétní postup, jak přistupovat k samotné šifře, a jak jí rozluštit. I u tohoto popisu jsem se snažil žákům popsat, jak nejlépe a nejrychleji šifru luštit. Nicméně první část popisu je trochu odborná, avšak cílová skupina žáků by si s tím měla poradit buď znalostí pojmů, nebo vlastní intuicí. Také je zde nastíněna nevýhoda této metody a v neposlední řadě také zmíněno možné dešifrování pomocí počítačového software, který je pro toto určen. Tento software jsem schválně do pracovního listu neuváděl, protože jsem to bral jako zbytečnou informaci, když k němu žáci nemají přístup. Nicméně na dotaz, či vyžádání, bych žákům sdělil několik takových programů, nebo společností, které se počítačovou kryptografií zabývají.

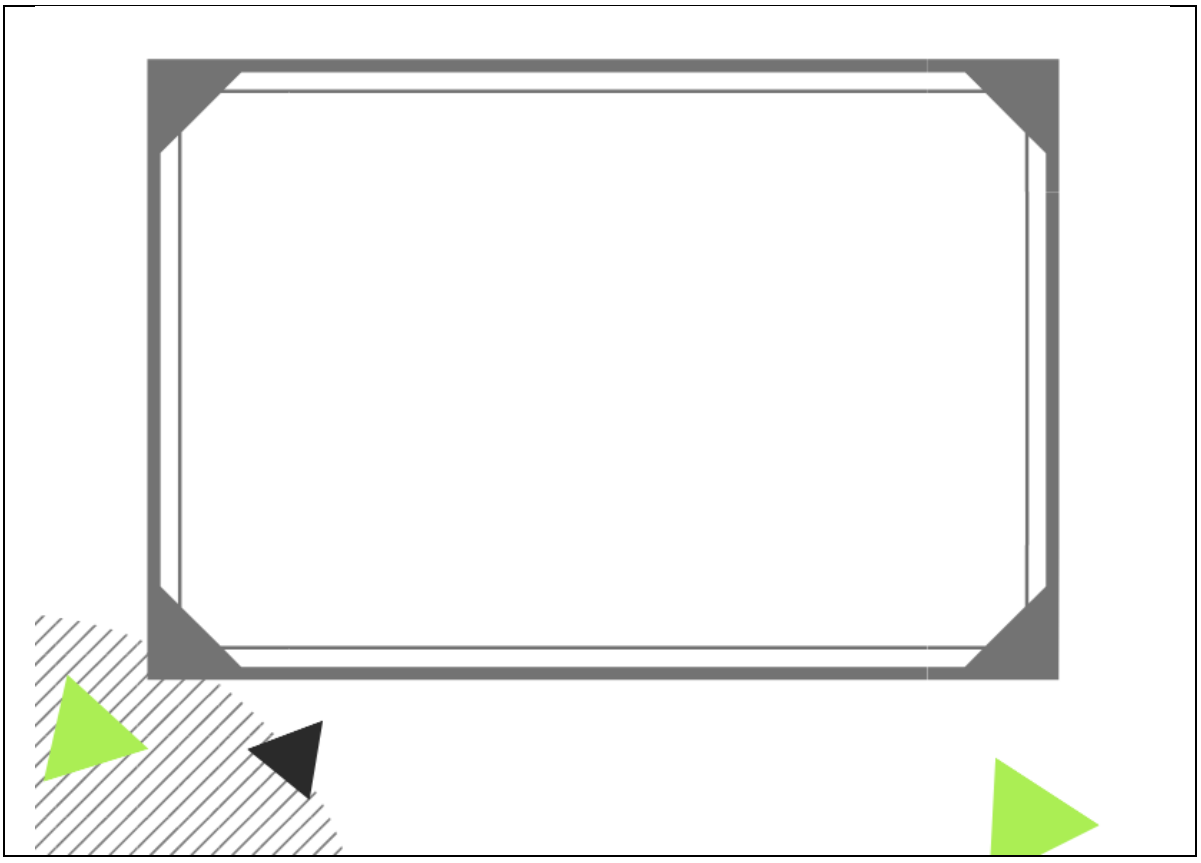
Samotný text by žákům příliš nepomohl a jen velmi stěží by si dokázali podle popisu představit, jak šifru luštit, proto jsem k textu připojil graf relativní četnosti znaků anglického jazyka, ve kterém je šifra napsána. Tento graf by měl žákům pomoci rozluštit první písmena šifry a čistou dedukcí a znalostí základů anglického jazyka doplnit písmena zbylá. Jako předchozí strana, tak i tato obsahuje odkaz na literaturu, ze které jsem čerpal a která může být pro žáky hodnotným zdrojem informací.

2.3.6 Zadání pracovního listu

Zadání pracovního listu - pro většinu žáků asi po těch všech předchozích listech konečně to, na co se připravují. Tento list je opět rozdělen na několik částí. První částí je nadpis, který však již není tak atraktivní, jako když ho žáci uvidí poprvé, avšak hned následuje část se šifrou.



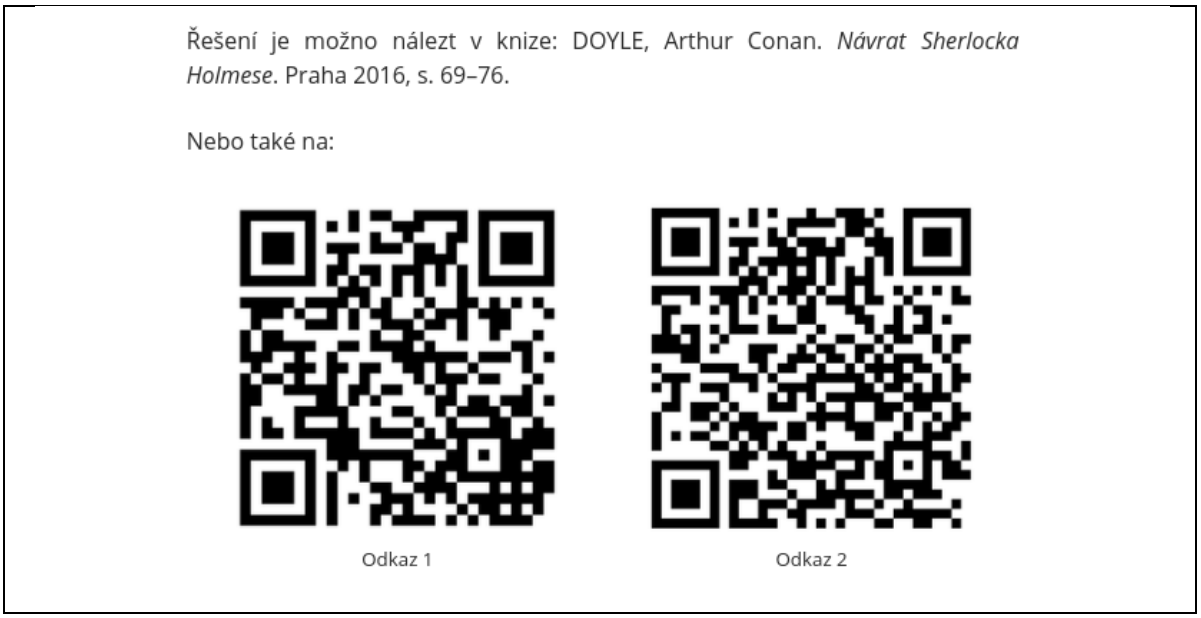
Část s označením šifra už podle názvu obsahuje text, který je zašifrován a který mají žáci rozluštit. V tomto případě se jedná o tančící figurky, které jsou v různých pozicích, a každá pozice znázorňuje jednu pozici. Tento pracovní list je v pořadí jako třetí a není to náhoda. Mnohem lépe se luští znaky, jež člověk zná, nebo které jsou lehce rozeznatelné. Tato šifra patří mezi substituční šifry, ale svojí prezentací vypadá velmi složitě, až nerozluštitelně. Tyto obrázky můžeme nalézt v knize, nebo na uvedeném zdroji, avšak v některých online zdrojích jsou nahrazeny tečkami, čárkami, či jinými písmeny.



Další část strany je volné pole pro řešení šifry, kde mají žáci prostor pro svoje pokusy o dešifrování šifry. Toto pole jsem označil šedým zdobeným obdélníkem, který má zachovat design celého pracovního listu. Na této straně je pouze malým obdélníkem, avšak zadání pracovního listu pokračuje ještě jednou stranou (viz. Příloha A03), kde je tento obdélník téměř přes celou stranu.

2.3.7 Řešení

Oproti předchozím pracovním listům, kde je přímo napsané řešení, jsem zvolil trochu jinou možnost. Jsem toho názoru, že když si žáci sami přečtou část knihy, kde je postup řešení popsán, bude to pro ně mnohem přínosnější, protože si budou muset najít řešení v textu. V tomto vidím především pozitivum této formy řešení. Samotná stránka řešení je rozdělena na dvě pomyslné části, kde v první části vysvětluji, proč jsem zvolil možnost odkazu na knihu a nenapsal přímo řešení.



V této části jsem jako odkaz použil citaci na knihu, kde lze šifru najít a s ní i samotné řešení. Při tvorbě pracovního listu jsem nepředpokládal, že by žáci u sebe měli

tuto knihu a ještě ve větším počtu, tak jsem zvolil odkaz pomocí QR kódu (https://www.qrgenerator.cz/), který lze lehce na zmíněném webu vygenerovat. Žáci mohou lehce pomocí čtečky QR kódu a mobilních dat získat přístup k řešení a nemusí ho nikde složitě hledat. Právě v moderních technologiích je dle mého názoru budoucnost a škola by s nimi měla jít ruku v ruce.

2.3.8 Metodické poznámky

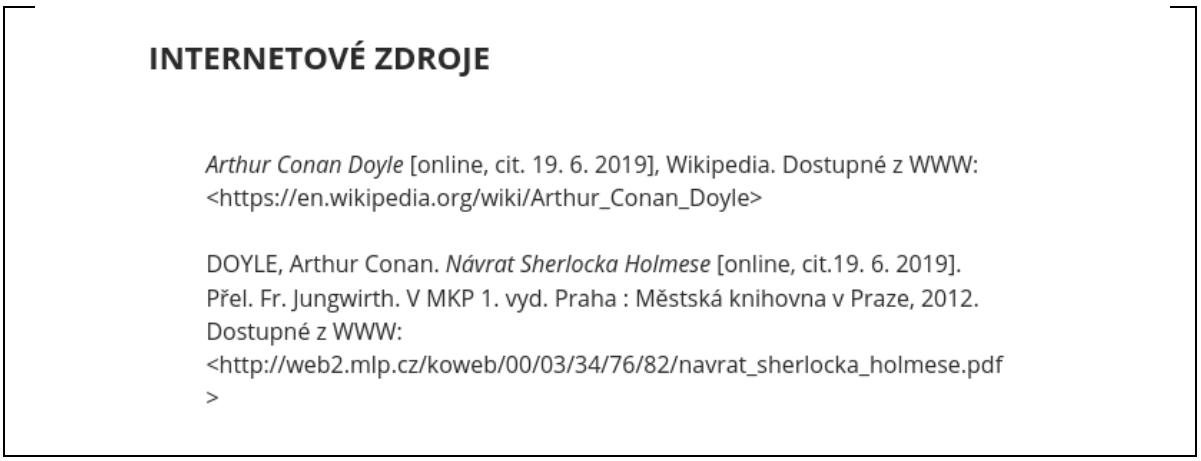
Metodické poznámky jsou pro učitele nejdůležitější věc z celého pracovního listu. Tuto stránku jsem rozdělil na dvě části a to z důvodu lepší přehlednosti popisu. Nejvíce stěžejní část je cíl. Cíl musí být stanoven vždy, protože bez něj pracovní list postrádá význam. Po cíli následuje věková skupina, konkrétně žáků, pro kterou je daný pracovní list určen. Věkové rozmezí je taktéž velmi důležité, protože pro žáky nad rozmezí by byl pracovní list příliš jednoduchý a minul by se účinkem, pro mladší by byl naopak velmi těžký, až nesplnitelný. Následuje organizace činnosti, kde je dle mého názoru, vhodné uplatnit skupinovou práci, nicméně organizace činnosti je jen doporučení autora pracovního listu a není povinná. Tato část se může upravit dle libosti a možností cílové skupiny žáků. Čas potřebný ke zpracování je též doporučený, žáci by měli stihnout vyřešit šifru v daný čas, avšak záleží na konkrétní třídě, čas může být upraven dle potřeby.

pomůcky:	psací potřeby, mobilní telefon
reflexe:	skupinová diskuse nad vypracovanými pracovními listy
klíčové kompetence:	kompetence k učení kompetence sociální a personální kompetence k řešení problému
očekávané výstupy:	žák popíše konkrétní způsob, jak k řešení šifry došel
průřezová témata:	Osobnostní a sociální výchova Výchova k myšlení v evropských a globálních souvislostech Multikulturní výchova

Nedílnou součástí metodických poznámek jsou pomůcky. Tento pracovní list zahrnuje do pomůcek, kromě psacích potřeb, i mobilní telefon a to z důvodu ověření řešení. Nicméně není nutný, jelikož dalším bodem poznámek je reflexe, která slouží ke shrnutí a diskusi celého pracovního listu, tedy i k diskusi nad řešením. Nezbytnou součástí je taktéž výpis klíčových kompetencí, které jsou u žáků rozvíjeny a které jsou ve vzdělávání stěžejní. Další položkou jsou očekávané výstupy, ve kterých je popsáno, co by měl žák na konci hodiny, po práci s pracovním listem, zvládnout. Poslední položkou je seznam průřezových témat, do kterých pracovní list zasahuje a které by si žáci měli osvojovat.

2.3.9 Zdroje

Na závěr pracovního listu patří zdroje. Já jsem používal zdroje průběžně v pracovním listu, avšak teprve na tomto listě je možné najít konkrétní název díla, rok vydání apod., nebo odkaz na webovou stránku. Zdroje jsem rozdělil na dvě části a to z praktických důvodů. První část obsahuje seznam literatury a to konkrétně knižní vydání. Druhá část, která nese jméno internetové zdroje, odkazuje na online zdroje, které byly v práci využity.



3 Empirická část

Empirická část je věnována kvalitativnímu výzkumnému šetření problematiky začlenění literárních a klasických šifer do informatické výuky pomocí případové studie a dotazníkového šetření a jejich analýze a vyhodnocení.

3.1 Kvalitativní výzkum

„*Kvalitativní výzkum je proces hledání porozumění založen)" na různých metodologických tradicích zkoumání daného sociálního nebo lidského problému. Výzkumník vytváří komplexní, holistický obraz, analyzuje různé typy textů, informuje o názorech účastníků výzkumu a provádí zkoumání v přirozených podmínkách*.“ (Hendl, 2005, s. 50)

Kvalitativním výzkumem se také zabývá Jan Hendl, který ve své publikaci *Kvalitativní výzkum: základní metody a aplikace* vydané v roce 2005, v níž uvedl:

„*Někteří metodologové chápou kvalitativní výzkum jako pouhý doplněk tradičních kvantitativních výzkumných strategií, jiní zase jako protipól nebo vyhraněnou výzkumnou pozici ve vztahu k jednotné, na přírodovědných základech postavené vědě. Postupně získal kvalitativní výzkum v sociálních vědách rovnocenné postavení s ostatními formami výzkumu.*

Neexistuje jediný obecně uznávaný způsob jak vymezit nebo dělat kvalitativní výzkum.“

Kvalitativní výzkum jsem si vybral, protože pro cíle mé práce je vhodnější zabývat se konkrétními případy, než statistickým, tedy kvantitativním šetřením. Tento výzkum se skládá z případové studie, která je zaměřena na využití klasických a literárních šifer v informatické výuce pomocí pracovních listů. Výzkum dále obsahuje dotazníkové šetření, které spolu s případovou studií pomůže zodpovědět výzkumné otázky a vyhodnotit stanovené hypotézy.

3.1.1 Cíl výzkumu

Cílem výzkumu je ověřit jeden z vytvořených pracovních listů ve výuce a zhodnotit tuto výuku formou kvalitativního výzkumu sestávajícího z případové studie popisující výuku s využitím zvoleného pracovního listu a z dotazníkového šetření, ve kterém žáci

odpovědí na několik otevřených otázek vztahujících se k posouzení atraktivity, názornosti a srozumitelnosti výuky a k jejímu přínosu pro osobní rozvoj respondentů.

3.1.2 Formulace výzkumných otázek a hypotéz

Pro splnění cílů tohoto výzkumu je nutné stanovit výzkumné otázky a k nim hypotézy. Pro správné stanovení hypotézy uvádí Chráska (2006, s. 10) tuto definici:

„*Hypotéza je tvrzení, které je vyjádřeno oznamovací větou.*

Hypotéza musí vyjadřovat vztah mezi dvěma proměnnými (pokud se nejedná o vyjádření vztahů, není možno hovořit o hypotéze). Proto musí být hypotéza vždy formulována jako tvrzení o rozdílech, vztazích nebo následcích.

Hypotézu musí být možno empiricky ověřovat. Proměnné, které v hypotéze vystupují, musí být měřitelné (byť jen na základě kategorizace).“

Po zvážení cílů diplomové práce jsem se rozhodl stanovit následující výzkumné otázky:

Otázka č. 1 - Je výuka s pracovním listem pro žáky atraktivní?

Otázka č. 2 - Je výuka s pracovním listem pro žáky názorná?

Otázka č. 3 - Je výuka s pracovním listem pro žáky srozumitelná?

Otázka č. 4 - Je výuka s pracovním listem pro žáky přínosná s hlediska osobního rozvoje?

A následující hypotézy:

Hypotéza č. 1 - Výuka s pracovním listem bude pro žáky spíše atraktivní, než neatraktivní.

Hypotéza č. 2 - Výuka s pracovním listem bude pro žáky názorná, než nenázorná.

Hypotéza č. 3 - Výuka s pracovním listem bude pro žáky spíše srozumitelná, než nesrozumitelná.

Hypotéza č. 4 - Výuka s pracovním listem bude pro žáky spíše přínosná pro osobní rozvoj, než nepřínosná.

3.1.3 Metodologie

Pro potřeby tohoto výzkumu je nutné si stanovit, v rámci metodologie, výzkumné metody. První metodou je analýza, pomocí níž je možné získat data z dotazníkového šetření. Dále je možné tuto metodu využít při případové studii i v rámci analyzování průběhu vyučovací hodiny. Analýzu popisuje například tato definice:

„*Analýza spočívá v rozdělení celku na jeho komponenty a zkoumání, jak tyto komponenty fungují jako relativně samostatné prvky a jaké jsou mezi nimi vztahy. Každá analýza se vyznačuje určitým stupněm explorace. Znamená to, že při ní provádíme průzkumové a objevující aktivity.*“ (Hendl, 2005, s. 35)

Další metodou je případová studie, kterou jsem vybral vzhledem k jejímu praktickému využití. Případovou studií se zabývá hned několik autorů. Velmi podrobně se jí zabývá Hendl (2005, s. 104), který jí popisuje následujícím způsobem:

„V případové studii jde o detailní studium jednoho případu nebo několika málo případů. Zatímco ve statistickém šetření shromažďujeme relativně omezené množství dat od mnoha jedinců (nebo případů), v případové studii sbíráme velké množství dat od jednoho nebo několika málo jedinců. V případové studii jde o zachycení složitosti případu, o popis vztahů v jejich celistvosti. Případová studie v sociálněvědním výzkumu je podobná mikroskopu: její hodnota závisí na tom, jak dobře je zaostřená. Předpokládá se, že důkladným prozkoumáním jednoho případu lépe porozumíme jiným podobným případům. Na konci studie se zkoumaný případ vřazuje do širších souvislostí. Může se srovnat s jinými případy, provádí se také posouzení validity výsledků.“

3.1.4 Charakteristika místa šetření

Šetření proběhlo na Gymnáziu Boženy Němcové v Hradci Králové. Toto gymnázium je šestileté, tudíž je zde pouze jeden typ studia. Gymnázium se zaměřuje na matematiku, český jazyk a cizí jazyky. Samotné šetření proběhlo 25. 6. 2019 a to hned ve dvou třídách (8:00 - 9:40) a ve dvou různých učebnách. První učebna měla klasické uspořádání, kde byla rovná podlaha a lavice uspořádány za sebou s uličkami mezi nimi. Ve druhé bylo uspořádání naprosto odlišné, protože třída byla stupňovitá a katedra učitele byla od žákovských míst vzdálená. V prvním případě se jednalo o učebnu dějepisu, v tom druhém (zcela výjimečně) o učebnu fyziky.

3.1.5 Charakteristika výzkumného vzorku

Do zkoumaného vzorku spadají žáci dvou tříd šestiletého gymnázia, druhého ročníku. Jedná se o žáky tříd 2. B a 2. C. Do těchto tříd chodí celkem 57 žáků, přičemž 18 z nich bylo na různých školních soutěžích, aktivitách, nebo nebylo přítomno z jiných důvodů. Genderově byly třídy poměrně vyvážené, lehce převažovaly dívky nad chlapci.

3.2 Zpracování získaných dat

Výzkum obsahuje vypracovanou případovou studii, která je zásadní pro zodpovězení výzkumných otázek a stanovených hypotéz.

Dále bylo pro výzkum žáky vypracováno 39 kvalitativních dotazníků, přičemž z první třídy jich bylo 22 a z druhé 17. Tyto dotazníky byly reakcí na vyučovací hodinu, ve které žáci vypracovávali pracovní list (jedná se o tutéž hodinu). Dotazník obsahoval 7 hlavních otázek a 4 podotázky, na které měli žáci odpovídat. Otázky byly otevřené a celé šetření bylo zcela anonymní.

3.2.1 Případová studie

Objektem případové studie je využití klasických a literárních šifer v informatické výuce. Cílem je zjistit, zda pracovní listy, které obsahují zpracované literární nebo historické šifry, jsou pro žáky atraktivní, názorné, srozumitelné, přínosné pro další jejich rozvoj a jak na ně budou reagovat.

Celá studie proběhla dne 25. 6. 2019 v Hradci Králové, kdy jsem navštívil jednoho fakultního učitele na Gymnáziu Boženy Němcové. S panem fakultním učitelem jsme už v minulosti učili v tandemu dějepis, tak jsme tuto možnost využili znovu. Jelikož jsme se dohodli, že uděláme žákům překvapení, tak hned první hodinu jsme šli spolu do třídy, ale já jsem zůstal na chodbě a pan učitel žákům řekl, že na chodbě čeká překvapení. Následně jsem přišel do třídy na jeho vyzvání a žáci byli naprosto zaskočení, protože jsem dodržel svůj slib a přišel jsem se na ně ještě jednou podívat. Byla to totiž stejná třída, kterou jsem předtím učil. Žákům jsme řekli, co se bude dít a postupně si začali chodit pro pracovní listy, které dostávali do dvojic, protože se jednalo o skupinovou práci. Žáci byli z počátku udivení z množství stránek pracovního listu, avšak potom, co jsem je ubezpečil, že se jedná o jeden pracovní list, jejich udivení opadlo. Posléze jsem žákům vysvětlil, co mají dělat a ať se pustí do práce. Ihned po tomto zadání jejich práce jsme začali chodit s panem

fakultním učitelem po třídě, každý jiným směrem. Sledovali jsme, jak žáci postupují. Atmosféra ve třídě byla velmi uvolněná, jelikož se jednalo o jejich poslední hodinu daného předmětu tento školní rok. Někteří žáci nás požádali, zda by bylo možné pustit ve výuce hudbu, načež jsme se zeptali celé třídy, zda s tím souhlasí, nebo ne. V rámci zachování spravedlnosti jsme se rozhodli pro hlasování, ve kterém si třída odhlasovala, že hudbu pustit chce. Iniciátoři vybrali konkrétní hudbu, kterou jsme s fakultním učitelem posoudili, schválili a pustili. Poté, co jsme hudbu pustili, zpozoroval jsem u žáků větší zapojení, avšak zvýšil se i ruch ve třídě, který však nepřekračoval hranici rušivého chování při práci ve skupině. Průběžně jsem chodil třídou a ptal se všech dvojic, jak pokračují, jestli je jim všechno jasné. Přibližně polovina žáků pochopila způsob šifrování a zadání práce. Začala tedy šifru správným způsobem dešifrovávat. Někteří žáci nepochopili z pracovního listu, co se má konkrétně dělat, a hlásili se. Zbylí žáci potichu seděli a snažili se přijít na postup, jak šifru vyřešit. Já jsem po třídě chodil a snažil se žákům poradit, jak mají postupovat, aby se jim podařilo šifru alespoň částečně vyřešit. Mezitím jsem žákům rozdal dotazníky, které jsem jim dal na okraj lavice. Řekl jsem, jim, že ty budou vyplňovat až na konci hodiny. Ve třídě se držela stále velmi uvolněná atmosféra a žáci intenzivně pracovali na rozluštění šifer. I v tento moment se ve třídě našli žáci, kterým se nepodařilo pochopit systém, jak šifru luštit a byla nutná moje asistence, aby drželi krok s ostatními. Nicméně s tímto problémem jsem již na začátku počítal, nejedná se o nic neobvyklého. Celých 30 minut jsem žákům dával tipy, jak co nejrychleji luštit šifru a jak k ní přistupovat. Atmosféra ve třídě byla stále velmi uvolněná, i když věděli, že za to nebudou mít žádnou známku. Objevil se však jeden rušivý element a to bylo teplo. I když bylo mezi 8 a 9 hodinou, tak venkovní teplota rostla. Tomuto nebylo jak zabránit, jelikož otevření oken do rušné ulice bylo nežádoucí. Žáci pracovali zodpovědně a uvolněně, nebyl na nich vidět žádný stres. Po uplynutí 30 minut jsem žáky požádal, zda by mohli během 10 minut vyplnit dotazníky, které jsem jim předtím rozdal. Žáci v tento moment nevypadali nadšeně, protože se chtěli dál věnovat luštění šifry a já je tím od toho odtrhával. Následně tedy vyplnili dotazníky, kdy jsem se žáků ptal, zda všemu rozumějí a všichni do jednoho kývali, že ano. Po napsání dotazníku jsem s žáky diskutoval, jak se jim dařilo šifru luštit, v čem byla tato hodina jiná, co by chtěli udělat jinak, apod. Po této diskusi jsem žákům popřál, ať se jim daří jak ve škole, tak v osobním životě a poděkoval, že jsem měl příležitost je učit. V reakci na moje přání žáci vstali a začali tleskat.

K získání více dat k objektu případové studie, dohodl jsem se s fakultním učitelem, že provedeme totéž šetření u paralelní třídy hned následující hodinu. Počátek hodiny byl velmi podobný, jako v předchozí hodině, avšak tentokrát jsem byl ve třídě první já a pan učitel žáky teprve přivedl. Tato třída byla stupňovitá s katedrou velmi vzdálenou od žáků. Fakultní učitel mi řekl, že chce dát žákům na rozloučenou nanuky, tudíž se pravděpodobně nějakou dobu zdrží. Přibližně po deseti minutách začali přicházet žáci, kteří byli na první pohled, překvapení mojí přítomností. Atmosféra ve třídě byla velmi uvolněná a klidná, až na horko. Během toho, co žáci jedli nanuky, jsem jim do dvojic rozdal pracovní listy a řekl jim instrukce k pracovnímu listu. Následně se žáci pustili do práce. Na žádost žáků jsme pustili hudbu, kterou jsme, jako minulou hodinu, nejdříve posoudili a schválili. Někteří žáci se hlásili o radu, protože ani po mém vysvětlení jim nebylo jasné, co mají přesně dělat. V takových případech jsem jim individuálně vysvětlil postup a navedl je správným směrem. Po tomto dovysvětlení již mohli všichni žáci pracovat na dešifrování. Když jsem během jejich skupinové práce procházel třídu, byl jsem mile překvapen, že se všichni žáci věnovali pracovním listům s plným nasazením. Vzhledem k tomu, že hodina byla zkrácena, rozdal jsem žákům dotazníky a požádal je o jejich rychlé vyplnění. Přerušení jejich skupinové práce bylo nutné z důvodu časového deficitu. U žáků jsem zaznamenal zklamání, že nemohou dešifrování dokončit. Z čehož usuzuji, že je práce s pracovními listy bavila. Po vyplnění dotazníků jsme s žáky diskutovali, jak se jim hodina líbila, zda by chtěli více takových hodin a zda je tento pracovní list oslovil. Na úplný závěr hodiny jsem se s žáky rozloučil a popřál jim hodně úspěchů při studia a v osobním životě. Žáci na to reagovali hlasitým potleskem, u kterého dokonce vstávali ze svých lavic. Sběr dat případové studie skončil celkovou reflexí s fakultním učitelem.

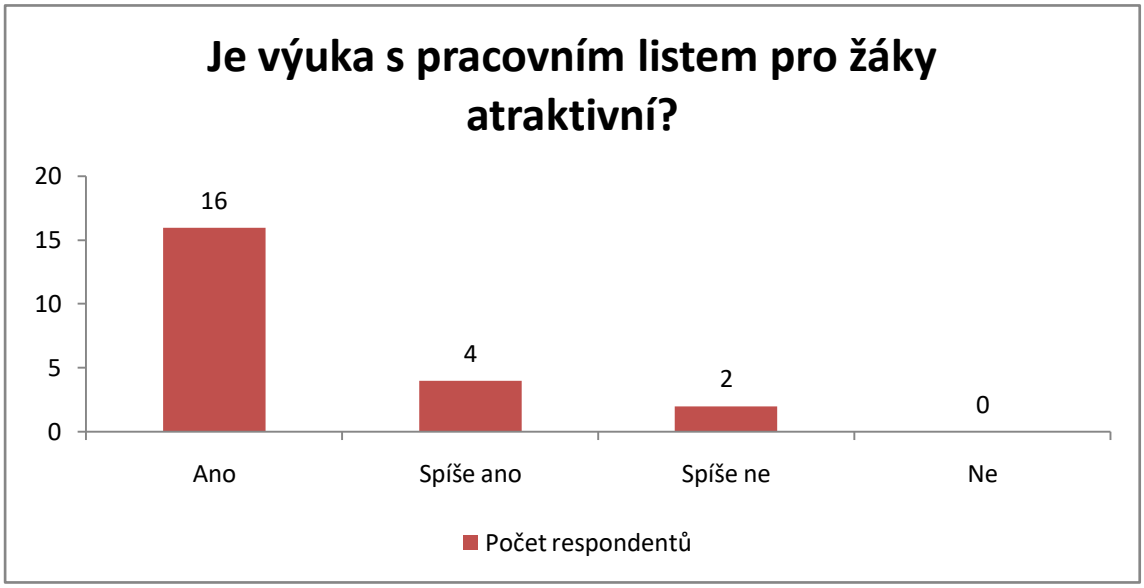
3.2.2 Analýza získaných dat prvního dotazníkového šetření

Při svém výzkumu jsem oslovil 22 žáků ze třídy 2. B, všichni oslovení se anonymního dotazníkového šetření zúčastnili. Dotazník se skládal ze 7 hlavních otevřených otázek a 4 otevřených podotázek. První až čtvrtá hlavní otázka a s nimi dvě podotázky byly zaměřeny na atraktivitu hodiny a pracovního listu. Další otázka byla věnována názornosti výuky. Šestá otázka se zaměřovala na srozumitelnost. Poslední otázka se týkala osobního přínosu a rozvoje pro žáky. Dotazníky byly vyplněny převážně dvojím způsobem, buď strohé odpovědi, nebo se žáci rozepsali i do několika souvětí. Většina žáků odpověděla na všechny otázky, pouze jeden žák nezodpověděl jednu otázku, konkrétně otázku, která se týkala srozumitelnosti. Při analýze jednotlivých odpovědí dotazníkového

šetření jsem vyhodnotil odpovědi podle jejich kladných, nebo záporných znění. V některých odpovědích se vyskytla i konstruktivní kritika, která byla na místě. Díky této kritice jsem zjistil, že pracovní list měl několik chyb.

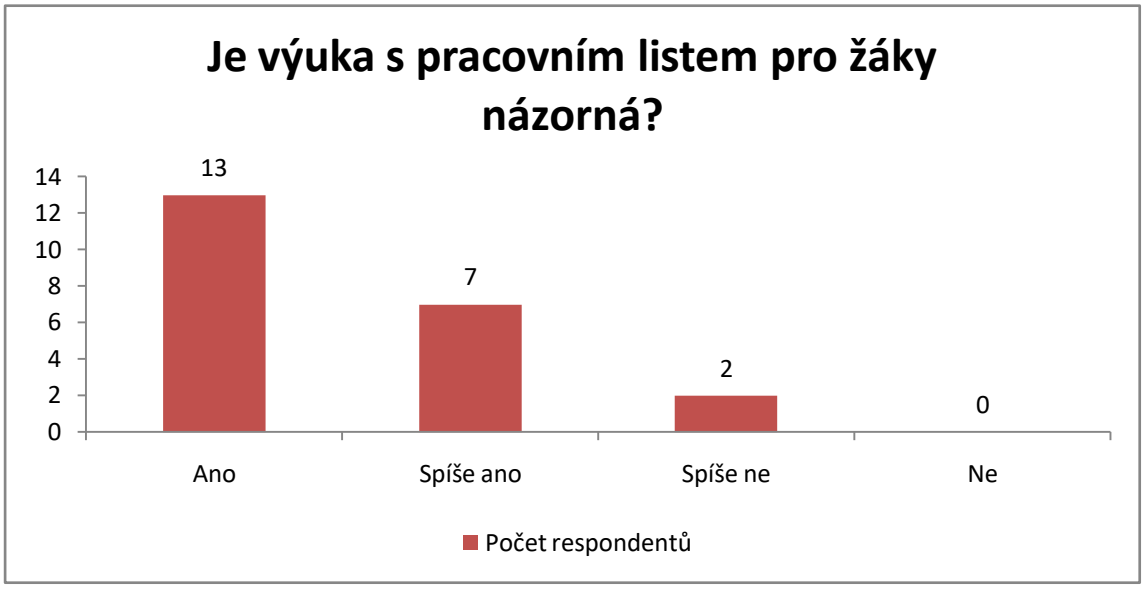
V následující části jsem v MS Excel vypracoval grafy, které se týkají výzkumných otázek a jsou podloženy dotazníkovým šetřením.

Graf č. 1 Je výuka s pracovním listem pro žáky atraktivní? (Vzorek 1)



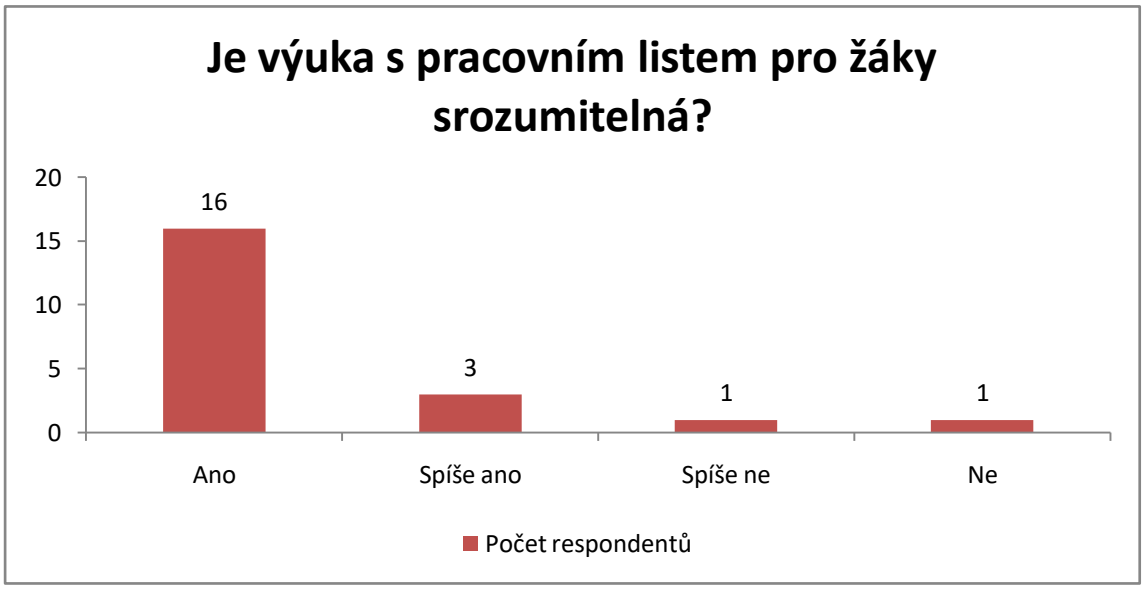
Z následujícího grafu vyplývá, že pro většinu žáků byla hodina atraktivní. Z odpovědí 16 žáků jsem usoudil, že "Ano". U žáků, u kterých jsem si nebyl jistý jednoznačně pozitivním postojem, jsem zvolil možnost druhou, tzn. pro "Spíše ano" byly 4 žáci. Avšak ne všechny odpovědi byly pozitivní, za což sem rád. Dva respondenty jsem zařadil do "Spíše ne", jelikož jejich odpovědi byli lehce negativní, avšak nebyly úplně. Ve třídě nebyl žák, který by ohodnotil atraktivitu vyloženě negativně.

Graf č. 2 Je výuka s pracovním listem pro žáky názorná? (Vzorek 1)



Z následujícího grafu je patrné, že větší část žáků byla pro "Ano", avšak už to není tak jednoznačné. Podle jednotlivých odpovědí usuzuji, že pracovní list, včetně vyučovací hodiny, nebyl tak názorný, jak byl atraktivní. Zcela pozitivně odpovědělo 13 žáků, oproti tomu žáci, jejichž odpověď byla pozitivní, avšak ne zcela, bylo 7. Žáci, kteří byli spíše negativní, byli 2. Zcela negativní nebyl žádný ze žáků.

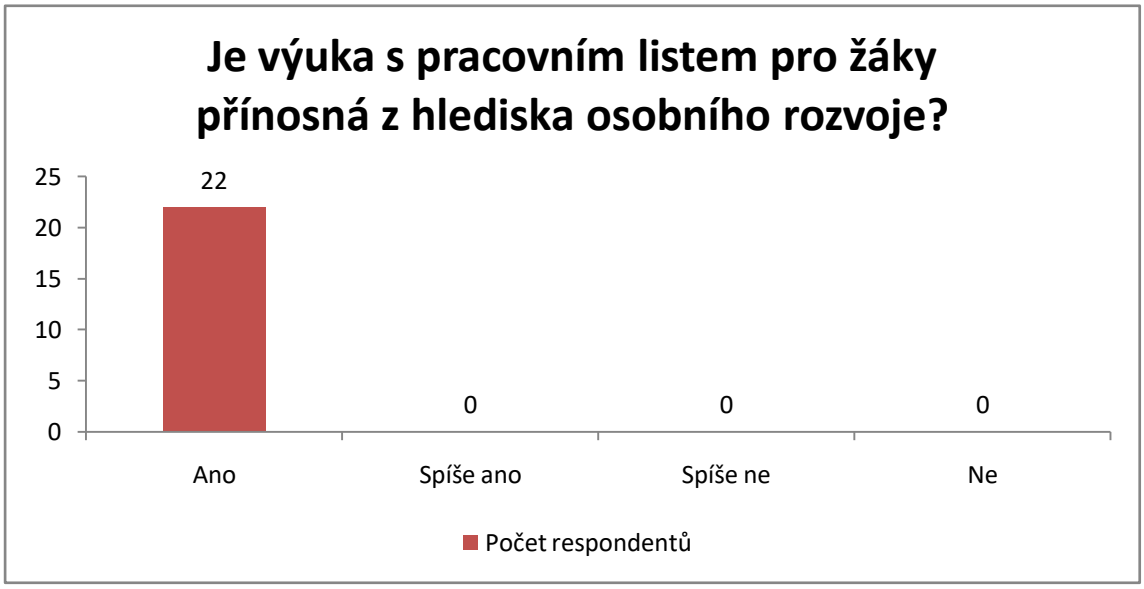
Graf č. 3 Je výuka s pracovním listem pro žáky srozumitelná? (Vzorek 1)



Z výše doloženého grafu je patrné, že pro většinu žáků byla výuka s pracovním listem srozumitelná, avšak už zde se objevuje první, čistě negativní zpětná vazba. Zcela pozitivně se vyjádřilo celkem 16 žáků. Žáci, kteří odpověděli stále pozitivně, nicméně

nebylo to jasné "Ano", byl celkový počet 3. Jeden žák odpověděl lehce negativně a jeden žák zcela negativně.

Graf č. 4 Je výuka s pracovním listem pro žáky přínosná z hlediska osobního rozvoje? (Vzorek 1)



Na tuto otázku odpověděli všichni žáci a byl jsem velmi překvapen, že všechny ohlasy byly zcela pozitivní. Někteří žáci psali čistě "Ano" nebo se více rozepsali a jejich odpovědi byly pozitivní, ani u jedné odpovědi jsem neshledal zaváhání.

Z tohoto vzorku bych chtěl taktéž zařadit několik odpovědí, které jsou velmi přínosné pro tento výzkum. U první otázky, která se zabývala hodnocením pracovního listu z hlediska atraktivity, dva žáci napsali podnětnou odpověď. V jedné z nich žák sdělil: „*Byl zajímavý a originální, ale rozluštit šifru bylo těžké, některé znaky nebyly moc vidět.*“. Další žák poznamenal, že by bylo potřeba více času k vyřešení šifry.

Na druhou otázku ve znění: „*Co vás na pracovním listu z grafické stránky nejvíce zaujalo?*“, odpověděl jeden žák kresbou hlavního motivu pracovního listu.

Třetí otázka se soustředila na to, co žákům na pracovním listu chybí. Převážná část odpovědí byla stejná a odpověď zněla „*Nic*“. Šest odpovědí od žáků se lišilo. Jeden z žáků uvedl: „*Možná by bylo lepší nabídnout vypracovávatelům více možností řešení (pokud tedy nějaké jiné jsou).*“. K tomuto se přikláněl i další žák. Další dva žáci se svou odpovědí shodují, že v pracovním listu chybí „*pořádné vysvětlení konkrétního úkolu*“. Zbylým dvěma žákům chybí v pracovním listu „*kvalitní zpracování panáčků*“ - lepší kvalita "Tančících figurek".

První podotázka souvisí s třetí otázkou a zabývá se tím, co v pracovním listu přebývá. K této otázce se vyjádřili odlišně jen čtyři žáci, kteří se shodli na tom, že v pracovním listu přebývá moc textu a tím pádem moc stránek.

Ve čtvrté otázce, týkající se atraktivity hodiny pro žáky, se všichni dotázaní shodli na tom, že hodina atraktivní byla.

Další a to pátá otázka se žáků ptala na jejich hodnocení názornosti výuky. Dvacet žáků odpovědělo, bez dalších připomínek, že hodina byla názorná. Avšak dva žáci se vyjádřili i s konstruktivní kritikou. Jeden z nich uvedl: „*Dobře, ale na papíře* (tzn. v pracovním listu) *by to chtělo lépe vysvětlit.*“ Druhý žák uvedl, že ze začátku sice nevěděl, jak postupovat, avšak později na to přišel.

U šesté otázky, ve které jsem se žáků ptal, zda byla výuka a práce s pracovním listem srozumitelná, většina žáků odpověděla, že ano, a pouze tři žáci odpověděli rozdílně s připomínkou, že bez doplňujících otázek a mého vysvětlení by to nepochopili.

Další hlavní otázka a dvě podotázky byly žáky zodpovězeny bez rozdílů.

3.2.3 Analýza získaných dat druhého dotazníkového šetření

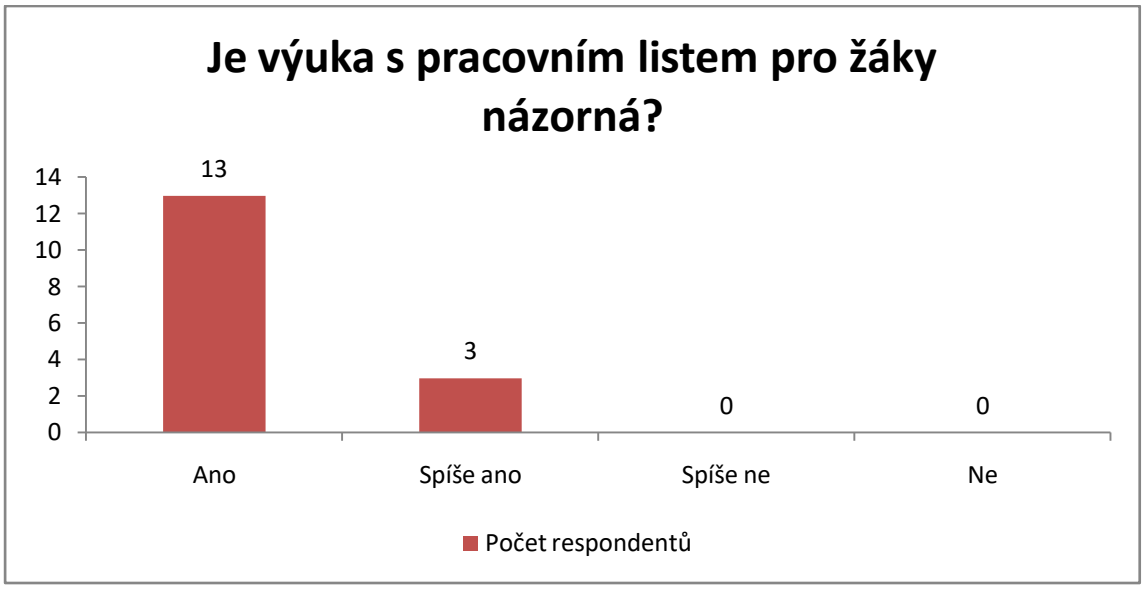
Při svém výzkumu jsem oslovil 17 žáků ze třídy 2. C, všichni oslovení se anonymního dotazníkového šetření zúčastnili. Dotazník se skládal ze 7 hlavních otevřených otázek a 4 otevřených podotázek. První až čtvrtá hlavní otázka a s nimi dvě podotázky byly zaměřeny na atraktivitu hodiny a pracovního listu. Další otázka byla věnována názornosti výuky. Šestá otázka se zaměřovala na srozumitelnost. Poslední otázka se týkala osobního přínosu a rozvoje pro žáky. Dotazníky byly vyplněny převážně dvojím způsobem, buď strohé odpovědi, nebo se žáci rozepsali i do několika souvětí. Většina žáků odpověděla na všechny otázky, dva žáci nezodpověděli jednu otázku, konkrétně otázku, která se týkala srozumitelnosti a názornosti. Při analýze jednotlivých odpovědí dotazníkového šetření jsem vyhodnotil odpovědi podle jejich kladných, nebo záporných znění. V některých odpovědích se vyskytla i konstruktivní kritika, která byla na místě. Díky této kritice jsem zjistil, že pracovní list měl několik chyb.

V následující části jsem v MS Excel vypracoval grafy, které se týkají výzkumných otázek a jsou podloženy dotazníkovým šetřením.

Graf č. 5 Je výuka s pracovním listem pro žáky atraktivní? (Vzorek 2)

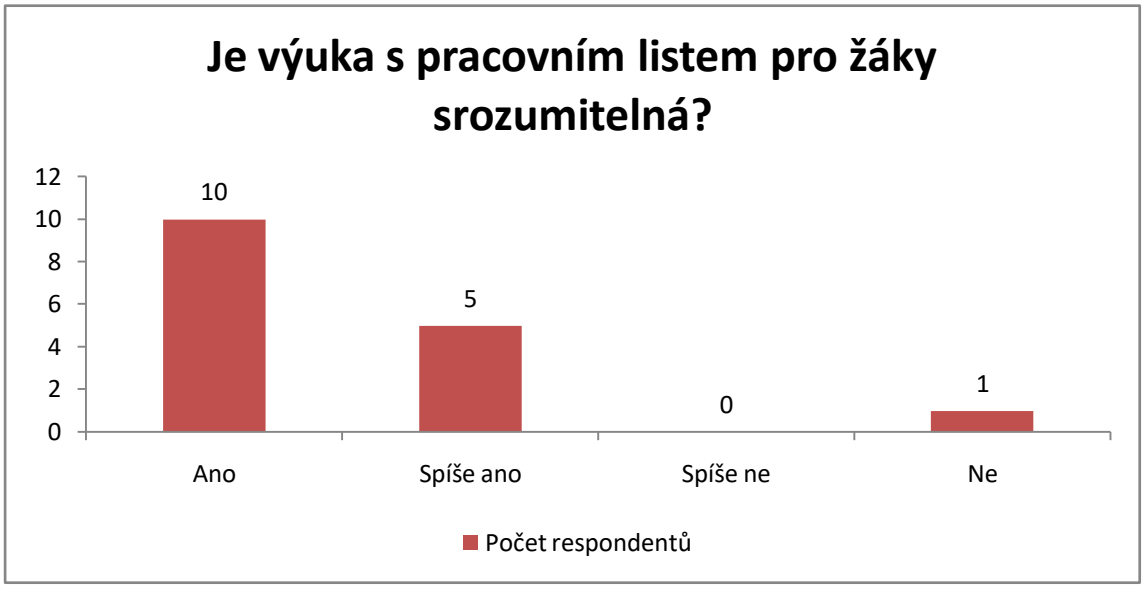
Z tohoto grafu vyplývá, že pro všechny žáky byly hodina i pracovní list atraktivní. Zcela pozitivní reakcí odpovědělo 8 žáků. Spíše pozitivně odpovědělo 9 žáků. Žádný ze žáků neodpověděl negativně, ani částečně negativně.

Graf č. 6 Je výuka s pracovním listem pro žáky názorná? (Vzorek 2)



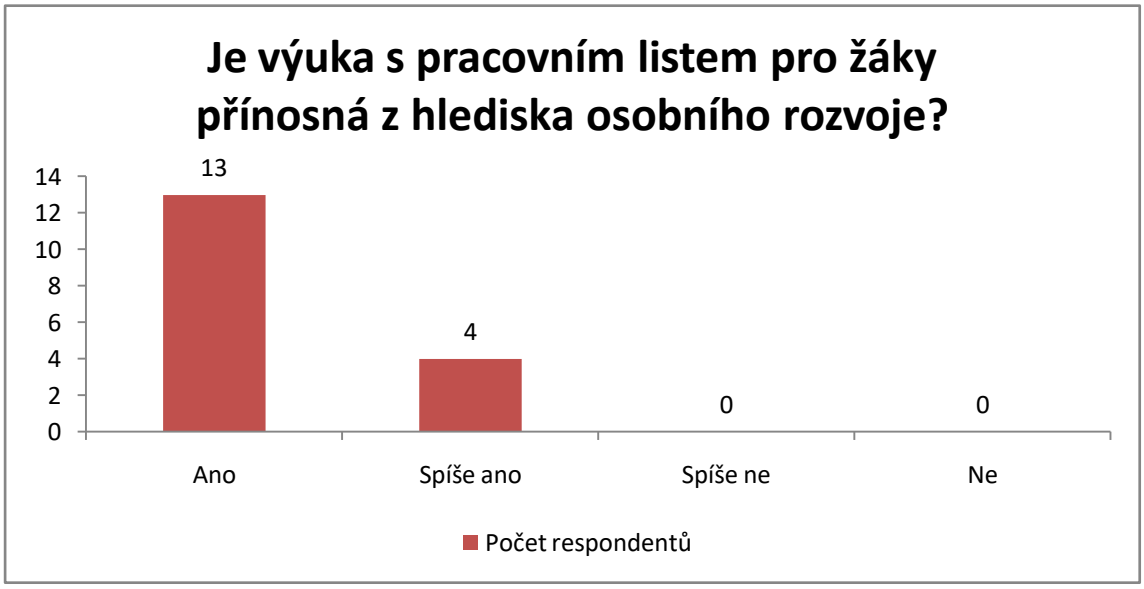
Z výše doloženého grafu je patrné, že názornost hodnotilo pozitivně 13 žáků. Do možnosti "Spíše ano" jsem zařadil 3 žáky. Pro možnost "Spíše ne" nebo "Ne" neodpověděl jediný žák. Na tuto otázku neodpověděl jeden žák.

Graf č. 7 Je výuka s pracovním listem pro žáky srozumitelná? (Vzorek 2)



Z tohoto grafu je možné zjistit, že pro větší část žáků byla výuka s pracovním listem srozumitelná. Pro 10 žáků byla hodina zcela srozumitelná, nebyl zde jediný náznak pochybností o tomto faktu. Dalších 5 žáků jsem zařadil do odpovědí "Spíše ano", protože se u nich objevovala často fráze "Ano, ale..." v mnoha různých variantách. Do varianty "Spíše ne" jsem nezařadil ani jednoho žáka, ale objevil se zde jeden žák, pro kterého byla hodina zcela nesrozumitelná. Jeden žák neodpověděl na otázku.

Graf č. 8 Je výuka s pracovním listem pro žáky přínosná z hlediska osobního rozvoje? (Vzorek 2)



Posledním grafem druhého vzorku je znázornění přínosnosti osobního rozvoje. Z tohoto grafu je patrné, že většina dotazovaných odpověděla zcela pozitivně. Pro možnost

"Ano" jsem zařadil 13 žáků. Další 4 žáci, kteří tam měli nějaké svoje "ale" jsem zařadil do "Spíše ano". Nikdo ze žáků neodpověděl negativně.

Z tohoto vzorku bych chtěl taktéž zařadit několik odpovědí, které jsou velmi přínosné pro tento výzkum. U první otázky ve znění: „*Jak hodnotíte pracovní list z hlediska jeho atraktivity?*“ se zde vyskytly tři zajímavé poznatky. Prvním z nich bylo, že ačkoliv pracovní list byl originální a zajímavý, byl také poněkud složitý. Druhá zajímavá odpověď byla, že ačkoliv to byla zajímavá aktivita, mohla být lépe zpracována. Třetím podnětem k zamyšlení byla odpověď, ve které bylo zmíněno: „*Dešifrování bylo docela složité a možná by to chtělo použít jiné znaky, než panáčky*.“

Na otázku druhou, která vypadala takto: „*Co vás na pracovním listu z grafické stránky nejvíce zaujalo?*“ jsem zaznamenal tři zajímavé odpovědi. První z nich byla, že žáka nejvíce zaujalo neobvyklé zadání. Druhou odpovědí bylo: „*Font, úprava textu a ty "obrázky" po krajích stránek jsou povedené. Ale samotná ta věc, ve které to spočívalo, což je šifra, byla asi v té nejhorší kvalitě, co vůbec šlo*.“ Třetí odpověď byla netradiční. Jednalo se o napodobení části designu pracovního listu.

Třetí otázka v dotazníkovém šetření byla zaměřena na to, co v pracovním listu chybí. Nejčastější odpověď byla „*Nic*“. Jednou z prvních odpovědí, která se od ostatních lišila, byl postřeh jednoho z žáků, který si všiml, že ve slově "nelidský" mi chybí písmeno "s". Další dvě odpovědi se shodly, že by bylo zapotřebí více upřesněné zadání. Čtvrtá a pátá odpověď naznačily, že pracovnímu listu chybí náznaky řešení. Poslední zajímaví odpověď u této otázky zněla takto: „*Nejdříve se zde řeklo, že je dobré to dělat pomocí analytiky, potom se ale řeklo, že je tato metoda špatná na krátké texty a my máme vyluštit šifru z pěti slov. Takže mi tam chyběla nějaká efektivní metoda, či rada*.“

První podotázkou, která spadá pod otázku číslo 3, byla: „*Co naopak přebývá?*“. I u této otázky byla nejčastější odpověď „*Nic*“. Čtyři z šesti zajímavých odpovědí se shodli na tom, že v pracovním listu je moc obecných informací, tzn. textu. Čtvrtá odpověď byla od žáka, který zaznamenal chyby v textu, takže vtipně poznamenal, že v pracovním listu přebývají právě tyto chyby. V poslední odpovědi se žák zmínil, že v pracovním listu bylo příliš mnoho volného prostoru.

Ve čtvrté otázce se žáci, až na jednoho, shodli ve svých odpovědích. Naproti tomu pátá otázka poskytla hned několik zajímavých odpovědí. Otázka pátá se týkala názornosti

výuky. První zajímavou odpovědí bylo: „*No, dostali jsme papír a luštili jsme to, takže ta výuka byla max. v tom, že jsme si přečetli ten dlouhý text. Co se týče ostatních hodin, všechno bylo v pohodě.*“ Další odpověď poznamenala, že jsem během výuky mohl mluvit více nahlas. Poslední odpověď podotkla, že jsem v pracovním listu mohl zdůraznit, že šifra byla psána v angličtině.

Šestá otázka se zabývala srozumitelností výuky a prací s pracovním listem. K této otázce jsem shledal zajímavou pouze jednu odpověď, kdy žák podotkl, že by mohlo být v pracovním listu lépe řečeno, co se po nich vlastně chce.

U zbylých otázek jsem již neshledal žádnou zajímavou odpověď.

3.2.4 Testování hypotéz

Hypotéza první - *Výuka s pracovním listem bude pro žáky spíše atraktivní, nežneatraktivní.*

K této hypotéze se váže graf číslo 1, 5 a případová studie.

V grafu číslo 1 žáci 2.B odpovídali takto: 72,72 % žáků odpovědělo zcela pozitivně, 18,18 % žáků odpovědělo spíše pozitivně, 9,09 % spíše negativně, avšak zcela negativně neodpověděl nikdo.

V grafu číslo 5 žáci 2.C odpovídali takto: 47,05 % žáků odpovědělo zcela pozitivně, 52,94 % žáků odpovědělo spíše pozitivně, spíše negativně nebo negativně neodpověděl nikdo.

V rámci případové studie jsem vypozoroval, že žákům se na první pohled pracovní list líbil, avšak byli lehce zaskočení jeho délkou. Nicméně po celou dobu jejich skupinové práce panovala velmi uvolněná a pozitivní atmosféra, tudíž si myslím, že ačkoliv byli zpočátku zaskočení množstvím, myslím si, že je dešifrování bavilo. Tento fakt je podložen zklamáním, které u nich nastalo, když museli práci přerušit.

Hypotéza druhá - *Výuka s pracovním listem bude pro žáky názorná, než nenázorná.*

K této hypotéze se váže graf číslo 2, 6 a případová studie.

V grafu číslo 2 žáci 2.B odpovídali takto: 59,09 % žáků odpovědělo zcela pozitivně, 31,81 % žáků odpovědělo spíše pozitivně, 9,09 % spíše negativně, avšak zcela negativně neodpověděl nikdo.

V grafu číslo 6 žáci 2.C odpovídali takto: 76,47 % žáků odpovědělo zcela pozitivně, 17,67 % žáků odpovědělo spíše pozitivně, spíše negativně nebo negativně neodpověděl nikdo.

V rámci případové studie jsem vypozoroval, že pro většinu žáků byla hodina názorná, protože neměli další doplňující otázky.

Hypotéza třetí - *Výuka s pracovním listem bude pro žáky spíše srozumitelná, než nesrozumitelná.*

K této hypotéze se váže graf číslo 3, 7 a případová studie.

V grafu číslo 3 žáci 2.B odpovídali takto: 72,72 % žáků odpovědělo zcela pozitivně, 13,63 % žáků odpovědělo spíše pozitivně, 4,54 % spíše negativně, negativně odpovědělo 4,54 % žáků.

V grafu číslo 7 žáci 2.C odpovídali takto: 58,82 % žáků odpovědělo zcela pozitivně, 29,41 % žáků odpovědělo spíše pozitivně, spíše negativně neopověděl nikdo a negativně odpovědělo 5,88 % žáků.

V rámci případové studie jsem vypozoroval, že samotná výuka byla srozumitelná, avšak práce s pracovním listem už tolik ne. Tento fakt mi potvrdili doplňující otázky žáků, co mají dělat.

Hypotéza čtvrtá - *Výuka s pracovním listem bude pro žáky spíše přínosná pro osobní rozvoj, než nepřínosná.*

K této hypotéze se váže graf číslo 4, 8 a případová studie.

V grafu číslo 4 žáci 2.B odpovídali takto: 100 % žáků odpovědělo zcela pozitivně.

V grafu číslo 8 žáci 2.C odpovídali takto: 76,47 % žáků odpovědělo zcela pozitivně, 23,52 % žáků odpovědělo spíše pozitivně, spíše negativně nebo negativně neodpověděl nikdo.

Během pozorování, v rámci případové studie, jsem zjistil, že pro většinu žáků byla výuka i práce s pracovním listem přínosná. Žáci mi tento fakt potvrdili v diskusi, která na konci hodiny proběhla.

3.3 Výsledky výzkumného šetření

Po analýze dat získaných z anonymního dotazníkového šetření a případové studie jsem byl schopen odpovědět na všechny výzkumné otázky a stanovené hypotézy. V rámci tohoto výzkumu se mi podařilo také splnit veškeré stanovené cíle.

3.3.1 Odpovědi na výzkumné otázky

Otázka č. 1 - *Je výuka s pracovním listem pro žáky atraktivní?*

Tato otázka byla pro mne nejdůležitější, protože zaujmout žáky ve výuce s použitím pracovních listů není vždy jednoduché. Proto jsem se snažil hned ze začátku žáky zaujmout grafickou stránkou pracovního listu. Podle získaných dat, které jsou podloženy, jak případovou studií, tak i dotazníkovým šetřením, jsem zjistil, že můj stanovený osobní cíl byl splněn. Výuka byla atraktivní a to nejen z hlediska designu pracovního listu, který na tom měl podíl. Odpovědí na výzkumnou otázku je tedy ANO, i když je nutné brát v úvahu všechny odpovědi.

Otázka č. 2 - *Je výuka s pracovním listem pro žáky názorná?*

Názornost ve výuce je pro mne i žáky velmi důležitá, protože ne každý žák musí hned pochopit, co jsem se chtěl předat v pracovních listech. Tudíž pracovní listy pro ně nemusí být vždy naprosto srozumitelné. V takovémto případě je nutné, aby můj ústní doprovod byl co nejvíce názorný a uměl jsem žáky navést správným směrem. Pro někoho je srozumitelnost a názornost synonymem, avšak já v tom vidím rozdíl. Dle případové studie a odpovědí z dotazníkového šetření tento rozdíl vnímají i dotázaní žáci. Podle mého pozorování v rámci případové studie a jejich odpovědí v dotazníkovém šetření usuzuji, že hodina byla názorná, odpovědí je tedy ANO. Nicméně i zde je nutné brát v potaz všechny odpovědi a podle nich hodinu i pracovní list upravit a přizpůsobit.

Otázka č. 3 - *Je výuka s pracovním listem pro žáky srozumitelná?*

Ačkoliv jsem myslel, že jsem pracovní listy napsal dosti srozumitelně, při analýze získaných dat jsem zjistil, že ne všichni žáci semnou sdíleli tento názor. Objevilo se i několik žáků, kteří měli na srozumitelnost zcela negativní zpětnou vazbu nebo názor. U této otázky je, pokud se na ní díváme z hlediska čísel, odpovědí ANO, avšak objevuje se tu více negativních ohlasů, z čehož usuzuji, že ne vše bylo v pracovním listu srozumitelné. Tento fakt mi potvrzuje i pozorování, které jsem dělal v rámci případové studie. Nesrozumitelnost se projevovala dotazy žáků, co tedy mají dělat, nebo jak. Díky těmto odpovědím je možné upravit pracovní listy a strukturu výuky tak, aby byla pro žáky lépe srozumitelná.

Otázka č. 4 - *Je výuka s pracovním listem pro žáky přínosná s hlediska osobního rozvoje?*

Vzhledem k tomu, že jsem se snažil žáky naučit něco nového, nad rámec klasické výuky, většina z nich hodnotila hodinu jako přínosnou. Žádný ze žáků nehodnotil přínosnost této hodiny negativně. V podotázce, která zjišťovala, v čem konkrétně byla hodina přínosná, odpovídali žáci většinou, že se naučili něco nového, z čehož vyplývá, že odpovědí na tuto otázku je opět ANO. Tuto odpověď podložila i případová studie.

3.3.2 Vyhodnocení stanovených hypotéz

Hypotéza č. 1 - *Výuka s pracovním listem bude pro žáky spíše atraktivní, než neatraktivní.*

Vzhledem k sesbíraným datům jsem vyhodnotil tuto hypotézu jako pravdivou. Toto tvrzení podkládá případová studie i dotazníkové šetření.

Hypotéza č. 2 - *Výuka s pracovním listem bude pro žáky názorná, než nenázorná.*

Vzhledem k sesbíraným datům jsem vyhodnotil tuto hypotézu jako pravdivou. Toto tvrzení podkládá případová studie i dotazníkové šetření.

Hypotéza č. 3 - *Výuka s pracovním listem bude pro žáky spíše srozumitelná, nežnesrozumitelná.*

Vzhledem k sesbíraným datům jsem vyhodnotil tuto hypotézu jako pravdivou. Toto tvrzení podkládá případová studie i dotazníkové šetření.

Hypotéza č. 4 - *Výuka s pracovním listem bude pro žáky spíše přínosná pro osobní rozvoj, než nepřínosná.*

Vzhledem k sesbíraným datům jsem vyhodnotil tuto hypotézu jako pravdivou. Toto tvrzení podkládá případová studie i dotazníkové šetření.

Závěr

Cílem diplomové práce bylo využít silný motivační potenciál klasických ručních šifer jako téma v informatickém vzdělávání. Z provedené analýzy dotazníkového šetření plyne, že tento vytyčený cíl byl splněn. Práce byla rozdělena na tři hlavní tematické celky a jejich kapitoly.

Prvním tematickým okruhem byla teoretická část, jejímž cílem bylo podat stručný přehled faktorů motivace žáků, forem výuky a metod výuky a z nich vybrat ty, které jsou vhodné k výuce tématu historické a literární šifry. Tuto část jsem rozdělil na pět kapitol. První kapitola shrnovala v úvodu základní poznatky o motivaci. Tuto kapitolu jsem dále rozdělil na čtyři podkapitoly, které se zabývali vnitřní a vnější motivací, motivujícími a demotivujícími činiteli výuky, metodám rozvíjející motivaci a současným kognitivním teoriím motivace.

Druhá kapitola se věnovala klíčovým kompetencím, kde jsem shrnul a vypsal kompetence pro gymnázia.

Třetí kapitolou jsem zvolil formy a metody výuky. Jak už název této kapitoly napovídá, rozdělil jsem tuto kapitolu, podle jména kapitoly, na dvě podkapitoly. V první podkapitole jsem shrnul formy výuky a rozdělil je podle určitých kritérií. Druhou podkapitolou jsem popsal a rozčlenil metody výuky.

Ve čtvrté kapitole jsem se věnoval především kryptologickým pojmům, kde jsem hned v obecném úvodu kapitoly popsal, co to je kryptologie. K tomuto popisu jsem dopsal seznam pojmů, které kryptologie používá.

Poslední kapitolou tohoto tematického celku jsou základní typy šifer. V této části jsem popsal a vysvětlil základní druhy šifer, kdy jsem se více zaměřil na šifru substituční, kterou jsem ve své práci využíval.

Dalším tematickým celkem je praktická část práce, jejíž cílem bylo vytipovat tři až pět konkrétních šifrových systémů, pro něž jsem zpracoval pracovní listy pro žáky. Tuto část jsem rozdělil na tři kapitoly, podle počtu pracovních listů, které jsem pro práci vytvořil a které byly hlavním prvkem výzkumu této práce. Tato část práce se věnovala popisu pracovních listů a komentářů k nim.

První kapitola se tedy věnuje pracovnímu listu. Tento list obsahuje devět podkapitol a každá popisuje určitou část pracovního listu. První částí, kterou jsem popsal a okomentoval, je titulní strana. Následoval úvod, definice šifrového systému, popis šifrování a dešifrování, metody luštění, zadání pracovního listu, řešení, metodické poznámky a zdroje. Všechny tyto části obsahují části pracovního listu, ke kterým jsem doplnil popis a náležitý komentář. V druhé a třetí kapitole jsem taktéž detailně popsal pracovní listy, ve kterých se lišila zadaná šifra.

Třetím a posledním tematickým okruhem byla empirická část, která se věnovala celkově kvalitativnímu výzkumu, jak teoreticky, tak i prakticky. Cílem empirické části práce bylo ověřit jeden z vytvořených pracovních listů ve výuce a zhodnotit tuto výuku formou kvalitativního výzkumu sestávajícího z případové studie popisující výuku s využitím zvoleného pracovního listu a z dotazníkového šetření, ve kterém žáci odpoví na několik otevřených otázek vztahujících se k posouzení atraktivity, názornosti a srozumitelnosti výuky a k jejímu přínosu pro osobní rozvoj respondentů. Tato část se dále věnovala zpracováním dat získaných případovou studií, kvalitativního dotazníkového šetření a samozřejmě výsledkům tohoto výzkumu. Tento celek jsem rozdělil na tři kapitoly, které se dále dělily na podkapitoly.

První kapitola je věnována kvalitativnímu výzkumu, kde jsem teoreticky shrnul co to kvalitativní výzkum je. Dále jsem v této části formuloval výzkumné otázky a hypotézy. V této kapitole jsem taktéž formuloval metodologii a popsal místo šetření a výzkumný vzorek.

Druhou kapitolu, kterou jsem taktéž rozdělil na několik podkapitol, jsem věnoval zpracování získaných dat. V této části jsem napsal případovou studii, jejímž objektem byla právě výuka s pracovními listy obsahujícími šifru. Následně jsem zanalyzoval první a druhé dotazníkové šetření. Poslední podkapitola se věnovala testování stanovených hypotéz.

Poslední kapitola se zabývala výsledky výzkumného šetření, kde jsem odpověděl na všechny výzkumné otázky a vyhodnotil stanovené hypotézy.

Podle mého názoru se cíle práce podařilo splnit. Tento názor jsem si ověřil v poslední kapitole této práce, kde jsem shrnul a vyhodnotil výsledky celé práce. Podařilo se mi odpovědět na všechny výzkumné otázky, které se týkaly základních pilířů této práce a to atraktivnosti, názornosti, srozumitelnosti a osobního rozvoj žáků. Na všechny tyto otázky jsem získal odpovědi, že informatická výuka s využitím klasických a literárních šifer, je pro žáky atraktivní, názorná, srozumitelná a je přínosná s hlediska osobního rozvoje. Dále se mi

podařilo potvrdit stanovené hypotézy, kdy jsem předpokládal, že hodina pro žáky bude atraktivní, názorná, atd.

Osobně se domnívám, že práce byla přínosná z hlediska využití klasických a literárních šifer v informatické výuce. Dále se domnívám, že tato práce a její výsledky mohou být odrazovým můstkem pro širší začlenění těchto netradičních pracovních listů do běžné výuky, nebo alespoň inspirací pro pedagogy, kteří by se o tuto problematiku zajímali.

Použité zdroje

Seznam literatury

1. BELZ; Siegrist. *Klíčové kompetence a jejich rozvíjení: východiska, metody, cvičení a hry*. Praha: Portál, 2001. 375 s. ISBN 80-7178-479-6.

2. ČAPEK, Robert. *Odměny a tresty ve školní praxi: kázeňské strategie, zásady odměňování a trestání, hodnocení a klasifikace, podpora a motivace žáků*. 2., přeprac. vyd. Praha: Grada, 2014, 186 s. Pedagogika. ISBN 978-80-247-4639-5.

3. HENDL, Jan. *Kvalitativní výzkum: základní teorie, metody a aplikace*. Čtvrté, přepracované a rozšířené vydání. Praha: Portál, 2016, 437 s. ISBN 978-80-262-0982-9.

4. CHRÁSKA, Miroslav. *Úvod do výzkumu v pedagogice*. 2. vyd. Olomouc: Univerzita Palackého v Olomouci, 2006. ISBN isbn80-244-1367-1.

5. JANEČEK, Jiří. *Odhalená tajemství šifrovacích klíčů minulosti: ruční šifry*. Praha: Naše vojsko, 1994, 183 s. Mozaika. ISBN 80-206-0462-6.

6. LOKŠOVÁ, Irena a Jozef LOKŠA. *Pozornost, motivace, relaxace a tvořivost ve škole*. Praha: Portál, 2006, 199 s. Pedagogická praxe. ISBN 80-7178-205-X.

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

8. NELEŠOVSKÁ, Alena. *Pedagogická komunikace v teorii a praxi*. Praha: Grada, 2005. Pedagogika (Grada). ISBN 80-247-0738-1.

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

10. SINGH, Simon. *Kniha kódů a šifer: tajná komunikace od starého Egypta po kvantovou kryptografii*. 2. vyd. v českém jazyce. Přeložil Dita ECKHARDTOVÁ, přeložil Petr KOUBSKÝ. Praha: Dokořán, 2009, 382 s. Aliter. ISBN 978-80-7363-268-7.

11. VALIŠOVÁ, Alena, Hana KASÍKOVÁ a Miroslav BUREŠ. *Pedagogika pro učitele*. 2., rozš. a aktualiz. vyd. Praha: Grada, 2011. Pedagogika (Grada). ISBN 978-80-247-3357-9.

12. VLNAS, Václav. *Počítačová analýza šifrované korespondence rodu Piccolomini.* Hradec Králové: Přírodovědecká fakulta Univerzity Hradec Králové, 2017. 72 s. Bakalářská práce.

13. VONDRUŠKA, Pavel. *Kryptologie, šifrování a tajná písma*. Praha: Albatros, 2006, 340 s. Oko. ISBN 80-00-01888-8.

14. ZORMANOVÁ, Lucie. *Obecná didaktika: pro studium a praxi*. Praha: Grada, 2014. Pedagogika (Grada). ISBN 978-80-247-4590-9.

15. ZORMANOVÁ, Lucie. *Výukové metody v pedagogice: tradiční a inovativní metody, transmisivní a konstruktivistické pojetí výuky, klasifikace výukových metod*. Praha: Grada, 2012. Pedagogika (Grada). ISBN 978-80-247-4100-0.

Seznam internetových zdrojů

1. *RVP pro gymnázia* [online, cit. 21. 4. 2019], Národní ústav pro vzdělávání. Dostupné z WWW: < http://www.nuv.cz/t/rvp-pro-gymnazia>

2. *Formy výuky* [online, cit. 11. 7. 2019], Metodický portál RVP. Dostupné z WWW: <https://wiki.rvp.cz/Knihovna/1.Pedagogick%C3%BD_lexikon/F/Formy_v%C3%BDuky>

Seznam grafů

Přílohy

A. Pracovní listy, které jsou v práci popisovány

A01. Pracovní list – 1 „Caesarova šifra“

A02. Pracovní list – 1 „Zlatý Brouk“

A03. Pracovní list – 1 „Tančící figurky“

B. Dotazníkové šetření

B01. Dotazník

PRACOVNÍ LIST

Caesarova šifra

Obsah

ÚVOD

První písemně doloženou existenci této šifry můžeme najít v *Zápiscích o válce galské*, které napsal slavný vojevůdce Gaius Julius Caesar během svého tažení do Gálie. Caesar používal hned několik typů šifer, jako například jednoduchou substituci římských písmen za řecká, nebo posun písmen o tři. Tento slavný vojevůdce používal šifry tak často, že o nich napsal Valerius Probus celé dílo, které se však nedochovalo. Další autor, který o Caesarovi a jeho šifrách psal, byl Gaius Suetonius Tranquillus. Suetonius napsal dílo *Životopisy dvanácti císařů*, kde detailně popisuje šifru s posunem písmen o tři znaky.

(SINGH, 2003, s. 12–13)

DEFINICE ŠIFROVÉHO SYSTÉMU

Tento šifrovací systém nese název **substituční šifrování**. U toho typu šifrování je jeden znak otevřeného textu nahrazen jedním znakem šifrové abecedy. Šifrová abeceda může jak jednotlivá písmena v jiném pořadí, nebo i různé speciální znaky, které si autor vymyslí. Tento typ šifrování byl používán pro velmi dlouhou dobu díky jeho oblibě a jednoduchosti, nicméně s rozvojem šifrování jednoduchá substituce (znak za znak) začínala být lehce prolomitelná. Tento systém si udržel svojí oblíbenost a využitelnost, avšak došlo ke stížení šifrování a dešifrování a vzniklo více poddruhů tohoto systému. Tento systém se používá také jako pomůcka, například Morseova abeceda nebo Braillovo písmo.

Otevřený text - je text, který ještě neprošel procesem šifrování a je ho možné přečíst

Šifrová abeceda - je to skupina znaků, která slouží k zašifrování otevřeného textu, mohou to být písmena otevřeného textu, čísla, nebo obrazce

Šifrování - proces, při kterém dochází k přeměně otevřeného textu do textu šifrovaného pomocí šifrového systému

Šifrový text - je text, který prošel procesem šifrování a obsahuje určitý systém šifrování

(JANEČEK, 1994, s. 73–76)
(VONDRUŠKA, 2006, s. 29–31)

POPIS ŠIFROVÁNÍ A DEŠIFROVÁNÍ

Zašifrování u jednoduché substice je velmi jednoduché, protože se nahradí jeden znak otevřeného textu za jeden znak šifrovací abecedy. Takto jednoduše se otevřený text zašifruje, avšak v tenhle moment nastává problém s rozluštěním. Z tohoto důvodu má šifra i svůj klíč, podle kterého příjemce lehce šifru rozluští a nemusí jít podrobovat různým metodám luštění. U jednoduché substituce musí příjemce znát znaky šifrovací abecedy a musí vědět, co jaký znak znamená. Vetšinou to bývá formou seznamu, kde je ke každému znaku šifrovací abecedy přiřazeno písmeno abecedy.

METODY LUŠTĚNÍ

Metod luštění u tohoto typu šifer je hned několik, avšak nejčastěji používaná je frekvenční analýza znaků. Tato analýza pracuje s tím, že pro každý jazyk je specifická frekvence používání souhlasásek a samohlásek.
Pro příklad jsem vytvořil v MS Excel tabulku s podmíněným formátováním, kde jsem využil data z *https://matematika.cz/frekvencni-analyza.* Na této tabulce můžeme vidět, že nejčastěji používaným písmenem jsou písmena e, a, o,i. Tato metoda má však jednu nevýhodu, je težce uplatnitelná na krátké texty, kde frekvence znaků nemusí odpovídat tabulce níže. V takovémto případě se musí využít následujícího postupu.

První krok je shrnout si fakta, která jsou zřejmá. V našem případě se jedná o substituční šifru, konkrétně Caesarovu šifru, o které víme, že pracuje na posunu písmen. Nicméně nevíme o jaký přesný počet písmen. Nabízí se tu možnost, že zkusíme všechny kombinace (posuny) a budeme sledovat, jestli klíč zapadl, nebo nikoliv.
Nicméně je zde ještě možnost hledání určitých indicií. V úvodu je zmíněno, že Caesar šifry používal během vojenského tažení, proto se nabízí možnost, že zpráva bude vojenského charakteru. Další indicie je, že listina pravděpodobně obsahuje podpis, tudíž je to velký bonus když víme, kdo onu zprávu psal.

FREKVENČNÍ ANALÝZA ČESKÉHO JAZYKA

a	134675829	9,589%
c	42120335	2,999%
b	24944593	1,776%
e	153141622	10,904%
d	53015496	3,775%
g	3087128	0,220%
f	2458624	0,175%
i	93903002	6,686%
h	35075708	2,497%
k	49549907	3,528%
j	32383080	2,306%
m	50636489	3,605%
l	80345129	5,721%
o	112776769	8,030%
n	83104322	5,917%
q	83322	0,006%
p	43747863	3,115%
s	78451777	5,586%
r	61750942	4,397%
u	50265458	3,579%
t	75633324	5,385%
w	762129	0,054%
v	55510103	3,952%
y	40132126	2,858%
x	504334	0,036%
z	46383740	3,303%

Zdroj: https://matematika.cz/frekvencni-analyza

ZADÁNÍ PRACOVNÍHO LISTU

Zpráva **IX.** legii

AXCHTICHH

YAMBDWXDC UMORR WI BMEMA I CIV YXKIC WI LIUBR AXCHTICHH
YXTDL WMSITH EXSIT LMCHMACDSM CIT PX QHCCM I MGMVYUIAWM YXYAIECM
CHI TICHLXD KMWD LACHCM BEM YXCHRKM

EIB OMWMAIU MIRDB SDURDB KIMBIA

pozn.: 1) písmena **C a H** jsou v textu jeden znak (**CH**)
2) abeceda je **bez** diakritiky

ZADÁNÍ PRACOVNÍHO LISTU

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

ŘEŠENÍ

Následující řešení je pomocí tabulky, která je zároveň klíčem k šifře výše. Pod tabulkou je přepsaný celý text.

1	2	3	4	5	6	7	8	9	10
a	b	c	d	e	f	g	h	ch	i
i	j	k	l	m	n	o	p	q	r

11	12	13	14	15	16	17	18	19	20
j	k	l	m	n	o	p	q	r	s
s	t	u	v	w	x	y	z	a	b

21	22	23	24	25	26	27
t	u	v	w	x	y	z
c	d	e	f	g	h	ch

Kompletní řešení

ROZKAZY

PRESUNOUT LEGII NA SEVER A TAM POCKAT NA DALSI ROZKAZY
POKUD NEJAKY VOJAK DEZERTUJE TAK HO CHYTTE A EXEMPLARNE POPRAVTE
ZA KAZDOU CENU DRZET SVE POZICE

VAS GENERAL GAIUS JULIUS CAESAR

METODICKÉ POZNÁMKY

cíle:	žák pomocí indicií rozluští systém šifrování a převede šifrovaný text do textu otevřeného
věková skupina:	13-16
organizace činnosti:	žáci do dvojic dostanou pracovní list, kromě řešení a metodických poznámek.
čas potřebný ke zpracování:	30-45 minut
pomůcky:	psací potřeby
reflexe:	skupinová diskuse nad vypracovanými pracovními listy
klíčové kompetence:	kompetence k učení kompetence sociální a personální kompetence k řešení problému
očekávané výstupy:	žák popíše konkrétní způsob, jak k řešení šifry došel
průřezová témata:	Osobnostní a sociální výchova Výchova k myšlení v evropských a globálních souvislostech Multikulturní výchova

ZDROJE

SEZNAM LITERATURY

JANEČEK, Jiří. *Rozluštěná tajemství: luštitelé, dešifranti, kódy a odhalení.* Praha: XYZ, 2006, 268 s. ISBN 80-86864-54-5.

SINGH, Simon. *Kniha kódů a šifer: tajná komunikace od starého Egypta po kvantovou kryptografii.* 2. vyd. v českém jazyce. Přeloţil Dita ECKHARDTOVÁ, přeloţil Petr KOUBSKÝ. Praha: Dokořán, 2009, 382 s. Aliter. ISBN 978-80-7363-268-7.

VONDRUŠKA, Pavel. *Kryptologie, šifrování a tajná písma.* Praha: Albatros, 2006, 340 s. Oko. ISBN 80-00-01888-8.

Pracovní list

Zlatý Brouk

EDGAR ALLAN POE

OBSAH

Úvod

Edgar Allan Poe

(19. 1. 1809 – 7. 10. 1849)

Byl americký prozaik, esejista, básník a literární teoretik.
Narodil se v Bostonu v USA do rodiny kočovných herců Poových. Jeho otec trpěl alkoholismem a v roce 1810 zemřel. Poova matka zemřela rok poté na tuberkulózu. Malý Edgar se stal sirotkem, kterého se ujala rodina Allanových.

Zdroj: https://en.wikipedia.org/wiki/Edgar_Allan_Poe

Edgar se se svojí novou rodinou přestěhoval z USA do Liverpoolu, do Anglie, která se mu stala inpirací pro jeho díla. Edgar studoval na univerzitě ve Virginii, kde začal mít problém s alkoholismem a díky hráčství se zadlužil. Jako jediné východisko se mu stal zápis na vojenskou akademii ve West Pointu, kterou taktéž nedodělal. V roce 1836 se Edgar oženil a vzal si svoji sestřenici Virginii Clemm, která v roce 1847 zemřela. Po její smrti začal propadat drogám a alkoholu a následně depresím, díky kterým často měnil zaměstnání. 3. října 1849 byl Poe nalezen na chodníku v bezvědomí, kdy byl okamžitě hospitalizován. Z tohoto kómatu se však neprobral a zemřel 7.10.1849 na překrvení mozku.

Jeho život a dílo

Zlatý brouk

Též Zlatý Skarabeus (Scarabeus) nebo Zlatý Chrobák (v anglickém originále The Gold-Bug) je dobrodružná povídka Edgara Allana Poa. Tato povídka vyšla v roce 1843 a čtenáře zaujme hned několika věcmi. V povídce se objevují zvláštní náhody, které jsou až magické povahy. Na všechny tyto náhody čtenář najde logické vysvětlení. Tato povídka je též zajímavá tím, že obsahuje substituční šifru, která povídce dává mysteriózní nádech. Děj se odehrává na Sullivanově ostrove v Jižní Karolině (USA), kde hlavní zápletkou je najít ukrytý poklad.

Zdroj: https://en.wikipedia.org/wiki/Edgar_Allan_Poe

Definice šifrového systému

Definice

Tento šifrovací systém nese název substituční šifrování. U toho typu šifrování je jeden znak otevřeného textu nahrazen jedním znakem šifrové abecedy. Šifrová abeceda může jak jednotlivá písmena v jiném pořadí, nebo i různé speciální znaky, které si autor vymyslí. Tento typ šifrování byl používán pro velmi dlouhou dobu díky jeho oblibě a jednoduchosti, nicméně s rozvojem šifrování jednoduchá substituce (znak za znak) začínala být lehce prolomitelná. Tento systém si udržel svojí oblíbenost a využitelnost, avšak došlo ke stížení šifrování a dešifrování a vzniklo více poddruhů tohoto systému. Tento systém se používá také jako pomůcka, například Morseova abeceda nebo Braillovo písmo.

Pojmy

Otevřený text - je text, který ještě neprošel procesem šifrování a je ho možné přečíst

Šifrová abeceda - je to skupina znaků, která slouží k zašifrování otevřeného textu, mohou to být písmena otevřeného textu, čísla, nebo obrazce

Šifrování - proces, při kterém dochází k přeměně otevřeného textu do textu šifrovaného pomocí šifrového systému

Šifrový text - je text, který prošel procesem šifrování a obsahuje určitý systém šifrování

(JANEČEK, 1994, s. 73–76)
(VONDRUŠKA, 2006, s. 29–31)

Popis šifrování a dešifrování

Šifrování

Zašifrování u jednoduché substice je velmi jednoduché, protože se nahradí jeden znak otevřeného textu za jeden znak šifrovací abecedy. Pro úspěšné zašifrování oteřeného textu je potřeba mít šifrovou abecedu a otevřený text. Pokud má pisatel tyto dvě věci, tak může začít zprávu otevřeného textu začít převádět do textu zašifrovaného. Pokud pisatel nezná šifrovou abecedu zpaměti, jde mu šifrování poměrně pomalu, když píše nějakou zprávu, proto se v dnešní době používají různé programy a algoritmy. Tyto programy lehce provedou tento úkon a je to během mžiku.

Dešifrování

Dešifrování probíhá téměř stejně, jako šifrování, jen opačným způsobem. Jedná se o převod z šifrovaného textu do otevřeného textu. Pro dešifrování potřebuje příjemce šifry znát šifrovou abecedu (tedy klíč k šifře), nebo šifru podrobit frekvenční analýze a následně ji rozluštit.

(JANEČEK, 1994, s. 73–76)
(VONDRUŠKA, 2006, s. 29–31)

Metody luštění

Definice

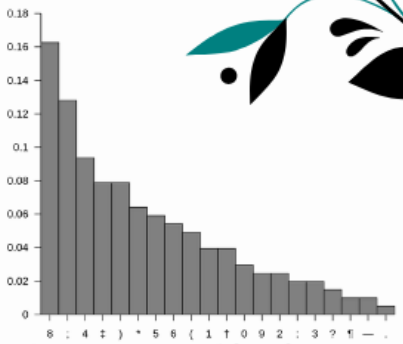
Metod luštění u tohoto typu šifer je hned několik, avšak nejčastěji používaná je frekvenční analýza znaků. Tato analýza pracuje s tím, že pro každý jazyk je specifická frekvence používání souhlasásek a samohlásek.

Frekvenční analýza

Základem pro frekvenční analýzu je znát jazyk, kterým je šifra psána. Následně musí sečíst, kolikrát se daný znak v šifře objeví a z tohoto součtu udělat graf četnosti, viz. graf vpravo. Tento graf je pak nutné porovnat s grafem relativní četnosti znaků konkrétního jazyka. Následuje rozluštění nejčastěji se opakujících znaků a určování členů (typické pro angličtinu). Pomocí tohoto postupu získáváme víc a víc písmen, které nám odkrývají další a další, dokud není šifra zcela rozluštěna.

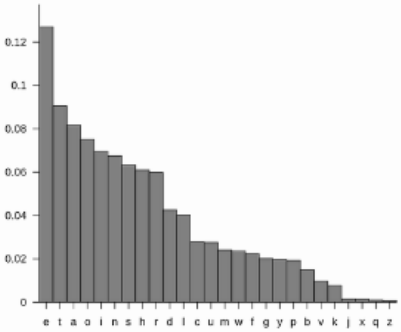
Tato metoda má však jednu nevýhodu, je težce uplatnitelná na krátké texty, kde frekvence znaků nemusí odpovídat grafu.

Tato šifra je poměrně jednoduchá, pro složitější substituce se používají moderní kryptografické programy a různé dešifrovací algoritmy, které šifru rozluští v mžiku.



Relativní četnost znaků v šifře

Zdroj: https://en.wikipedia.org/wiki/The_Gold-Bug



Relativní četnost znaků (angličtina)

Zdroj: https://en.wikipedia.org/wiki/The_Gold-Bug

Zadání pracovního listu

Šifra

53‡‡†305))6*;4826)4‡.)4‡);806*;48†8¶60))85;;]8*;:‡*8†83(88)5*†;46(;88*96
?;8)‡(;485);5*†2:*‡(;4956*2(5*—4)8¶8*;4069285);)6†8)4‡‡;1(‡9;48081;8:8‡
1;48†85;4)485†528806*81(‡9;48;(88;4(‡?34;48)4‡;161;:188;‡?;

(POE, 2013, s. 35)

Zadání pracovního listu

Řešení

Kompletní řešení šifry

Tabulka s klíčem

Znak(y)	8	;	4	‡	)	*	5	6	(	1	†	0	9	2	:	3	?	¶	–	.
Písmeno	e	t	h	o	s	n	a	i	r	f	d	l	m	b	y	g	u	v	c	p

Šifra

53‡‡†305))6*;4826)4‡.)4‡);806*;48†8

¶60))85;1‡(;:‡*8†83(88)5*†;46(;88*96

* ?;8)*‡(;485);5*†2:*‡(;4956*2(5*—4)8

¶8*;4069285);)6†8)4‡‡;1(‡9;48081;8:8‡

1;48†85;4)485†528806*81(‡9;48;(88;4

(‡?34;48)4‡;161;:188;‡?;

Kompletní řešení

agoodglassinthebishopshostelinthede

vilsseatfortyonedegreesandthirteenmi

nutesnortheastandbynorthmainbranchse

venthlimbeastsideshootfromthelefteyeo

fthedeathsheadabeelinefromthetreeth

roughtheshotfiftyfeetout

Pro doplnění nebo český překlad:

Doplnění

Překlad

(POE, 2013, s. 35)

Metodické poznámky

cíle:	žák pomocí indicií rozluští systém šifrování a převede šifrovaný text do textu otevřeného
věková skupina:	15-18
organizace činnosti:	žáci do dvojic dostanou pracovní list, kromě řešení a metodických poznámek.
čas potřebný ke zpracování:	30-45 minut
pomůcky:	psací potřeby, v případě vyššího zájmu mobilní telefon
reflexe:	skupinová diskuse nad vypracovanými pracovními listy
klíčové kompetence:	kompetence k učení kompetence sociální a personální kompetence k řešení problému
očekávané výstupy:	žák popíše konkrétní způsob, jak k řešení šifry došel
průřezová témata:	Osobnostní a sociální výchova Výchova k myšlení v evropských a globálních souvislostech Multikulturní výchova

Zdroje

Seznam literatury

JANEČEK, Jiří. *Odhalená tajemství šifrovacích klíčů minulosti: ruční šifry*. Praha: Naše vojsko, 1994, 183 s. Mozaika. ISBN 80-206-0462-6.

VONDRUŠKA, Pavel. *Kryptologie, šifrování a tajná písma*. Praha: Albatros, 2006, 340 s. Oko. ISBN 80-00-01888-8.

Internetové zdroje

Edgar Allan Poe [online, cit. 18. 6. 2019], Wikipedia. Dostupné z WWW: < https://en.wikipedia.org/wiki/Edgar_Allan_Poe>

POE, Edgar Allan. Zlatý chrobák [online, cit. 18. 6. 2019]. Přel. Vácslav ČERNÝ. V MKP 1. vyd. Praha: Městská knihovna v Praze, 2013. Dostupné z WWW: <http://web2.mlp.cz/koweb/00/03/92/94/90/zlaty_chrobak.pdf>

The Gold-Bug [online, cit. 18. 6. 2019], Wikipedia. Dostupné z WWW: <https://en.wikipedia.org/wiki/The_Gold-Bug>

PRACOVNÍ LIST

TANČÍCÍ FIGURKY

ARTHUR CONAN DOYLE

OBSAH

ÚVOD

ARTHUR CONAN DOYLE

(22. 5. 1899 – 7. 7. 1930)

Celým jménem Sir Arthur Conan Ignatius Doyle, byl britský lékař a spisovatel. Za svého života byl velmi aktivní, byl například vojenským zpravodajem, a jako šlechtic byl aktivní v politice. Velmi často vystupoval proti špatnému zacházení, až nelidským podmínkám, v belgickém Kongu.

Proslavil se především svými příběhy o Sherlocku Holmesovi. Mimo psaní detektivek se též věnoval psaní historických a fantastických poídek, dramat, románů a též literatuře faktu.

Mezi jeho díla patří například: *Příběhy Sherlocka Holmese*, *Příběhy profesora Challengera* a mnohé další romány, povídky a divadelní hry.

Zdroj: https://en.wikipedia.org/wiki/Arthur_Conan_Doyle

TANČÍCÍ FIGURKY

Tato povídka je jedna z mnoha ve sbírce povídek Návrat Sherlocka Holmese. Celá tato sbírka je v celistvém díle, které nese název *Příběhy Sherlocka Holmese*. Mimo tuto sbírku dílo obsahuje například román *Pes baskervillský*, nebo *Dobrodružství Sherlocka Holmese*.

Tuto povídku jsem vybral, protože obsahuje velmi zajímavou substituční šifru a to, jak název napovídá, tančící figurky. V celé povídce je šifra zásadní klíč k pointě a pochopení celého děje, který se snaží Sherlock Holmes rozluštit a vyřešit tak případ.

Zdroj: https://en.wikipedia.org/wiki/Arthur_Conan_Doyle

DEFINICE ŠIFROVÉHO SYSTÉMU

DEFINICE

Tento šifrovací systém nese název substituční šifrování. U toho typu šifrování je jeden znak otevřeného textu nahrazen jedním znakem šifrové abecedy. Šifrová abeceda může jak jednotlivá písmena v jiném pořadí, nebo i různé speciální znaky, které si autor vymyslí. Tento typ šifrování byl používán pro velmi dlouhou dobu díky jeho oblibě a jednoduchosti, nicméně s rozvojem šifrování jednoduchá substituce (znak za znak) začínala být lehce prolomitelná. Tento systém si udržel svojí oblíbenost a využitelnost, avšak došlo ke stížení šifrování a dešifrování a vzniklo více poddruhů tohoto systému. Tento systém se používá také jako pomůcka, například Morseova abeceda nebo Braillovo písmo.

POJMY

Otevřený text - je text, který ještě neprošel procesem šifrování a je ho možné přečíst

Šifrová abeceda - je to skupina znaků, která slouží k zašifrování otevřeného textu, mohou to být písmena otevřeného textu, čísla, nebo obrazce

Šifrování - proces, při kterém dochází k přeměně otevřeného textu do textu šifrovaného pomocí šifrového systému

Šifrový text - je text, který prošel procesem šifrování a obsahuje určitý systém šifrování

(JANEČEK, 1994, s. 73–76)
(VONDRUŠKA, 2006, s. 29)

POPIS ŠIFROVÁNÍ A DEŠIFROVÁNÍ

ŠIFROVÁNÍ

Zašifrování u jednoduché substice je velmi jednoduché, protože se nahradí jeden znak otevřeného textu za jeden znak šifrovací abecedy. Pro úspěšné zašifrování oteřeného textu je potřeba mít šifrovou abecedu a otevřený text. Pokud má pisatel tyto dvě věci, může začít zprávu otevřeného textu převádět do zašifrovaného textu. Pokud pisatel nezná šifrovou abecedu zpaměti, jde mu šifrování poměrně pomalu, když píše nějakou zprávu, proto se v dnešní době používají různé programy a algoritmy. Tyto programy lehce provedou tento úkon a je to během mžiku.

DEŠIFROVÁNÍ

Dešifrování probíhá téměř stejně, jako šifrování, jen opačným způsobem. Jedná se o převod z šifrovaného textu do otevřeného textu. Pro dešifrování potřebuje příjemce šifry znát šifrovou abecedu (tedy klíč k šifře), nebo šifru podrobit frekvenční analýze a následně ji rozluštit.

(JANEČEK, 1994, s. 73–76)
(VONDRUŠKA, 2006, s. 29–31)

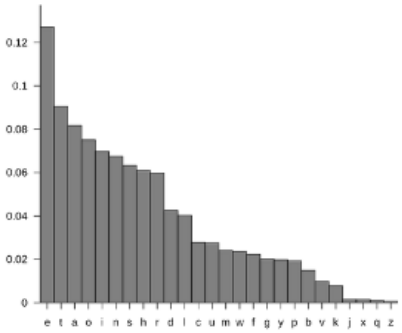
METODY LUŠTĚNÍ

DEFINICE

Metod luštění u tohoto typu šifer je hned několik, avšak nejčastěji používaná je frekvenční analýza znaků. Tato analýza pracuje s tím, že pro každý jazyk je specifická frekvence používání souhlasásek a samohlásek.

FREKVENČNÍ ANALÝZA

Základem pro frekvenční analýzu je znát jazyk, kterým je šifra psána. Následně musí sečíst, kolikrát se daný znak v šifře objeví a z tohoto součtu udělat graf četnosti, viz. graf vpravo. Tento graf je pak nutné porovnat s grafem relativní četnosti znaků konkrétního jazyka. Následuje rozluštění nejčastěji se opakujících znaků a určování členů (typické pro angličtinu). Pomocí tohoto postupu získáváme víc a víc písmen, které nám odkrývají další a další, dokud není šifra zcela rozluštěna.



Relativní četnost znaků (angličtina)

Zdroj: https://en.wikipedia.org/wiki/The_Gold-Bug

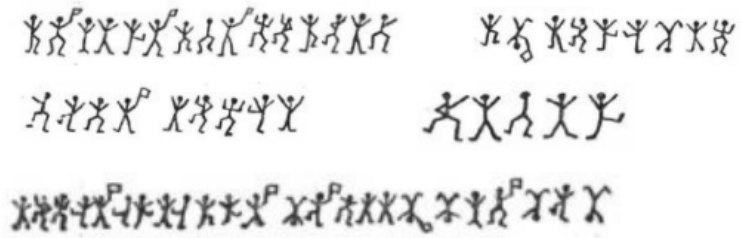
Tato metoda má však jednu nevýhodu, je težce uplatnitelná na krátké texty, kde frekvence znaků nemusí odpovídat grafu.

Tato šifra je poměrně jednoduchá, pro složitější substituce se používají moderní kryptografické programy a různé dešifrovací algoritmy, které šifru rozluští v mžiku.

(JANEČEK, 1994, s. 73–76)
(VONDRUŠKA, 2006, s. 29–31)

ZADÁNÍ PRACOVNÍHO LISTU

ŠIFRA



Zdroj: http://ld.johanesville.net/doyle-03-navrat-sherlocka-holmese?page=3

ZADÁNÍ PRACOVNÍHO LISTU

ŘEŠENÍ

ŠIFRA

Samotná substituční šifra není složitá, avšak samotné rozluštění může být občas trochu problematické, zvláště když nám abecedu nahrazují figurky. Proto jsem zvolil formu řešení odkaz na knihu, kde je postup řešení velmi zdařile popsán, a umožní to tak luštiteli lépe pochopit uvažování autora, který šifru vymyslel.

Řešení je možno nálezt v knize: DOYLE, Arthur Conan. *Návrat Sherlocka Holmese*. Praha 2016, s. 69–76.

Nebo také na:

Odkaz 1

Odkaz 2

METODICKÉ POZNÁMKY

cíle:	žák pomocí indicií rozluští systém šifrování a převede šifrovaný text do textu otevřeného
věková skupina:	15–17
organizace činnosti:	žáci do dvojic dostanou pracovní list, kromě řešení a metodických poznámek.
čas potřebný ke zpracování:	30-45 minut
pomůcky:	psací potřeby, mobilní telefon
reflexe:	skupinová diskuse nad vypracovanými pracovními listy
klíčové kompetence:	kompetence k učení kompetence sociální a personální kompetence k řešení problému
očekávané výstupy:	žák popíše konkrétní způsob, jak k řešení šifry došel
průřezová témata:	Osobnostní a sociální výchova Výchova k myšlení v evropských a globálních souvislostech Multikulturní výchova

ZDROJE

SEZNAM LITERATURY

JANEČEK, Jiří. *Odhalená tajemství šifrovacích klíčů minulosti: ruční šifry*. Praha: Naše vojsko, 1994, 183 s. Mozaika. ISBN 80-206-0462-6.

VONDRUŠKA, Pavel. *Kryptologie, šifrování a tajná písma*. Praha: Albatros, 2006, 340 s. Oko. ISBN 80-00-01888-8.

INTERNETOVÉ ZDROJE

Arthur Conan Doyle [online, cit. 19. 6. 2019], Wikipedia. Dostupné z WWW: <https://en.wikipedia.org/wiki/Arthur_Conan_Doyle>

DOYLE, Arthur Conan. *Návrat Sherlocka Holmese* [online, cit.19. 6. 2019]. Přel. Fr. Jungwirth. V MKP 1. vyd. Praha : Městská knihovna v Praze, 2012. Dostupné z WWW: <http://web2.mlp.cz/koweb/00/03/34/76/82/navrat_sherlocka_holmese.pdf >

Dotazníkové šetření (anonymní)

1. **Jak hodnotíte pracovní list z hlediska jeho atraktivity?**

2. **Co vás na pracovním listu z grafické stránky nejvíce zaujalo?**

3. **Co vám na pracovním listu chybí?**

   3.1. Co naopak přebývá?

4. **Myslíte si, že pro vás byla tato hodina atraktivní?**

4.1. V čem?

5. Jak byste hodnotili názornost výuky? (názornost - všechno bylo jasné, atd.)

6. Byla výuka a práce s pracovním listem srozumitelná?

6.1. Jak se to projevilo?

7. Jaký vidíte největší přínos této hodiny?

7.1. Využili byste někdy v budoucnu šifry? Jak?