Univerzita Hradec Králové
Přírodovědecká fakulta
Katedra kybernetiky

Základy kryptologie jako téma výuky informatiky na 2. stupni ZŠ

Diplomová práce

Autor:	Bc. Sabina Hájková
Studijní program:	N1101 Matematika
Studijní obor:	Učitelství matematiky pro střední školy, Učitelství pro střední školy – informatika
Vedoucí práce:	PhDr. Michal Musílek, Ph.D.

Hradec Králové březen 2017

PROHLÁŠENÍ:

Prohlašuji, že jsem diplomovou práci vypracovala samostatně a že jsem v seznamu použité literatury uvedla všechny prameny, ze kterých jsem vycházela.

V Hradci Králové dne Sabina Hájková

PODĚKOVÁNÍ

Ráda bych poděkovala PhDr. Michalu Musílkovi, Ph.D. za odbornou pomoc, cenné rady a vstřícný přístup během vedení mé diplomové práce. Zároveň bych ráda poděkovala Základní škole Nasavrky za umožnění realizace projektu.

ANOTACE

HÁJKOVÁ, S. *Základy kryptologie jako téma výuky informatiky na 2. stupni ZŠ*. Hradec Králové, 2017. Diplomová práce na Přírodovědecké fakultě Univerzity Hradec Králové. Vedoucí diplomové práce PhDr. Michal Musílek, Ph.D. 74 s.

Cílem diplomové práce je začlenit jednoduché formy šifrování a dešifrování do výuky informatiky na druhém stupni základní školy. První část práce je zaměřena na základní teoretické poznatky z kryptologie, ale i z oblasti různých metod výuky informatiky. Praktická část diplomové práce je rozdělena na empirickou část a tvorbu pracovních listů pro žáky a jejich využití ve výuce. Cílem praktické části je zjistit předpoklady žáků pro zvládnutí zmíněného učiva a popsat přínos základů kryptologie do vyučování. Na závěr jsou shrnuty výsledky šetření, poznatky a zkušenosti spojené s výukou kryptologie a výhody a nevýhody zavedení této problematiky do výuky informatiky.

KLÍČOVÁ SLOVA

kryptologie, šifry, informatika, výuka na ZŠ, aktivizační metody, pracovní listy

ANNOTATION

HÁJKOVÁ, S. *Fundaments of cryptology as teaching topic in subject "Informatics" at lower secondary school*. Hradec Králové, 2017. Diploma Thesis at Faculty of Science University of Hradec Králové. Thesis Supervisor PhDr. Michal Musílek, Ph.D. 74 p.

The object of the Diploma Thesis is the integration of simple forms of encryption and decryption to the subject "Informatics" at lower secondary school. The first part includes the basic theoretical knowledge of cryptology and a range of different teaching methods. The practical part of the Diploma Thesis is divided into the empirical part and creating worksheets for pupils and its utilization in teaching. The object of the practical part is to find out the pupils preconditions for mastering the curriculum and describe the benefits of the fundaments of cryptology for teaching. The final part of the Diploma Thesis summarizes the research results, knowledge and experience related with teaching of cryptology and the advantages and disadvantages of the integration of this issue to teaching "Informatics".

KEYWORDS

cryptology, ciphers, Informatics, teaching at lower secondary school, activation methods, worksheets

OBSAH

ÚVOD

Diplomová práce zčásti navazuje na bakalářskou práci s názvem *Luštění transpozičních šifer s podporou počítače* a problematiku kryptologie pojímá z didaktického hlediska. Cílem diplomové práce je zjistit výhody a nevýhody začlenění základů kryptologie do výuky na druhém stupni základní školy a jak důležitou roli by měla kryptologie hrát ve vzdělávání.

Práce je rozdělena na několik částí, a sice teoretickou, empirickou a praktickou. Cílem teoretické části je podat základní poznatky z oblasti kryptologie v rozsahu, který jsou žáci základní školy schopni zvládnout. V jedné z kapitol je uveden přehled několika typů jednoduchých šifrových systémů, které lze řešit pouze za pomoci tužky a papíru. Teoretická část také pojednává o organizačních formách a metodách výuky a stručně zmiňuje pojem myšlení a jeho rozvoj. Dále je popsán přínos výuky šifrování a možnosti provázání kryptologie s dalšími školními předměty.

Cílem empirické části diplomové práce je provést výzkum na téma *Kryptologie na základní škole* a zjistit, jaké předpoklady mají žáci pro zvládnutí zmíněné problematiky. Tato část je rozdělena do několika podkapitol.

V první kapitole empirické části je stanoven výzkumný cíl, který já následně rozdělen ještě na několik dílčích cílů, na jejichž základě bude probíhat výzkumný proces. V další kapitole jsou vytvořeny domněnky a hypotézy. Kapitola s názvem *Metodika* pojednává o formě a metodách použitých v procesu výzkumu. Je zde také zmínka o výzkumném souboru. Nejrozsáhlejší kapitola uvádí přehled sebraných dat, které jsou navíc převedeny do přehledných tabulek a grafů pro lepší názornost. Nakonec jsou výsledky shrnuty a je provedena jejich následná interpretace.

V rámci praktické části diplomové práce byl připraven a realizován projekt zaměřený na výuku základů kryptologie na druhém stupni základní školy. První kapitola uvádí přípravu hry nazvané *Cesta za pokladem*, jejíž hlavní součástí jsou pracovní listy s úlohami navazujícími na učivo kryptologie. Zahájení hry předchází zmiňovaná výuka základů kryptologie, jejíž přípravě a obsahu je věnována další kapitola. Dále je popsán a zhodnocen samotný průběh výuky a práce a aktivita žáků během vyučování i soutěžení. Poslední kapitola je věnována hodnocení projektu z pohledu samotných žáků. Do projektu byli zapojeni žáci šesté a sedmé třídy Základní školy Nasavrky.

V závěru práce jsou shrnuty poznatky, které čtenář najde v teoretické části, a získané výsledky z empirického šetření. Dále jsou uvedeny postřehy z vyučování a průběhu hry a také zhodnocení projektu a návrhy na jeho vylepšení. Nakonec jsou zdůrazněny výhody a přínosy zavedení kryptologie do výuky informatiky, ale i překážky a nevýhody.

1 TEORETICKÁ ČÁST

První část diplomové práce se bude zabývat teorií, která je nezbytná pro realizaci výuky kryptologie. První kapitoly této části se zaměří na výuku z pedagogického hlediska, a sice na organizační formy a metody výuky, ale také na možnosti rozvoje myšlení žáků.

Další kapitoly se budou již soustředit na odbornou stránku zmiňované výuky. Cílem těchto kapitol bude seznámit čtenáře se základními pojmy z oblasti kryptologie a uvést stručný přehled různých typů jednoduchých šifer, které lze řešit metodou „tužka a papír".

V neposlední řadě se zaměříme na roli kryptologie ve výuce informatiky, a tedy na důvody zařazení kryptologie do výuky, přínosy výuky kryptologie, mezipředmětové vztahy, apod.

1.1 Formy a metody výuky

Následující kapitoly se budou zabývat definicemi a klasifikací organizačních forem a metod výuky. V každé podkapitole budou uvedeny klasifikace více autorů, přičemž větší pozornost bude věnována členění uvedenému v knize Školní didaktika (Kalhous, Obst a kol., 2009). Zmíněné typy budou stručně popsány, podrobněji se budeme věnovat těm typům organizačních forem a metod, které jsou úzce spjaty s výukou kryptologie. Jedna podkapitola bude věnována aktivizačním metodám.

1.1.1 Organizační formy výuky

Pojem **organizační forma výuky** je definován jako organizace vyučovacího procesu, tedy uspořádání činností žáka a učitele ve vyučování, kde mimo jiné hraje důležitou roli čas a prostor. (Zormanová, 2014)

Vladimír Václavík (Kalhous, Obst a kol., 2009) uvádí následující klasifikaci organizačních výukových forem:

- Individuální výuka
- Hromadná (frontální) výuka
- Individualizovaná výuka
- Diferencovaná výuka
- Skupinová a kooperativní výuka
- Projektová výuka
- Otevřené vyučování
- Týmová výuka

Individuální výukou je označována organizační forma, při které se učitel věnuje každému žáku jednotlivě. To znamená, že každý žák má své vlastní individuální učivo a pracuje vlastním tempem. Žáci jsou věkově i vědomostně na různých úrovních

a nespolupracují, i když mohou být shromážděni v jedné místnosti. Toto uspořádání se hojně využívá při doučování nebo umělecké výchově. (Zormanová, 2014)

Nejvyužívanější organizační formou v praxi je **hromadná výuka**. Při této výuce jsou v jedné místnosti shromážděni žáci přibližně stejné věkové i mentální úrovně. Učitel vede činnost všech žáků najednou a žáci plní stejné úkoly a požadavky ve stejném čase. Výuka probíhá v jednotlivých vyučovacích hodinách. (Kalhous, Obst a kol., 2009)

Jako reakce na nevýhody hromadné výuky (přehlížení individuálních dispozic, potřeb a zájmů jednotlivých žáků) vznikla **individualizovaná výuka**, která spočívá v individuálním přístupu k žákům i během hromadné výuky na základě rozlišení výukových metod a cílů. V důsledku individualizace výuky vzniklo několik reformních pedagogických směrů, například daltonský plán. (Zormanová, 2014)

Při **diferencované výuce** dochází k **diferenciaci**, tedy k vytvoření homogenních skupin podle určitých kritérií, například podle intelektové úrovně žáků, podle zájmů, apod. Rozlišujeme vnější diferenciaci, při které jsou nadanější žáci oddělováni od ostatních (například víceletá gymnázia, paralelní třídy, …), a vnitřní diferenciaci, kdy dochází k utvoření skupin během výuky, a tedy spolu pracují žáci různého nadání. Díky takovému roztřídění je pak možné přistupovat k žákům individuálně. (Kalhous, Obst a kol., 2009)

Skupinová výuka je založena na práci žáků v menších skupinkách, kde většinou žáci spolupracují na řešení nějakého úkolu či problému. Během této výuky se učitel dostává do role pomocníka a dohlíží na to, aby skupina pracovala efektivně. Velikost skupin bývá volena libovolně podle typu činnosti, kterou skupina bude provádět, jako vhodný počet se udává 3 – 5 žáků, avšak i dvojice je již považována za skupinu. Složení jednotlivých skupin může určit učitel, ale i sami žáci. Skupiny mohou být tvořeny na základě různých kritérií, například podle prospěchu, nadání, zájmů, komunikačních schopností, atd. Zormanová (2014) uvádí dělení na homogenní a heterogenní skupiny. Ve skupině homogenní spolupracují žáci s podobným prospěchem a přibližně stejnou vědomostní úrovní, což může vést k rozvoji nadanějších žáků a posílení sebevědomí a motivace u slabších žáků. Heterogenní skupina je tvořena žáky různých prospěchů a úrovní intelektových schopností. Takové rozložení vede v dobrém případě k efektivní spolupráci a vzájemné pomoci žáků ve skupině. Velký důraz se také klade na rozvoj komunikačních a kooperativních schopností během práce ve skupinách.

Organizační výuková forma s názvem **projektová výuka** je charakterizována jako výuka, při které žáci pracují na nějakém rozsáhlém komplexním projektu. Projekt se vyznačuje časovou náročností, měl by být úzce spjat s praxí a skutečným životem, měl by prostupovat napříč různými předměty a obory. Žáci by si během výzkumu a práce na projektu měli osvojovat nové poznatky a získávat nové vědomosti. K vypracování projektu by měla žáky vést motivace, projekt by tedy měl vycházet z jejich potřeb a zájmů, žáci by měli dospět ke konkrétním výsledkům. K projektu lze přistupovat skupinově, ale i individuálně. Prací na projektu se žák učí nést zodpovědnost, učí se spolupracovat i jednat samostatně, učí se tvořivě a kriticky myslet a řešit problémy. U skupinových projektů se rozvíjejí žákovy komunikační schopnosti a sociální

dovednosti, neboť musí spolupracovat s ostatními členy skupiny, respektovat jejich názory, učí se argumentovat, ale i přiznat vlastní chyby, atd.

Příprava a organizace projektu je pro učitele velmi časově náročná. V průběhu žákovské práce se ale učitel stává spíše poradcem. Velmi obtížné je i celkové hodnocení projektu, neboť žáci při tvorbě musí sami rozhodovat o své činnosti, plánovat a volit vhodné postupy a metody tak, aby dosáhli očekávaných výsledků. (Černochová a kol., 1998) Projekty můžeme členit podle různých kritérií, například podle velikosti týmu, časové náročnosti, prostředí, ve kterém projekt probíhá, podle odborného zaměření a dalších kritérií.

Otevřeným vyučováním se rozumí organizační forma, která vede žáky k samostatné individuální práci. Znamená to ale také otevírání školy pro veřejnost, a sice pro rodiče, obyvatele obce, různá zájmová sdružení, apod. V otevřeném vyučování děti postupují podle týdenního plánu, v jehož rámci řeší různé úkoly. Tyto činnosti provozují v blocích nazvaných **volné práce**. Zmiňovanému způsobu výuky jsou vhodně přizpůsobeny i učebny a učební pomůcky. (Kalhous, Obst a kol., 2009)

Princip **týmové výuky** spočívá ve spolupráci několika učitelů, kteří se podílejí na práci s různými skupinami žáků, ať už v rámci tříd nebo nějakých seminárních aktivit. Toto uspořádání se v České republice vyskytuje hlavně na vysokých školách.

Někteří autoři uvádějí ještě další klasifikace organizačních forem výuky. Například Josef Maňák (2003) člení organizační formy podle několika hledisek:

- Hledisko vztahu k osobnosti žáka
    - Individuální výuka
    - Individualizovaná výuka
    - Skupinová výuka
    - Hromadná výuka
- Hledisko výukového prostředí
    - Výuka v klasické třídě
    - Výuka v odborných učebnách a laboratořích
    - Výuka v dílně a na školním pozemku
    - Exkurze a návštěvy kulturních akcí
    - Domácí úlohy
- Hledisko délky trvání
    - Vyučovací hodina
    - Zkrácená vyučovací jednotka
    - Dvouhodinová výuka
    - Přednášky, semináře, kurzy, workshopy, …

1.1.2 Vyučovací metody

Každý typ organizační formy zastřešuje vyučovací metody a prostředky, které jsou pro danou organizační formu vhodné. Josef Maňák (2003) definuje **vyučovací metodu** jako *„koordinovaný systém vyučovacích činností učitele a učebních aktivit žáků, který je*

zaměřen na dosažení výchovně vzdělávacích cílů", metodou tedy rozumíme cestu k nějakému cíli.

Zdeněk Kalhous (2009) ve své knize popisuje klasifikaci výukových metod podle I. J. Lernera:

- Reproduktivní metody
    - Informačně-receptivní metoda
    - Reproduktivní metoda
- Metoda problémového výkladu
- Produktivní metody
    - Heuristická metoda
    - Výzkumná metoda

Nejrozšířenější vyučovací metodou je **informačně-receptivní metoda**, jejíž podstatou je podávání hotových poznatků žákům na základě prezentování, vysvětlování, popisování, práce s textovým a obrazovým materiálem, apod. Předpokládá se, že žáci si takto podané informace zapamatují a porozumí jim. Mělo by se však dbát na to, že každý žák má rozdílné dispozice a vlastnosti, díky čemuž by se mělo přizpůsobit tempo a způsob předávání informací.

S informačně-receptivní metodou úzce souvisí **reproduktivní metoda**, která spočívá v opakování určité činnosti za účelem osvojení si daných vědomostí a dovedností. Opakování může probíhat formou řešení série úloh, ústního zkoušení, prověrek, čtení, tvorby určitého produktu, atd.

Metoda problémového výkladu je považována za přechodnou mezi reproduktivními a produktivními metodami. Základem této metody je řešení úkolu, problému, na který žáci neumí odpovědět. Při postupném řešení si žáci za pomoci učitele osvojují nové poznatky a zvnitřňují si obecný postup řešení problémů (pochopení podstaty problému, hledání možností řešení, výběr a realizace řešení, ověření správnosti).

Heuristická metoda navazuje na předchozí metodu, protože pro její efektivní uplatnění je důležité, aby žáci měli osvojeny jednotlivé kroky a fáze řešení problémů. Žákům jsou zadávány takové úlohy a otázky, které v nich vyvolávají potřebu hledat řešení a přijít problému na kloub. Činnost učitele a žáků by měla být vyrovnána.

Podstata **výzkumné metody** tkví ve snaze samostatně řešit problémy, žáci při hledání správných řešení a postupů aplikují vlastní znalosti a dovednosti. Rolí učitele je pouze konstrukce vhodných úloh. (Kalhous, Obst a kol., 2009)

Uvedeme ještě klasifikaci výukových metod podle Maňáka (2003):

- Aspekt didaktický (zdroje poznání a typy poznatků)
    - Slovní metody
        - Monologické metody
        - Dialogické metody
        - Metody písemných prací
        - Metody práce s učebnicemi a knihami

    - Názorně-demonstrační metody
        - Pozorování
        - Předvádění
        - Demonstrace statických obrazů
        - Statická a dynamická projekce
    - Praktické metody
        - Nácvik pohybových a pracovních dovedností
        - Žákovské laborování
        - Pracovní činnosti
        - Grafické a výtvarné činnosti
- Aspekt psychologický (aktivita a samostatnost žáků)
    - Sdělovací metody
    - Metody samostatné práce žáků
    - Výzkumné a badatelské metody
- Aspekt logický (myšlenkové operace)
    - Srovnávací postup
    - Induktivní postup
    - Deduktivní postup
    - Analyticko-syntetický postup
- Aspekt procesuální (fáze výchovně vzdělávacího procesu)
    - Motivační metody
    - Expoziční metody
    - Fixační metody
    - Diagnostické metody
    - Aplikační metody
- Aspekt organizační (výukové formy a prostředky)
    - Kombinace metod s výukovými formami
    - Kombinace metod s výukovými pomůckami

1.1.3 Aktivizační metody

Aktivizační metody jsou založené na řešení problémových úloh. Jak už název napovídá, jedná se o metody, které mají podněcovat žákovskou aktivitu, rozvíjet jejich tvořivé, kritické a samostatné myšlení. Vyznačují se silnou motivační tendencí. Role učitele ve vyučování ustupuje do pozadí, avšak příprava na takovou výuku je velmi časově i organizačně náročná. (Maňák, 2003)

Aktivizačních metod je nepřeberné množství, jedno z možných členění je následující (Zormanová, 2014):

- Diskusní metody
- Heuristické metody, řešení problémů
- Situační metody
- Inscenační metody

- Didaktické hry

V rámci **diskusních metod** je veden rozhovor či debata na určité téma mezi žákem a učitelem i mezi žáky navzájem. Žáci (účastníci diskuse) vznášejí své názory a na základě argumentů se společně snaží zaujmout určité stanovisko k danému tématu a dojít k nějakému řešení. Žáci se díky diskusím a rozhovorům učí komunikovat, argumentovat, respektovat názory druhých lidí, zamýšlet se nad vlastním stanoviskem k určitým tématům. Důležité je, aby debata byla dobře vedena, aby všichni účastníci měli možnost se vyjádřit, aby během diskuse docházelo ke kultivaci společenských mravů a chování (neskákat do řeči, učit se aktivně naslouchat, neodsuzovat, …). (Zormanová, 2014)

Jak již bylo řečeno výše, **heuristické metody** spočívají v objevování a hledání vhodných postupů k řešení úloh a problémů či projektů na základě dříve získaných poznatků a vědomostí.

Situační metody přibližují žákům řešení konfliktních situací z reálného života. Je ale důležité, aby žáci měli dostatek informací a poznatků na dané téma a problém přibližně odpovídal jejich mentální úrovni, aby byli schopni situaci porozumět a hledat adekvátní řešení.

Zařazení **inscenačních metod** do výuky znamená seznamovat se s řešením různých problémů, situací a životních rolí formou představení a scének s výchovně vzdělávacím podtextem. Hry a scénky mohou být řízené scénářem či nikoli. Žáci si díky podobným metodám rozvíjejí kreativní myšlení, představivost, sociální i komunikační dovednosti. Inscenační metody by však měly být do výuky zařazovány za jistým výchovným účelem, nikoli pouze pro pobavení a zábavu. (Maňák, 2011)

Didaktickou hrou je myšlena hra, činnost nebo nějaká aktivita, která sleduje nějaký výchovně vzdělávací cíl. Řadíme mezi ně různé hádanky, skládačky, společenské hry, hry s matematickým podtextem, manipulace s předměty a mnoho dalších. Didaktické hry mají silný motivační a aktivizující charakter, přispívají k rozvoji tvořivého, logického myšlení, soutěživosti, na jejich základě mají děti možnost lépe uchopit probírané učivo a porozumět mu do větší hloubky. Využití a pravidla didaktických her musí být však dobře promyšlena, aby hra neztrácela svůj účel. (Zormanová, 2014)

Josef Maňák (2011) ve svém článku řadí mezi aktivizační metody ještě například práci s textem, mentální mapování, skupinové metody a další.

1.2 Myšlení a jeho rozvoj

Myšlením je chápán poznávací proces, který umožňuje poznávat podstatné znaky, rysy a vlastnosti předmětů a jevů, umožňuje zpracovávat v paměti uložené vjemy a informace a konstruovat souvislosti mezi nimi a na jejich základě řešit problémy. (Chytrý, 2015)

S myšlením souvisejí ještě jeho tři základní produkty, a sice pojem, soud a úsudek. Jestliže známe nějaký **pojem**, známe jeho význam, tedy obecné vlastnosti a znaky

určitého předmětu či jevu, který je pojmem vyjádřen. Jednotlivé pojmy lze mezi sebou porovnávat a hledat mezi nimi vztahy a souvislosti, tyto vztahy nazýváme **soudy.** Hledáním vztahů mezi soudy docházíme k určitým závěrům, tedy **úsudkům**. (Juklová, 2012)

Myšlení je proces, který se člověk musí učit. Dítě v určitém věku ještě nemá tolik rozvinutý paměťový aparát, aby mohlo nové informace a poznatky získávat na základě myšlenkových operací, a proto si napomáhá pomocí názorných modelů (např. počítání na prstech) a přímým poznáváním. Myšlení a uvažování u dětí prochází několika vývojovými změnami. Chytrý ve své knize (2015) uvádí rozdělení do následujících stádií:

1. **Senzomotorické stádium** (0 – 2 roky) – dítě chápe svět a realitu zkresleně na základě vlastních potřeb
2. **Předoperační stádium** (2 – 7 let) – u dítěte se začíná rozvíjet představivost, schopnost uvědomění si sebe sama, rozvíjí se symbolické myšlení
3. **Stádium konkrétních operací** (7 – 11 let) – rozvoj logického myšlení, užívání logických úsudků a operací, avšak založených na konkrétních představách
4. **Stádium formálních operací** (12 a více let) – v myšlení dochází ke zdvihu od konkrétních modelů k abstraktním myšlenkám, dítě je schopno argumentovat

Učení se novým věcem, objevování a získávání nových poznatků, osvojování si nových dovedností, nových postupů jak řešit problémy by se neobešlo bez **tvořivého myšlení.** Člověk s vysokou tvořivostí dokáže na věci a situace nahlížet ze široka a objevovat tak další souvislosti, možnosti a informace, nejen ty potřebné. (Fisher, 1997)

Je jasné, že při automatickém uplatňování známých poznatků a vědomostí a rutinním používání postupů a algoritmů (např. různé matematické algoritmy) není tvořivé myšlení potřeba, tudíž se ani nerozvíjí. Pro rozvoj tvořivosti však existuje nepřeberné množství úloh, nástrojů a cvičení. Ve své publikaci Fisher (1997) popisuje například cvičení, při kterém žáci hledají možné činitele a okolnosti, které jsou potřebné při rozhodování v daných situacích. V dalším cvičení se žáci zase učí určovat priority a činitele, které jsou důležitější než ostatní, nebo konstruovat pozitiva a negativa určitého jednání, uvědomovat si následky činů, přemýšlet o dalších možnostech a podobně. Aby si žáci takové způsoby uvažování a rozhodování zvnitřnili a naučili se napřed o svých činech a jednání přemýšlet, musí se se zmiňovanými aktivitami a cvičeními setkávat pravidelně.

Proces myšlení, při kterém jedinec na základě svých úsudků, myšlenek a poznatků dochází k nějakému závěru či výsledku, se nazývá **logické myšlení**. Aby byl člověk schopen logicky uvažovat, musí se umět odpoutat od konkrétních modelů a myslet na abstraktní úrovni. (Chytrý, 2015) Logické myšlení je také spjato s **matematickým myšlením**, to je ale rozšířeno ještě o znalost matematických pojmů, algoritmů, vzorců, matematických dovedností, chápání čísel, atd.

K rozvoji logického i matematického myšlení lze opět nalézt obrovské množství úloh a aktivit, například manipulace s předměty a různými materiály, hledání vlastností,

srovnávání, experimenty, práce s textovým a obrazovým materiálem, učení se argumentovat, hrátky s pojmy, různé didaktické hry a další.

1.3 Základy kryptologie

V následujících dvou podkapitolách budou uvedeny základní pojmy, které je třeba znát pro práci s šiframi, a několik jednoduchých typů šifer, které lze řešit metodou tužka a papír a budou využity při výuce základů kryptologie na základní škole.

Informace a poznatky uvedené v těchto kapitolách se budou odrážet od mé bakalářské práce (Hájková, 2015), která se zabývala problematikou kryptologie, a tudíž pojmy a způsoby šifrování již byly v práci podrobněji rozebrány.

1.3.1 Základní pojmy

Nejzásadnějším pojmem v oblasti utajování informací je samozřejmě **kryptologie**, tedy nauka o šifrování. Kryptologie se dále dělí na tři obory, a sice kryptografii, steganografii a kryptoanalýzu.

Kryptografie, jejíž název byl odvozen od slova *kryptos* neboli *skrytý*, zahrnuje soubor metod a způsobů, které umožňují upravit text tak, aby byl pro nepovolaného člověka zcela nesrozumitelný. Taková úprava textu se děje na základě šifrování, tedy pomocí určitých pravidel, na kterých se domluví odesílatel i příjemce tajné zprávy, se změní podoba textu. Kryptografie se ale také zabývá informační bezpečností a ověřováním a zkoumáním vlastnictví dat. (Vondruška, 2006) Jednoduchými šifrovými systémy se budeme podrobněji zabývat v další kapitole.

Ze dvou řeckých slov *steganos* (schovaný) a *graphein* (psát) vznikl pojem s**teganografie**, což je označení pro obor zabývající se utajováním samotné existence tajných zpráv. Text zprávy sám o sobě však může zůstat beze změny, nemusí být žádným způsobem šifrován, cizí člověk ale nesmí poznat, že zpráva vůbec existuje. Mezi nejznámější steganografické metody patří například psaní neviditelným inkoustem. Neviditelných inkoustů bylo vynalezeno mnoho, mezi ty nejjednodušší a nejdostupnější patří například mléko, citronová šťáva, ocet nebo kostka cukru rozpuštěná ve lžíci vody, napsaný text potom stačí jenom nahřát a zpráva se objeví. Mezi dětmi je také oblíbený UV fix, zprávu psanou tímto fixem si lze přečíst pod UV světlem. Na obrázku 1 je zviditelněný tajný text psaný různými neviditelnými inkousty.

Text zprávy ale také můžeme schovat do jiného textu (novinového článku, nákupního seznamu, dopisu, …) jednoduše tak, že změníme font či velikost u písmen, které dohromady tvoří tajný text, nebo jednotlivá písmenka propíchneme špendlíkem, apod. (Pelánek, 2014) Mezi jednotlivá písmena tajné zprávy můžeme také vkládat nějaké heslo nebo lze číst pouze první písmena na začátků řádků, možností je opravdu mnoho. Tajnou zprávu nebo heslo můžeme ukrýt i do obrázku; v podobě mikrotečky nebo můžeme barvu textu změnit tak, aby splývala s okolím.

Obrázek 1 - Užití neviditelných inkoustů

Posledním odvětvím kryptologie je **kryptoanalýza,** kterou bychom mohli definovat jako opak kryptografie, neboť se zabývá luštěním tajných zpráv a analýzou odolnosti šifrových systémů. (Vondruška, 2006) Kryptoanalytici se tedy snaží zjistit obsah tajné zprávy i přes to, že neznají klíč ani pravidla, kterými byl text zašifrován. Pro úspěšné luštění je nutná vynikající znalost jazyka, trpělivost a znalost principů šifrování.

Další pojmy, které je nutno znát, se již týkají samotné práce s šiframi. Patří sem jistě pojem **šifra** nebo také **šifrovací systém**, jímž chápeme způsob utajení obsahu zprávy, například pomocí záměny písmen za jiná písmena, číslice nebo symboly.

Od šifry rozlišujeme pojem **kód**, kterým označujeme nějaké slovo (heslo), číslo nebo symbol pro nahrazení jiného slova nebo skupiny slov, například kód *ucho* pro příkaz *poslouchej*. **Kódováním** rozumíme převod textu do podoby vhodné pro vysílání elektrických, zvukových či optických signálů. Nejedná se o šifru, protože kódy jsou veřejně známé a zakódovaný text lze snadno zase převést zpět do původní podoby. Mezi nejznámější kódovací systémy patří Morseova abeceda (systém teček a čárek) nebo binární kód (znaky 0 a 1 pro uložení dat do počítače).

Text psaný v běžné abecedě, který je zcela srozumitelný, se nazývá **otevřený text.** Jedná se o text, který chceme zašifrovat. Po zašifrování otevřeného textu získáme pro oko běžného člověka nesrozumitelný **šifrový text**, který se jeví jako náhodná kombinace znaků. Postup vytváření šifrového textu nazýváme **šifrovací algoritmus.**

Šifrování se neobejde bez tajného **klíče**, tímto slovem označujeme pravidla, na jejichž základě probíhá šifrování. Klíč udává například, jakými znaky budeme nahrazovat písmena otevřeného textu nebo jaké heslo má být při šifrování použito nebo o kolik písmen se má posunout šifrová abeceda a podobně. Tajný klíč musí znát odesílatel i adresát a musí být bezpečně utajen. Bez šifrového klíče by totiž byly šifrovací systémy snadno prolomitelné.

Převádění otevřeného textu za pomoci klíče a šifrovacího algoritmu na šifrový text označujeme jako **šifrování**. Převod šifrového textu za pomoci klíče a opačného

šifrovacího algoritmu na otevřený text nazýváme **dešifrování**. Útočník, který šifru prolomil, to znamená, že dokázal přečíst obsah zprávy i bez znalosti klíče a pravidel, provedl **luštění.**

Při každém šifrování zbavíme otevřený text diakritiky a mezer a pracujeme s velkými písmeny (pro usnadnění práce a snahu zmást útočníka). Výsledný šifrový text lze ještě pro větší bezpečnost rozdělit do skupin po pěti znacích.

1.3.2 Přehled jednoduchých šifer

Podle způsobu šifrování rozlišujeme substituční a transpoziční šifry. Princip **substitučních šifer** spočívá v nahrazování znaků otevřeného textu za znaky šifrové abecedy, která se může skládat buď z písmen, číslic nebo různých symbolů. Záměna znaků může probíhat různými způsoby a podle různých pravidel, všechna písmena otevřeného textu lze šifrovat pomocí jediné šifrové abecedy nebo každé písmeno můžeme zašifrovat pomocí jiné abecedy a podobně.

Substituční šifra, která je založená na pouhém zaměňování znaků, se nazývá **jednoduchá záměna**, při níž je využita vždy jen jedna šifrová abeceda. Pro usnadnění se používá převodová tabulka, v jejímž prvním řádku jsou znaky otevřeného textu (tedy obyčejná abeceda) a v druhém řádku jsou zapsány odpovídající znaky šifrové abecedy. Na obrázku 2 je uvedeno několik převodových tabulek s různými šifrovými abecedami, například obrácená abeceda (A), taková substituční šifra se nazývá atbaš, dále náhodně uspořádaná abeceda (B), šifrová abeceda začínající heslem a doplněná zbývajícími písmeny v abecedním pořadí (C), abeceda posunutá o čtyři znaky doleva (D) či šifrová abeceda složená z kombinace čísel (E) nebo symbolů (F). Možností, jak vytvořit šifrovou abecedu, je velké množství, vše záleží na dohodě účastníků tajné komunikace.

A

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

B

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

C

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

D

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

E

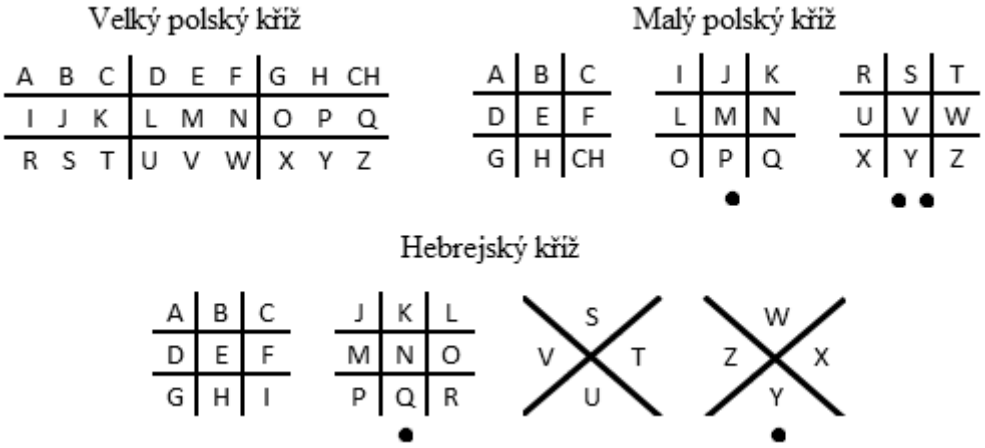
OT:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
ŠA:	12	21	13	31	23	32	14	41	24	42	34	43	15	51	25	52	35	53	45	54	11	22	33	44	55	0

F

OT:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
ŠA:	♋	♌	♍	♎	♏	♐	♑	♒	♓	✔	☠	☾	♥	🔒	📅	✖	🚗	ⓘ	✂	✈	✦	!	?	✉	☠	⌘

Obrázek 2 - Ukázky převodových tabulek

Následující typ substituční šifry bývá někdy nazýván jako **zednářská šifra** nebo **šifra podle kříže**. Zednářská se nazývá proto, že tuto šifru využívali svobodní zednáři k utajování svých záznamů. (Vondruška, 2006) Výstižnější je však druhý název, neboť napovídá, že k šifrování se používají kříže, které je možné vidět na obrázku 3. I když kříže lze vytvořit libovolně různými způsoby, nejznámější jsou tři šifrové systémy, a sice Velký polský kříž, Malý polský kříž a Hebrejský kříž.



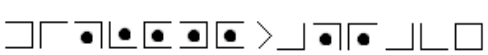
Obrázek 3 - Zednářské kříže

Samotné šifrování spočívá v záměně písmen otevřeného textu za grafické znaky tvořené „chlívkem“ a tečkou, které udávají pozici daného písmene. U Velkého kříže bude znak vždy tvořit chlívek a tečka na jedné ze tří pozic, znaky Malého kříže bude tvořit buď samotný chlívek, nebo chlívek s jednou či dvěma tečkami podle toho, ve kterém kříži se písmeno nachází (tečky naznačeny v obrázku 3). Oba zmiňované systémy obsahují i písmenko CH. Hebrejský kříž je složen ze dvou křížů Malého kříže a dvou zcela odlišných, které obsahují pouze čtyři znaky, tento systém písmeno CH zanedbává. Šifrová abeceda je opět tvořena odpovídajícími chlívky a tečkami.

Jako příklad uvedeme text *Diplomová práce* zašifrovaný všemi třemi uvedenými systémy:

VK: 

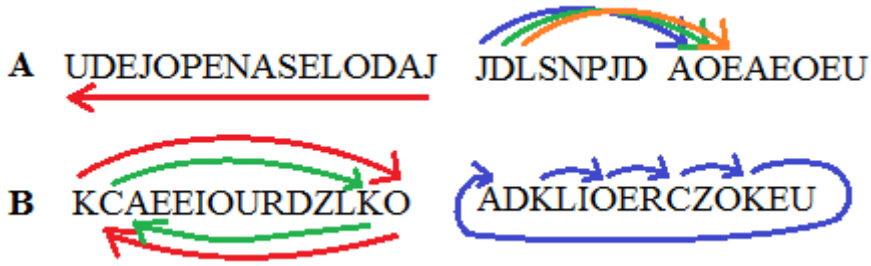
MK: 

HK: 

Tyto šifrovací systémy jsou ale veřejně známé, a tudíž velmi snadno luštitelné. Odesílatel s adresátem by se však mohli domluvit na tajném klíči, to znamená, že by mohli například jinak uspořádat abecedu v kříži, tečky znázorňovat u jiného kříže, než je běžné, nebo si vymyslet vlastní odlišnou podobu křížů či značení.

Na rozdíl od substitučních šifer spočívá princip **transpozičních šifer** ve změně pořadí znaků otevřeného textu, která se řídí určitými pravidly. Počet a tvar znaků šifrového textu je tedy stejný jako v textu otevřeném.

Mezi nejjednodušší transpozice se řadí systémy, které pracují pouze s připraveným řádkem pro šifrový text. Do této kategorie spadá například text psaný pozpátku či zápis otevřeného textu střídavě na přední a zadní pozice připraveného řádku, psaní textu na každou třetí pozici řádku a další systémy. Obrázek 4 ukazuje některé možnosti, jak pomocí jednoduchých transpozic zašifrovat věty *Já do lesa nepojedu* (A) a *Kočka leze dírou* (B).



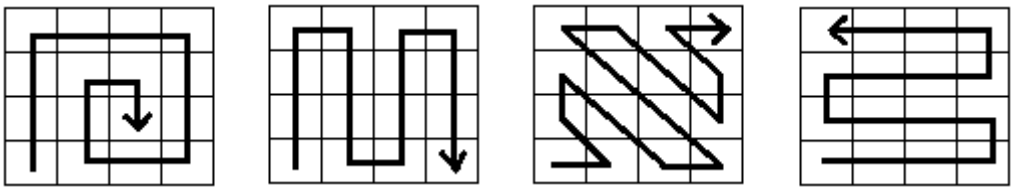
Obrázek 4 - Jednoduché transpoziční systémy

Ke změně pořadí znaků otevřeného textu se většinou používají tabulky. Možností, jak s takovou tabulkou pracovat, je spousta. Oblíbeným způsobem je šifra **podle plotu**. Otevřený text zapisujeme do tabulky o dvou či více řádcích „podle plotu“ (viz tabulka 1). Šifrový text potom čteme po řádcích: HELTY LDJOE SUNEK MD.

Tabulka 1- Šifrový systém podle plotu

H				E				L				T				Y
	L		D		J		O		E		S		U		N	
		E				K				M				D		

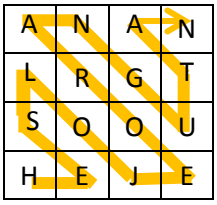
Dalším příkladem tabulkové transpozice je zápis znaků tajné zprávy do tabulky podle dohodnutého směru, například po spirále, po diagonále, po sloupcích a podobně. Obrázek 5 znázorňuje některé z mnoha možností. Šifrový text opět čteme po řádcích.



Obrázek 5 - Některé z možností zápisu textu do tabulky

Pro představu zašifrujeme pomocí tohoto systému text *heslo je orangutan*. Z počtu znaků otevřeného textu plyne, že je třeba připravit tabulku 4 x 4. Písmena zprávy do ní zapíšeme směrem, který se na obrázku 5 nachází na třetí pozici zleva (viz tabulka 2). Šifrový text čteme po řádcích: ANANL RGTSO OUHEJE.

Tabulka 2 - Šifrovací tabulka



Adresát po obdržení tajné zprávy napíše jednotlivá písmena po řádcích do připravené tabulky a podle předem dohodnutého směru si přečte pravý obsah zprávy.

Tabulku využívá i šifra s názvem **jednoduchá sloupcová transpozice**, která je však poněkud složitější než dosud uvedené šifrové systémy a navíc obsahuje tajný klíč, tedy heslo. Počet znaků domluveného hesla udává počet sloupců v tabulce. Počet řádků je dán délkou zprávy, kterou chceme zašifrovat.

Prvním krokem je permutační vyčíslení hesla, tj. přiřazení číslic každému znaku hesla podle abecedního pořadí. Pokud se v heslu vyskytuje některé písmeno vícekrát, nižší hodnotu má ten znak, který se vyskytuje jako první. Takto získané permutační vyčíslení zapíšeme do záhlaví tabulky. Nakonec napíšeme do jednotlivých řádků otevřený text zprávy zbavený diakritiky a mezer. Výsledný šifrový text čteme po sloupcích od 1 do *n*, kde *n* je počet sloupců. Otevřený text se může do tabulky vejít beze zbytku nebo mohou vzniknout volná políčka. Pokud volná políčka zaplníme náhodnými znaky (nejčastěji písmeny X, W, Q), říkáme, že šifrujeme pomocí **úplné tabulky**. Pokud však necháme políčka prázdná, využíváme **neúplnou tabulku**, která je mnohem bezpečnější, protože protivník bude mít problém s určením velikosti tabulky a s určením počtu sloupců, které jsou kratší.

Pomocí sloupcové transpozice zašifrujeme text: *Tak dlouho se chodí se džbánem pro vodu, až se ucho utrhne*. Jako heslo použijeme slovo *hlavolam*. Tabulka 3 představuje šifrovací tabulku s heslem a permutačním vyčíslením v záhlaví a po řádcích vepsaným otevřeným textem. Pro šifrování byla vybrána úplná tabulka, proto byla poslední dvě prázdná políčka vyplněna znaky X a Q.

Tabulka 3 - Šifrovací tabulka jednoduché sloupcové transpozice

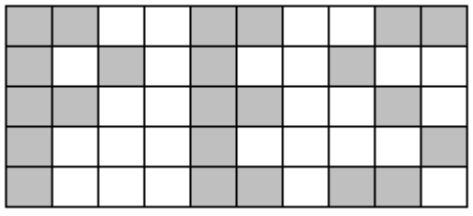
H	L	A	V	O	L	A	M
3	4	1	8	7	5	2	6
T	A	K	D	L	O	U	H
O	S	E	C	H	O	D	I
S	E	D	Z	B	A	N	E
M	P	R	O	V	O	D	U
A	Z	S	E	U	C	H	O
U	T	R	H	N	E	X	Q

Nyní stačí jen vypsat sloupce podle permutačního vyčíslení a získáme šifrový text, který ještě rozdělíme do skupin po pěti znacích: KEDRS RUDND HXTOS MAUAS EPZTO OAOCE HIEUO QLHBV UNDCZ OEH.

Příjemce zprávy musí při dešifrování nejprve spočítat počet znaků šifrového textu a vydělit ho počtem písmen předem domluveného hesla, tak získá rozměry tabulky. Do záhlaví připravené tabulky si opět napíše permutační vyčíslení hesla, na jehož základě vepisuje do tabulky po sloupcích šifrový text. Obsah zprávy si adresát přečte v řádcích tabulky.

Radek Pelánek (2014) do své knihy zahrnul ještě **grafické šifry**, jež nenesou přímo obsah zprávy, ale naznačují cestu, jak ho vykreslit či graficky znázornit. Takové šifry jsou určeny spíše pro rekreační použití. Výhodou těchto šifer je široká škála možností, jak zprávu zašifrovat, vše totiž závisí na tvořivosti a představivosti účastníků komunikace. Pro nezkušené luštitele mohou takto zašifrované zprávy být tvrdým oříškem.

Jedním z mnoha příkladů grafických šifer je například vybarvování mřížky. Příjemce zprávy dostane kombinaci číslic nebo písmen, což jsou odkazy na jednotlivá políčka mřížky. Odkazovaná políčka stačí vybarvit či nějakým způsobem zvýraznit a tajný text se odkryje. Na obrázku 6 jsou uvedeny dvě možnosti zakódování slova *pes*.



1A 1B 2A 2C 3A 3B 4A 5A
1E 1F 2E 3E 3F 4E 5E 5F
1I 1J 2H 3I 4J 5H 5I

11 12 21 23 31 32 41 51
11 12 21 31 32 41 51 52
12 13 21 32 43 51 52

Obrázek 6 – Slovo zakódované pomocí vybarvování mřížky

Takto můžeme zakódovat například heslo, pomocí něhož jsme zašifrovali tajnou zprávu, a jeho kód poslat spolu s šifrovým textem, aby příjemce byl schopen zprávu dešifrovat.

Tajnou informaci můžeme zašifrovat také pomocí šipek, které adresátovi napovídají, jakým směrem vést tužku, aby vykreslil požadovaný obsah zprávy (viz obrázek 7): ↑↑→↓← | ↑↑→↓↓← | ↑↑↘↙ | ↑↑→↓← | ↗↗↘←→↘ | ↑↑→↓←↘ | ←↑→←↑→ | ←↗↗← | ←↑→←↑→ | ↑↑↘↗↓↓

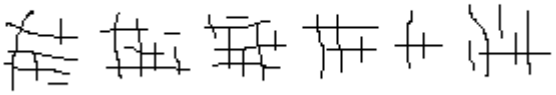
Obrázek 7 - Obsah zprávy psané šipkami

Zprávu můžeme zašifrovat i tzv. *čínštinou*. Text šifrovaný tímto způsobem vypadá jako čínské znaky, odtud samozřejmě vznikl název této šifry. (Zoubek, 1998) Základem tohoto systému je tabulka vyplněná písmeny z abecedy, kromě písmen s diakritikou

a CH a Q. Písmena mohou být v tabulce různě uspořádána, ale účastníci komunikace musí mít stejnou tabulku. Jednotlivá písmena šifrujeme tak, že přes sebe kreslíme svislé a vodorovné čáry, přičemž počet svislých čar odpovídá pořadí sloupce a počet vodorovných čar pořadí řádku, ve kterém se dané písmeno nachází. Čáry můžeme dělat různě dlouhé, abychom zmátli útočníka. Na obrázku 8 je vyvedena pomocná šifrovací tabulka a způsob šifrování. K vyplnění tabulky bylo použito heslo *kniha*, zbytek tabulky byl doplněn již v abecedním pořadí vyjma písmen, které jsou obsaženy v hesle.

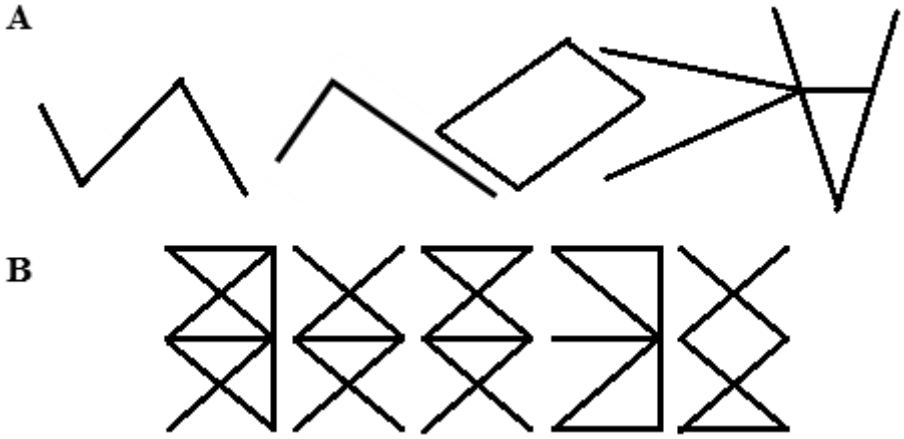
K	N	I	H	A
B	C	D	E	F
G	J	L	M	O
P	R	S	T	U
V	W	X	Y	Z

OT: STUDNA

ŠT: 

Obrázek 8 - Šifrovací systém Čínština

V rámci grafických šifer si lze také „hrát“ s jednotlivými písmeny. Písmena textu můžeme různě rotovat (obrázek 9 A – zašifrován text *slova*) nebo třeba využít jejich doplňky (obrázek 9 B – zašifrováno slovo *louka*). Tyto šifrovací systémy jsou velmi jednoduché a ne příliš bezpečné, ale na první pohled vypadají složitě.



Obrázek 9 - Rotace a doplňky písmen

Většina z uvedených šifrovacích systémů postrádají tajný klíč a jsou veřejně známé, a tedy snadno prolomitelné. Takové šifry se nejčastěji využívají pro rekreační šifrování, na táborech, v soutěžích a dětských hrách. Pro svoji jednoduchost jsou vhodné pro seznámení se se základy kryptologie, a proto budou některé z nich využity při výuce v rámci praktické části diplomové práce.

1.4 Role kryptologie ve výuce informatiky

Obsah této kapitoly bude zaměřen na důvody, přínosy a výhody zavedení kryptologie do výuky informatiky. Cílem první podkapitoly této části bude popsat význam základů kryptologie pro žáky druhého stupně základní školy.

Druhá podkapitola se zaměří na vztahy výuky kryptologie s dalšími předměty, jako například s matematikou, dějepisem, českým jazykem, výtvarnou výchovou a v neposlední řadě také s informatikou.

Poslední kapitola si klade za cíl popsat kryptologii jako vhodnou formu pro seznámení žáků s problematikou počítačové a informační bezpečnosti.

1.4.1 Přínos výuky kryptologie

Kryptologie je velmi významná, neboť se s ní v určité míře setkáváme každý den. Nejvýznamnější využití v praxi má kryptologie v rámci informační bezpečnosti, slouží k zabezpečení dat (například utajení kódu programů, cenných souborů a informací, atd.). Kryptologie také úzce souvisí s ověřováním identity (hesla, digitální podpisy, certifikáty, …). Díky kryptologii děti snáz pochopí princip práce počítače (převod dat na 0 a 1).

Díky hledání různých souvislostí a pravidel při luštění a dešifrování textu rozvíjejí klasické šifrové systémy logické myšlení a představivost. Při luštění musí děti přemýšlet a zjišťovat, jakým způsobem byla zpráva zašifrována, jaké prostředky byly využity, musí pracovat s textem a pohlížet na něj z různých úhlů a hledisek.

Jelikož šifrování probíhá podle daných pravidel a postupů, pracuje s čísly a neobejde se bez výpočtů, byť někdy jen elementárních (například při zjišťování rozměrů tabulky, počtu jednotlivých znaků, …), rozvíjí se při něm i algoritmické a matematické myšlení.

Vymýšlení a tvorba různých klíčů, způsobů a možností šifrování, hlavně v oblasti grafických šifer a steganografických metod, přispívá k rozvoji tvořivého myšlení a kreativity. Také snaha o utajení informace či klíče a znemožnění přístupu útočníka k obsahu zprávy nutí člověka samostatně a efektivně uvažovat.

Protože při práci s šifrovými systémy je důležitá schopnost orientace v textu, hledání souvislostí, znalost jazyka, a podobně, je nutno kultivovat tyto dovednosti pomocí různých křížovek, hlavolamů, logických úloh, hádanek a dalších. Křížovky a podobné úlohy se často používají jako forma motivace ve výuce nebo způsob upevňování učiva zábavnou formou (například doplňovačky s anglickými slovíčky). Jedna výzkumná práce dospěla k výsledku, že křížovky napomáhají při učení, a doporučuje využívání křížovek jako učební metodu pro lepší pochopení a zapamatování složitých pojmů. (Berry, Miller, 2008).

Jitka Fořtíková (2016) roztřídila různé typy logických úloh podle toho, kterou oblast rozumových schopností pomáhají rozvíjet. Kvízy a šifry rozvíjejí logické myšlení ve smyslu „*hledání správné myšlenkové cesty*“. Verbální schopnosti a slovní zásobu zase rozvíjejí křížovky, přesmyčky a podobně.

Ze zmíněných důvodů potřeby křížovek, kvízů a podobných logických úloh byl proveden výzkum, jehož úkolem bylo zjistit, jaký vztah mají děti ke zmiňovaným úlohám. Výsledky výzkumu jsou popsány v empirické části.

1.4.2 Mezipředmětové vztahy

Kryptologie má velmi široké využití napříč různými obory a vyučovacími předměty. Největší využití má pravděpodobně v informatice, jelikož šifrování i dešifrování rozvíjí algoritmické myšlení, které je velmi důležité pro oblast programování. Děti, které jsou v programování zdatnější a zajímají se o kryptologii, si mohou navrhnout aplikace, které budou všechnu práci ohledně utajování textu či luštění tajných zpráv provádět za ně. Na kódování zase děti snadno pochopí, jak pracuje počítač, tedy že musí veškerá data převádět na kombinace znaků 0 a 1. V další kapitole se podrobněji zaměříme na využití kryptologie pro lepší pochopení problematiky datové bezpečnosti.

Kryptologie je úzce spjata s dějepisem, prameny totiž uvádějí, že se začínalo šifrovat již v 5. století před naším letopočtem a často se šifrovalo za účelem válečné komunikace a utajení válečných strategií. (Janeček, 1998) Mnozí autoři uvádějí příběhy, jak šifrovali například Peršané, že prvními úspěšnými luštiteli byli Arabové, a spoustu různých šifrových systémů a strojů, které umožňovaly zprávy šifrovat i dešifrovat a napomáhaly k prolomení neznámých systémů. (Singh, 2009) V hodinách dějepisu je často zmiňována například Morseova abeceda.

I matematika má v rámci kryptologie své uplatnění. Jak již bylo řečeno, informace můžeme zašifrovat i tak, že vypadají jako kombinace čísel, a žák, který se snaží zprávu rozluštit, musí přemýšlet, co s číslicemi provést, aby se dobral ke správnému výsledku, čímž je kultivováno jeho logické i matematické uvažování. Matematické operace využívá i při sestavování pomocné tabulky (například dělení počtu znaků textu počtem znaků hesla, prvočíselný rozklad, …) při dešifrování i luštění.

K výtvarné výchově mají nejblíže grafické šifry a steganografické metody, u nichž je velmi důležitá tvůrčí činnost a originální nápady. Děti mohou vymýšlet různé směry či obrazce pro transpoziční systémy, různé transformace a grafické podoby písmen, vlastní šifrové abecedy, vlastní možnosti, jak ukrýt zprávu do obrázku, apod. Podobné nápady mohou být uplatněny v rámci praktických činností, při kterých si děti mohou vyrábět různé steganografické či šifrovací pomůcky, třeba dvojitou mapu (zpráva je vlepena mezi dva listy papíru), keramickou destičku s návodem k dešifrování (šifrový text zprávy je uvnitř destičky a pro jeho získání je nutno destičku rozbít), šifrovací hůl (skytala) a další pomocné předměty.

Při šifrování, dešifrování i luštění však člověk pracuje hlavně s textem a písmeny, neboť všechny tyto procesy probíhají za účelem utajit nebo přečíst si nějakou zprávu. Děti se tak musí naučit pracovat s abecedou, hledat slova v nepřehledné změti písmen, porozumět textu psanému bez diakritiky a mezer. Při luštění navíc musí zkoumat, které znaky se vyskytují nejčastěji, tudíž musí dobře znát svůj jazyk a vědět, která písmena či skupiny znaků se v češtině nejčastěji používají a které nikoli, a hledat mezi nimi souvislosti. Kryptologie má tedy úzký vztah k českému jazyku a dokonce i k literatuře, neboť existuje spousta publikací, odborných článků či příběhů o šifrování pro nadšené zájemce.

Kryptologii lze spojit i s chemií. Děti si v laboratořích mohou vyrábět a zkoušet různé druhy neviditelných inkoustů, které jsou složitější na přípravu a přísady nejsou tak dostupné jako například mléko či citronová šťáva.

Do hudební výchovy mohou být začleněny aktivity, při kterých si žáci mohou zkoušet různé metody posílání zakódovaných či zašifrovaných tajných zpráv. Takové aktivity mohou zahrnovat například vyťukávání znaků Morseovy abecedy, brnkání různých tónů (každý tón může znamenat jiný znak), šifrování pomocí zpěvníků či notových zápisů, apod.

Možností, jak začlenit kryptologii do jednotlivých školních předmětů, existuje velká spousta. Za účelem motivace, rozptýlení a probuzení zájmu žáků o daný předmět, by občas (například jednou za měsíc) mohla být zařazena speciální vyučovací hodina, kde by docházelo k rozvíjení schopností a dovedností typických pro daný předmět, avšak ve spojitosti s kryptologií.

1.4.3 Kryptologie a počítačová bezpečnost

Kryptologie bývá využívána především z důvodu informační a datové bezpečnosti. Pomocí šifrovacích algoritmů a šifrovacích klíčů lze zabezpečit citlivé a důvěrné informace a hesla mohou zamezit přístup nepovolaného člověka k našim datům. S počítačovou bezpečností se seznamují žáci již na prvním stupni základní školy, učí se, jak si správně zvolit a používat heslo, jak nakládat s cennými informacemi, jak se bezpečně pohybovat na internetu a sociálních sítích, seznamují se s pojmem kyberšikana, apod. Ne vždy ale žáci tyto rady a hrozby berou vážně, mají pocit, že jich se nic podobného netýká, a neuvědomují si, co všechno může útočník použít v jejich neprospěch. Nejen děti, ale i dospělí lidé často volí jednoduchá a snadno prolomitelná hesla, používají stejné heslo k několika účtům, nejsou schopni heslo bezpečně uschovat (napíší si je na papír a nechají ležet v okolí počítače nebo heslo sdělí druhému člověku), na sociálních sítích sdílejí příliš mnoho informací od těch zdánlivě neškodných (nové auto, odjezd na dovolenou, fotky dětí, …) po ty osobní a cenné (vysvědčení, občanský průkaz, telefonní čísla, soukromé fotografie, …). Pro útočníky je pak snadné dostat se k informacím, které mohou zneužít, a poškodit tak daného člověka.

Zavedení výuky kryptologie do škol by mohlo dětem pomoci lépe pochopit zásady počítačové bezpečnosti. Na základě seznámení s různými šifrovacími metodami a způsoby luštění by totiž zjistily, jak snadné je prolomit nějaké heslo či šifru a získat tak potřebné informace.

2 EMPIRICKÁ ČÁST

Z důvodu získání přehledu o zkušenostech žáků s kryptologií a jejich zájmu o výuku zaměřenou na toto téma bylo provedeno výzkumné šetření na téma *Kryptologie na základní škole*.

Cílem empirické části bude popsat výzkumný proces. V následujících podkapitolách budou nejprve sepsány výzkumné cíle a hypotézy. Následně bude popsána výzkumná metoda a výzkumný soubor. Nakonec bude uveden přehled výsledků a jejich podrobná interpretace.

2.1 Výzkumné cíle

Před tím, než byla zahájena výuka základů kryptologie v rámci diplomové práce, byl proveden výzkum, jehož cílem bylo zjistit, jaké mají žáci předpoklady zvládnout základy kryptologie. Tento cíl byl ještě rozdělen na několik dílčích cílů:

- Zjistit, jak jsou na tom děti s luštěním křížovek.
    - Jak často luští křížovky?
    - Jaké typy křížovek mají nejraději?
    - Jakým způsobem luští osmisměrky?
- Zjistit, jestli mají děti rády hádanky, logické úlohy a hlavolamy.
    - Baví je řešit takové úlohy?
    - Dělá jim to potíže?
- Zjistit, jaké mají děti zkušenosti s kryptologií.
    - Znají nějaké formy utajení textu, a jaké?
    - Používají sami nějakou formu utajení textu?
- Zjistit, jaký mají děti zájem o výuku kryptologie.

2.2 Hypotézy

Po sestavení jednotlivých cílů byly ještě vytvořeny domněnky a hypotézy. Jedním z předpokladů bylo tvrzení, že děti luští křížovky spíše častěji, tedy alespoň jednou za měsíc, a nejoblíbenějším typem křížovek u dětí je doplňovačka s tajenkou a osmisměrka. Předpokládalo se také, že osmisměrku děti řeší tak, že postupně hledají všechna slova z nabídky.

Další domněnkou bylo, že děti mají rády různé hádanky a hlavolamy, ale řešení matematických logických úloh je pro ně obtížné.

Také byla vytvořena hypotéza, že děti znají některé jednoduché šifrové systémy a způsoby ukrývání textu a sami je hojně využívají, například k tajné korespondenci nebo tvorbě taháků. Byl předpokládán velký zájem ze strany respondentů o výuku

základů kryptologie s domněnkou, že respondenti chápou zmiňovanou výuku jako zpestření klasické výuky.

K tématu popularita křížovek a logických úloh u dětí se nepovedlo dohledat žádné podobné výzkumy nebo publikace. Většina autorů různých sbírek s křížovkami, hádankami a logickými úlohami se shoduje na tom, že děti luští křížovky rády. Nicméně v článku Jiřího Sotony (2016) si můžeme přečíst slova Neila Warea, Skota učícího v České republice angličtinu: „*Jen děti moc neluští, ty mají radši hry na mobilech*.“

2.3 Metodika

Šetření proběhlo formou kvantitativního výzkumu. Byl vytvořen dotazník vlastní konstrukce (viz příloha 1), v jehož úvodu se nacházelo vysvětlení a důvod šetření a také zde byly uvedeny pokyny ke správnému vyplňování. Dotazník se skládal z 18 otázek uzpůsobených věku respondentů. Vyskytovaly se jak otázky uzavřené, tak i otevřené a polootevřené. V případě uzavřených otázek měli respondenti na výběr většinou z tří nebo pěti odpovědí.

Výzkumný soubor se skládal z 39 respondentů, z nichž bylo 23 žáků šesté třídy a 16 žáků sedmé třídy Základní školy Nasavrky. Výuka kryptologie bude vyučována pouze v šesté třídě, ale sedmá třída bude sloužit jako kontrolní skupina při vypracovávání pracovních listů, proto byli sedmáci do dotazníkového šetření zahrnuti také.

Vypracovaný dotazník byl nejprve rozdán respondentům, kteří jej vyplnili, čímž byl proveden sběr dat. Data byla postupně zpracovávána do jednoduchých tabulek. Každá tabulka odpovídala jedné otázce v dotazníku. Ke každé otázce byly vytvořeny postupně čtyři tabulky; jedna zobrazovala data z šesté třídy, druhá ze sedmé třídy, třetí tabulka se týkala všech respondentů dohromady a čtvrtá tabulka porovnávala výsledky 6. a 7. třídy. U některých otázek byly možnosti odpovědí číselně ohodnoceny a byl proveden průměr získaných dat. Výsledky také byly pro lepší představu vyjádřeny v procentech. K většině tabulek byly vytvořeny názorné grafy (koláčové nebo sloupcové). Získané výsledky pomohly potvrdit nebo případně vyvrátit stanovené hypotézy a navržené teorie. Nakonec byla provedena interpretace získaných výsledků.

2.4 Přehled výsledků

V této kapitole bude uveden přehled získaných výsledků. Zmíněna bude postupně většina otázek z dotazníku, jejich přesné znění je k nahlédnutí v příloze 1. Sepsané výsledky budou doplněny přehlednými tabulkami a grafy.

Z první otázky v dotazníku bylo zjištěno, že průměrná doba luštění křížovek u žáků je několikrát za rok. V tabulce 4 je vidět, že největší počet respondentů zvolil právě odpověď „několikrát za rok“, druhou nejčastější byla odpověď „nikdy“. Tím byla vyvrácena první hypotéza, která předpokládala, že děti luští křížovky alespoň jednou měsíčně. Tuto možnost zaškrtlo pouze sedm respondentů. Byl tedy potvrzen názor Neila Warea, že děti místo křížovek radši hrají hry na mobilu.

Tabulka 4 - Přehled odpovědí na 1. otázku

1. Luštíš křížovky? Jak často?		Procenta:
Několikrát týdně	2	5,13%
Jednou týdně	5	12,82%
1 až 3x měsíčně	7	17,95%
Několikrát za rok	14	35,90%
Nikdy	11	28,21%
Průměr	3,69	

Na obrázku 10 také můžeme vidět srovnání odpovědí obou tříd, odkud je dobře vidět nejčastější odpověď žáků sedmé třídy. Lze také pozorovat, že v šesté třídě měly odpovědi „několikrát za rok“ a „nikdy“ stejné zastoupení.

Obrázek 10 - Srovnání odpovědí obou tříd na 1. otázku

Byla potvrzena hypotéza, že nejoblíbenějším typem křížovky jsou osmisměrky. U druhé otázky mohli žáci zaškrtnout více odpovědí a nejhojněji byla zastoupena právě osmisměrka. Na druhém místě se umístila doplňovačka s tajenkou (viz obrázek 11).

V obou třídách získala osmisměrka největší počet procent (dokonce byla v obou třídách procentuálně stejně zastoupena) a také doplňovačka byla v obou třídách druhá nejoblíbenější. Třetí místo se v jednotlivých třídách lišilo; v šesté třídě byl na třetím místě Kris-kros, kdežto v sedmém ročníku to byla klasická křížovka. Počet odpovědí u každého typu křížovky a jejich procentuální zastoupení je zapsáno v tabulkách 5 a 6.

Obrázek 11 - Koláčový graf udávající míru oblíbenosti různých typů křížovek

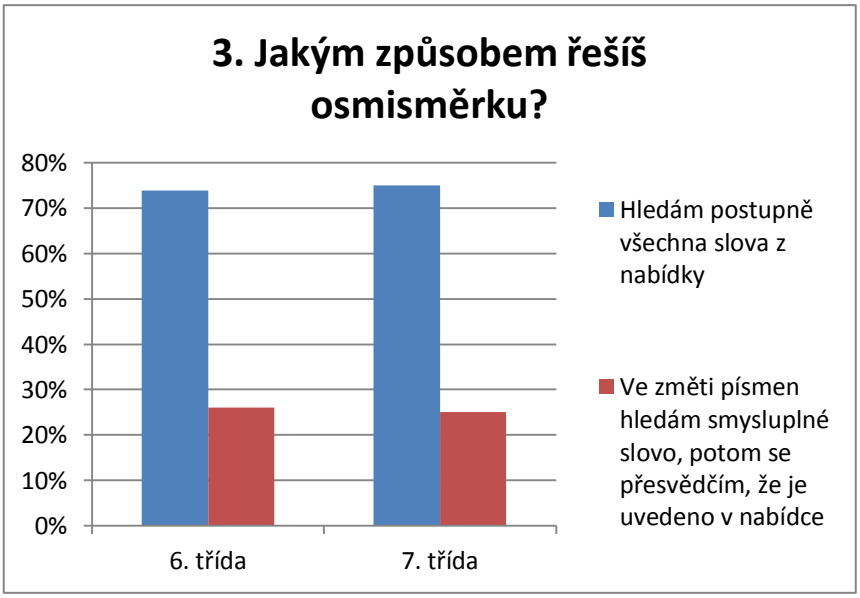
Další otázka zkoumala, jakým způsobem děti luští osmisměrky. Na výběr měly ze dvou možností. Nejčastěji byla v obou třídách zaškrtnuta možnost „hledám postupně všechna slova z nabídky“, což je znázorněno sloupcovým grafem na obrázku 12. Tento fakt opět potvrdil zvolenou domněnku.

Tabulka 5 - Odpovědi žáků 6. třídy

2. Jaký typ křížovek luštíš nejradši?		Procenta:
Švédská křížovka	1	4,35%
Osmisměrka	13	56,52%
Kris-kros	3	13,04%
Klasická křížovka	1	4,35%
Doplňovačka s tajenkou	5	21,74%
Jiné	0	0,00%

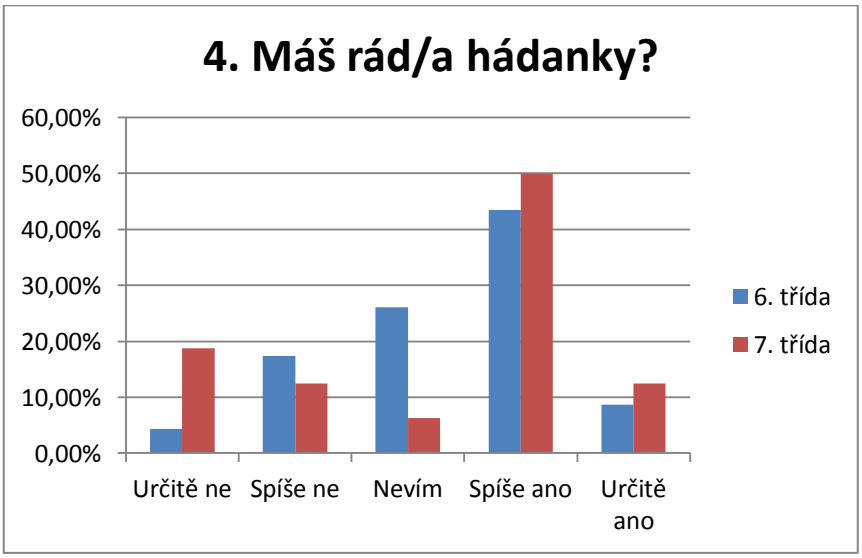
Tabulka 6 - Odpovědi žáků 7. třídy

2. Jaký typ křížovek luštíš nejradši?		Procenta:
Švédská křížovka	1	6,25%
Osmisměrka	9	56,25%
Kris-kros	1	6,25%
Klasická křížovka	3	18,75%
Doplňovačka s tajenkou	4	25,00%
Jiné	1	6,25%



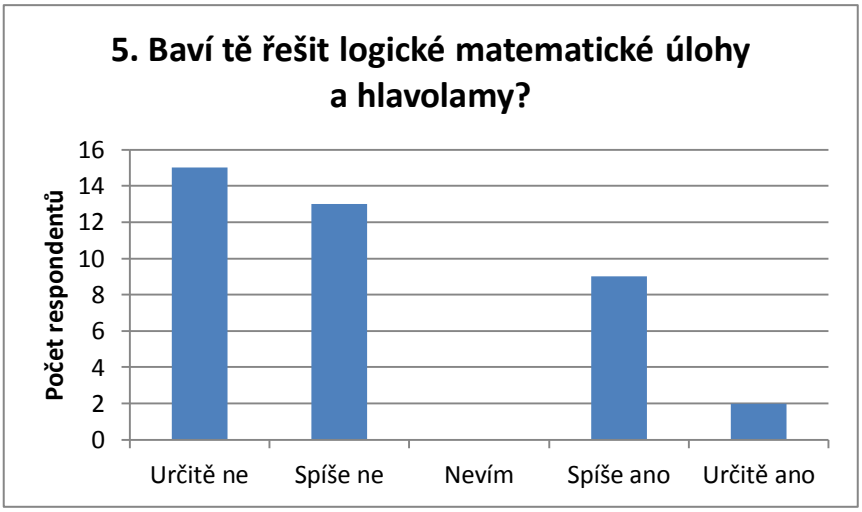
Obrázek 12 - Zastoupení odpovědí na 3. otázku v obou třídách

Následující tři otázky se zabývaly oblibou a obtížností různých druhů hádanek, hlavolamů a logických úloh. Respondenti mohli zaškrtnout jednu možnost z pětistupňové škály. U otázky, zda mají žáci rádi hádanky, byla nejpočetnější vybranou odpovědí „spíše ano“. Je zajímavé, že v šesté třídě byla druhá nejčastější odpověď „nevím“, zatímco v sedmé třídě to byla odpověď „určitě ne“, jak je vidět na obrázku 13.



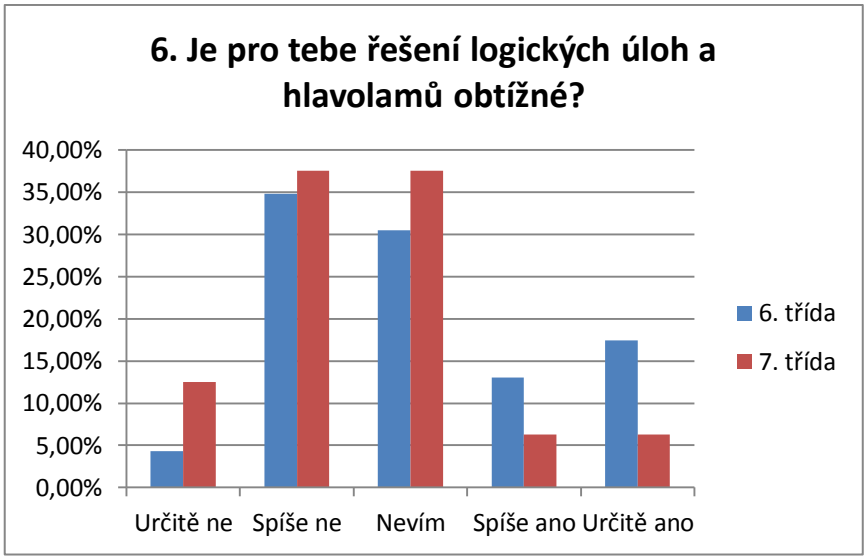
Obrázek 13 - Srovnání odpovědí jednotlivých tříd na 4. otázku

V další otázce už převládala odpověď „určitě ne“ (viz obrázek 14). Aby mohlo být zjištěno, jaké stanovisko zaujímá třída jako celek k určité otázce, byla každé odpovědi přiřazena hodnota a následně byl vypočítán aritmetický průměr. U čtvrté otázky tedy respondenti spíše nevědí, jestli mají rádi hádanky, a u páté otázky je průměrnou odpovědí „spíše ne“.



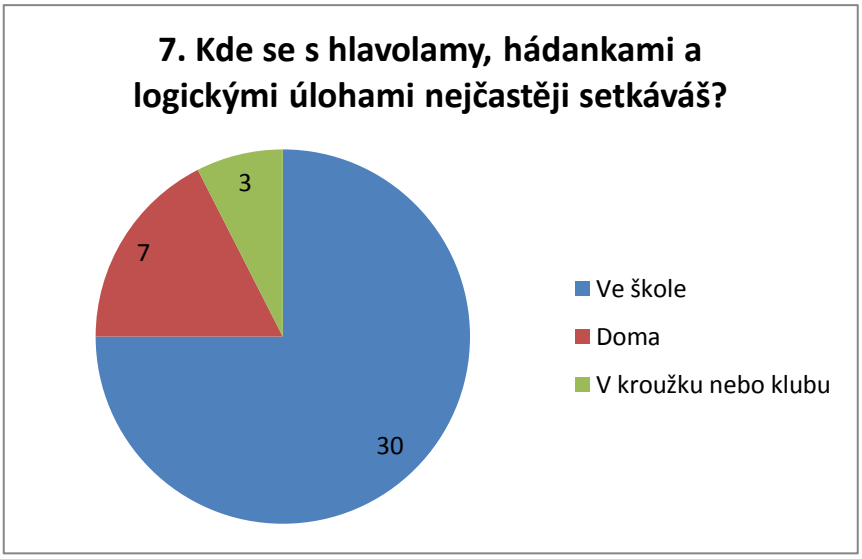
Obrázek 14 - Znázornění četností jednotlivých odpovědí na 5. otázku

Na obrázku 15 je vidět porovnání odpovědí obou tříd na šestou otázku. V šestém ročníku převládla odpověď „spíše ne“ a v sedmé třídě byly nejčetnější otázky „nevím“ a „spíše ne“ (tyto otázky zvolil stejný počet žáků, a sice 8). I u této otázky byl vypočítán aritmetický průměr a v obou třídách vyšla odpověď „nevím“ s tím rozdílem, že u šesťáků se průměr blížil k možnosti „nevím“ spíše zprava (průměrná hodnota 3,04) a u sedmáků spíše zleva (průměrná hodnota 2,56). Byla tedy vyvrácena domněnka, že řešení logických úloh je pro většinu žáků obtížné.



Obrázek 15 - Porovnání odpovědí na 6. otázku

Cílem sedmé otázky bylo zjistit, kde se žáci nejčastěji s logickými úlohami a hlavolamy setkávají. Nejvíce respondentů se s hlavolamy setkává nejčastěji ve škole (z toho 17 šesťáků a 13 sedmáků), sedm lidí uvedlo, že se s nimi nejčastěji setkává doma a nejméně žáků vybralo možnost „v kroužku nebo klubu“. Četnosti odpovědí na tuto otázku jsou znázorněny v koláčovém grafu na obrázku 16.



Obrázek 16 - Znázornění odpovědí na 7. otázku

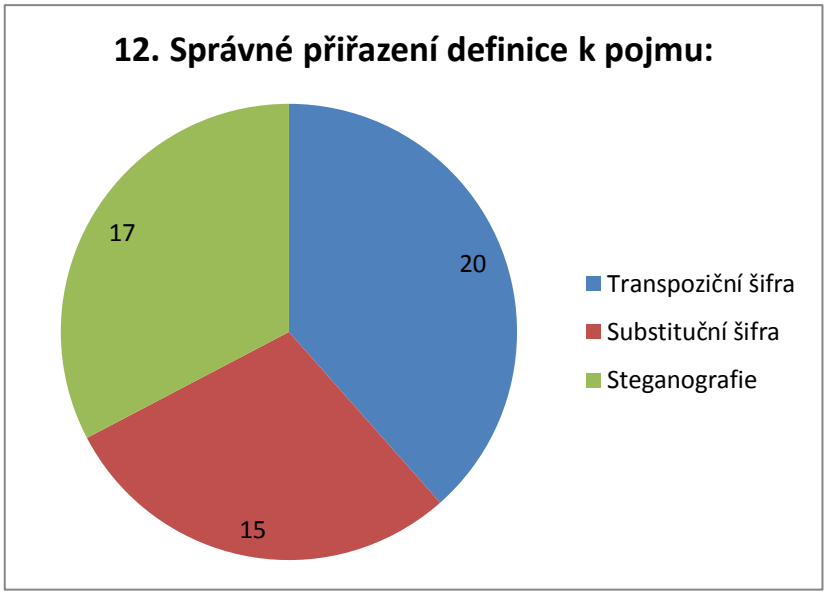
Díky další otázce se potvrdilo předpokládané tvrzení, že děti znají některé jednoduché formy utajování textu. V tabulce 7 je jasně vidět, že nejvíce žáků uvedlo, že se s nějakou formou utajení setkalo. V této otázce měli žáci navíc uvést, o jakou formu se jedná. Dohromady se sešlo hned několik příkladů, například přeházená písmena, slova psaná pozpátku, první písmeno na začátku slova nebo řádku, přesmyčky, Morseova abeceda, obrázkové písmo, neviditelný inkoust a další.

Tabulka 7 - Četnosti odpovědí na 8. otázku

8. Setkal/a jsi se někdy s nějakou formou utajení textu?		Procenta:
Ne	9	23,08%
Nevím	12	30,77%
Ano	18	46,15%
Průměr	2,23	

Překvapivé bylo zjištění, že pouze 6 žáků ze všech odpovědělo, že nějakou formu utajení přímo používá. Větší procento z těchto žáků zaujímala šestá třída. Respondenti opět uváděli, který způsob používají, a jednalo se hlavně o neviditelný inkoust, pozpátku psaný text a Morseovu abecedu. Předpoklad, že děti hojně využívají utajování textu, byl tímto vyvrácen.

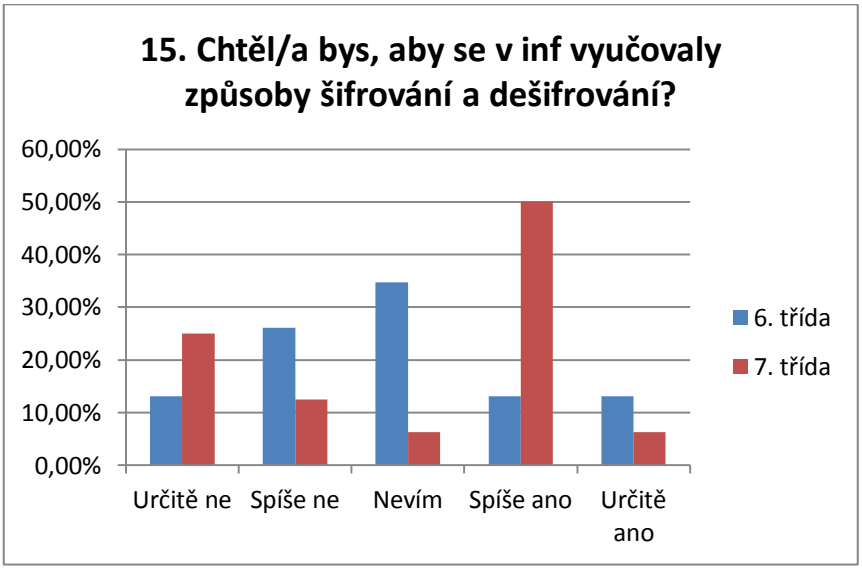
Ve dvanácté otázce měli žáci za úkol přiřadit k pojmu správnou definici. Byly vybrány tři pojmy z oblasti kryptografie. Nečekaný byl poměrně vysoký počet správně přiřazených definic. Graf na obrázku 17 zobrazuje, kolikrát byl daný pojem správně připojen ke své definici.



Obrázek 17 - Počet správně připojených definic k pojmům

Na třináctou otázku, která se ptala, zda děti znají význam slova „anagram“, všichni odpověděli záporně. Na čtrnáctou otázku, která na ni navazovala (úkolem bylo uvést příklad anagramu), tudíž neodpověděl nikdo.

Odpovědi žáků na otázku, jestli by měli zájem o výuku šifrování a dešifrování, byly nejočekávanější, ale přinesly spíše rozčarování a zklamání. I když většina respondentů zaškrtla možnost „spíše ano“, v šesté třídě byla nejpočetnější odpovědí „nevím“ a v sedmém ročníku byla hojně zastoupena možnost „určitě ne“. Celkově 15 žáků zaškrtlo „spíše ano“ a „určitě ano“, stejný počet žáků ale uvedl „spíše ne“ a „určitě ne“ a 9 respondentů odpovědělo neutrálně. Průměrně opět zvítězila odpověď „nevím“, čímž byla částečně vyvrácena teorie, že žáci projeví o kryptologii velký zájem. V následujícím grafu (obrázek 18) je opět vyobrazeno, jak odpovídaly jednotlivé třídy.



Obrázek 18 - Porovnání odpovědí obou tříd na 15. otázku

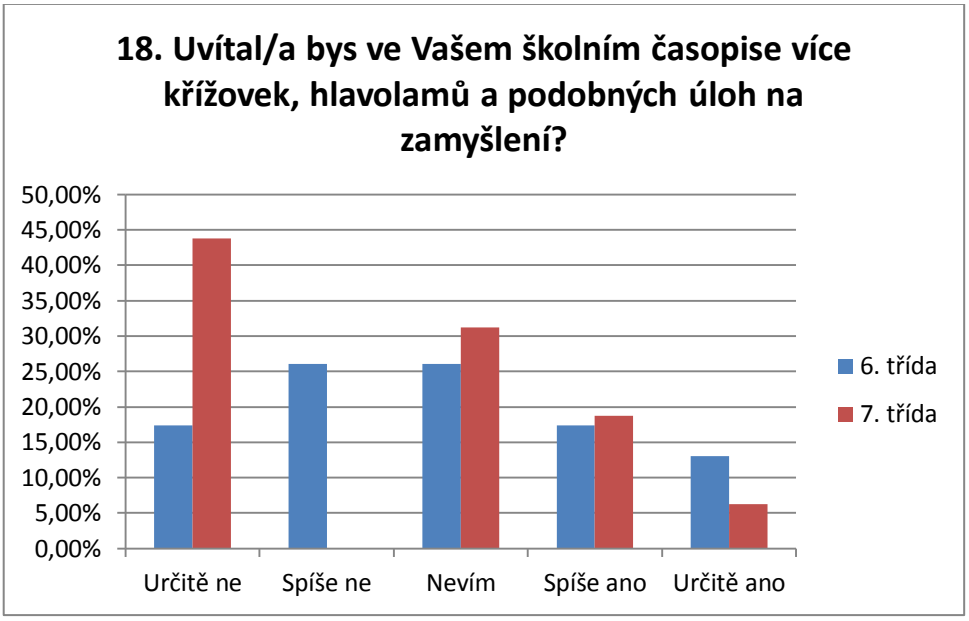
Protože bylo předem známé, že základní škola, na které byl výzkum prováděn, vede školní časopis, byly poslední tři otázky věnovány problematice křížovek ve školním časopisu. Otázka 16 tedy zjišťovala, zda jsou křížovky a hlavolamy do školního časopisu zahrnuty. Většina žáků odpověděla kladně, 15 žáků ale odpovědělo „nevím“ nebo „ne“, z čehož bylo usouzeno, že tito žáci si školní časopis nekupují.

Dále bylo zjištěno, že křížovky ve školním časopise luští pouze 14 žáků, z toho je větší procento žáků z šestého ročníku. V tabulce 8 jsou vidět odpovědi žáků šesté a sedmé třídy a všech žáků dohromady.

Tabulka 8 - Odpovědi žáků na 17. otázku

17. Řešíš křížovky a hlavolamy ve Vašem školním časopise?			
	6. třída	7. třída	Celkem
Ne	14	11	25
Ano	9	5	14

Na poslední otázku dávali respondenti spíše negativní odpovědi. Největší zastoupení měly možnosti „určitě ne“ a „nevím“ (každou z těchto možností vybralo celkem 11 žáků). Graf na obrázku 19 znázorňuje srovnání odpovědí žáků obou tříd na poslední otázku. U této otázky byl opět vypočítán aritmetický průměr všech odpovědí. Stanovisko, které zaujímá výzkumný soubor k této problematice, je neutrální.



Obrázek 19 - Srovnání odpovědí obou tříd na 18. otázku

2.5 Interpretace výsledků

V této kapitole budou vysvětleny získané výsledky a bude provedena diskuse o příčinách, které pravděpodobně vedly k faktům zjištěných na základě výzkumu.

Příčina toho, že děti luští křížovky v tak malé míře, nejspíš tkví ve způsobu života dnešních dětí. Děti tráví spoustu času hraním počítačových her či na sociálních sítích a o křížovky nejeví zájem. Když už se uchýlí k luštění nějaké křížovky, volí spíše osmisměrky a doplňovačky s tajenkou, protože k tomu potřebují pouze malé množství znalostí (nemusí tolik „namáhat mozek"), než je tomu například u švédských křížovek. V případě osmisměrky pouze hledají slova skrytá ve změti písmen a legenda u doplňovaček je většinou ilustrovaná.

Děti nemají rády hlavolamy a logické úlohy nejspíš proto, že jsou složité a jejich řešení trvá delší dobu. Což by ovšem znamenalo, že by děti měly méně času na hry a jiné počítačové aktivity. Navíc je zřejmé, že se těmito úlohami žáci již nechtějí „otravovat" doma, když se s nimi setkávají ve škole, jak uvedla většina respondentů.

Fakt, že žáci spíše nevědí, zda je pro ně řešení logických úloh obtížné, asi spočívá v tom, že s těmito úlohami nemají zkušenost. Tyto úlohy obvykle neřeší, a proto nemohou říct, zda jim dělají problémy či ne.

Na základě dotazníku bylo zjištěno, že nějaké formy utajování textu užívá pouze malé procento respondentů. Je to nejspíše opět způsobeno větším množství času, které šifrování a dešifrování zabírá. Navíc některé šifrové systémy nejsou nejjednodušší a vyžadují vyšší koncentraci.

Těžko říci, jestli je velká úspěšnost v přiřazování pojmů k definicím způsobena tím, že respondenti znají pojmy nebo jejich správnou definici vytušili (například pojem *substituční šifra* je odvozen od slova *substituce*, kterou žáci používají například při řešení rovnic – nahrazování výrazů proměnnou) anebo správné odpovědi pouze tipovali. Přikláním se spíše k variantě tipování (podle ledabylých spojovacích čar v dotaznících).

Neznalost významu slova *anagram* lze vysvětlit neznalostí tohoto termínu, neboť někteří žáci uváděli, že znají nebo používají přesmyčky, což je český překlad pro anagram.

Nezájem o výuku kryptologie může být spojen s neznalostí a nezkušeností s touto disciplínou. Děti si nejspíš nedokáží pod pojmy šifrování a dešifrování představit nic konkrétního a slova jako kryptologie nebo transpoziční šifra je mohou děsit. Jiným způsobem interpretace by mohla být představa dětí o výuce šifrování v rámci informatiky jako o činnosti, která je připravuje o možnost pracovat s počítačem.

3 PRAKTICKÁ ČÁST

V rámci praktické části diplomové práce bude připravena výuka na téma *Základy kryptologie* pro žáky druhého stupně základní školy, konkrétně pro 6. a 7. třídu Základní školy Nasavrky. Zároveň budou pro žáky vytvořeny pracovní listy, které prověří jejich znalosti a logické a tvořivé myšlení. V šesté třídě proběhne výuka i připravená aktivita. Sedmá třída bude považována za kontrolní skupinu, a proto žáci budou vyplňovat pracovní list bez předchozího seznámení s problematikou kryptologie.

Jednotlivé pracovní listy budou popsány v první podkapitole této části. Další kapitola se zaměří na přípravu výstupu, popíše cíle, metody, formy a prostředky potřebné pro realizaci výuky. Čtenář zde také zjistí, jak probíhala výuka i jak si počínali žáci během vyplňování pracovních listů.

V další kapitole bude vyhodnocena práce žáků, tedy v čem nejvíce chybovali, co jim naopak šlo lehce, jak hojně využívali nápovědy, jestli se jim podařilo dostat se do konce. Následně budou také srovnány výkony jednotlivých tříd.

Poslední kapitola přiblíží, jak žáci hodnotili celkový projekt, co se jim líbilo a nelíbilo, co jim projekt přinesl či co je zaujalo. Pro hodnocení projektu budou vytvořeny vhodné dotazníky.

3.1 Tvorba pracovních listů

Pro žáky šesté třídy byly připraveny dva typy pracovních listů. První pracovní list (viz příloha 2) je spíše teoretického rázu a bude žákům rozdán ještě před začátkem vyučování. Do tohoto listu si žáci mohou během vyučování zapisovat potřebné poznámky, zajímavosti nebo si zkoušet různé způsoby šifrování a dešifrování.

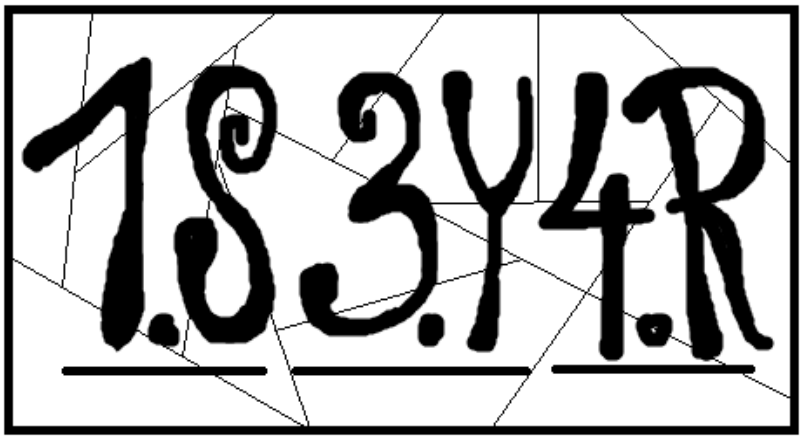
První část listu má předepsaný text a řádky, kam budou děti doplňovat správné informace, které uslyší během prezentace. Text se týká především důvodů, proč je kryptologie využívána, co vlastně kryptologie znamená, jsou zde také uvedeny dva nejznámější příklady šifrování z historie. V další části, která se týká odvětví kryptologie, budou žáci přiřazovat k definici správný pojem. Následují základní pojmy, které jsou hojně užívány při práci s šiframi a které je nutno znát. V pracovním listu jsou uvedeny pouze definice a úkolem žáků je na vyznačené řádky doplnit správné slovo či sousloví. U poslední teoretické otázky musí děti na základě uvedené definice škrtnout nehodící se typ šifrování. List obsahuje ještě dvě praktické úlohy, které jsou uvedeny i v prezentaci a žáci si je tak mohou zkoušet spolu s výkladem. Pro zjednodušení je zde uvedená převodová a šifrovací tabulka, aby je děti nemusely kreslit nebo rýsovat. Pracovní list je sestaven tak, aby sledoval výklad a prezentaci a žáci tak nemuseli pracně vyhledávat, kam mají informaci zapsat či vyplnit.

Takto zpracovaný list dostane každý žák šesté třídy a bude si ho smět ponechat. Informace uvedené v tomto pracovním listu mohou žáci využít při plnění druhého pracovního listu.

Druhý pracovní list (viz příloha 3) je koncipován spíše jako hra nazvaná *Cesta za pokladem*. Úkolem žáků je plnit posloupnost připravených úkolů. Každý úkol po vyřešení odkrývá určitou informaci, která je nezbytná pro další pokračování. Tento pracovní list dostanou žáci do dvojice, kterou si zvolí libovolně (zvolí si také název skupiny), a tedy budou celou hrou prostupovat společně. Na konci hry čeká na úspěšné luštitele sladká odměna.

Šifrovací úlohy v pracovním listu jsou doplněny hádankami a logickými úlohami pro větší různorodost a stimulaci logického a tvořivého myšlení. Inspirace při tvorbě úkolů v pracovním listu byla čerpána z knihy Radka Pelánka (2014).

První úloha je klasická hádanka. Počet písmen její správné odpovědi udává, o kolik se má posunout šifrová abeceda v druhém úkolu. Druhým úkolem je tedy zpráva zašifrovaná pomocí substituce a žáci ji musí dešifrovat. K dispozici mají připravenou převodovou tabulku, kde však není vyplněn řádek s šifrovou abecedou. Řešením úkolu je definice pojmu, jehož znalost budou během hry potřebovat. Odpověď na třetí úkol je ukryta pomocí steganografické metody, a sice čísla jsou odkazem na písmeno ve slově (nepočítají se zkratky jednotek – kg a l). Čtvrtá úloha je příklad grafické šifry. Na první pohled vypadá jako pole pro hru *Lodě*, avšak po vybarvení políček podle zadaných souřadnic, získá luštitel určité slovo. Pátá v pořadí je úloha na přemýšlení, děti musí na základě vlastních úvah zjistit, v jaké bedně se skrývá poklad. Text v posledním úkolu je zašifrován transpozicí, přičemž každý řádek je šifrován jiným způsobem. Úkolem žáků je na tyto způsoby přijít a rozluštit zprávu, která je informuje o dalším postupu. Pokud žáci úspěšně rozluští zprávu v šesté úloze, obdrží do dvojice skládanku (obrázek 20 rozstříhaný podle naznačených čar) a lísteček s náznakem pro číselný kód (viz poslední řádek v příloze 5). Sestavený obrázek obsahuje číslice a písmena; číslo ukazuje pořadí úlohy v pracovním listu *Cesta za pokladem* a písmeno je jedním znakem správné odpovědi na danou úlohu. Pořadí tohoto znaku ve slově udává jedno ze tří čísel kódu. Pro usnadnění jsou v obrázku znázorněny tři linky, stejně jako na zmiňovaném lístečku. Tyto linky napovídají, v jakém pořadí mají být číslice zapsány. Pomocí získaného číselného kódu děti otevřou krabici s pokladem.



Obrázek 20 - Skládanka

Ke každému úkolu je připravena nápověda, o kterou mohou děti požádat lístečkem se jménem jejich týmu a číslem úlohy, na kterou potřebují nápovědu. O nápovědu však mohou žáci požádat pouze čtyřikrát, proto si musí dobře rozmyslet, zda ji opravdu potřebují či nikoli. Aby nedošlo k nedorozumění, bude se počet vybraných nápověd zapisovat do archu s názvem *Přehled týmů* (již vyplněné archy jsou k vidění v příloze 6 a 7). Celý pracovní list a přesná zadání úloh jsou uvedeny v příloze 3, u každé úlohy je zelenou barvou uvedeno i její řešení.

Druhý zmiňovaný pracovní list dostanou také žáci sedmé třídy. Jak už bylo řečeno výše, sedmáci nebudou absolvovat přednášku o základech kryptologie, a tudíž nebudou seznámeni s příslušnou terminologií. Z tohoto důvodu byl pracovní list mírně upraven, aby jim neznalost terminologie nečinila příliš velké obtíže při řešení úkolů. Upravena byla převodová tabulka ve druhém cvičení (viz příloha 4), pro lepší pochopení byly doplněny některé znaky šifrové abecedy. Změny byly provedeny i s nápovědami. V příloze 5 jsou k nahlédnutí jak nápovědy pro šestou třídu, tak pozměněné nápovědy pro sedmáky. Žáci sedmé třídy budou mít k dispozici o jednu nápovědu více, tedy pět.

3.2 Realizace projektu

Následující podkapitoly se budou věnovat přípravě a průběhu vyučování. V první části bude stručně popsán obsah přednášky, tedy s čím budou žáci seznámeni. Budou zmíněny potřebné pomůcky a prostředky a také cíle výuky.

Druhá část se zaměří na popis průběhu výuky, jaké metody byly využity, kde výuka probíhala, jak se žáci zapojovali a podobně.

3.2.1 Příprava na vyučování

Součástí praktické části je také příprava na vyučování. Výstup bude veden formou výkladu na téma *Základy kryptologie*. Obsah přednášky si čtenář může přečíst v příloze 8, kurzívou jsou psány otázky pro žáky (podtržené modrou barvou).

Nejprve se žáci seznámí s pojmem kryptologie a jeho významem. Společně se žáky budou stanoveny důvody, proč lidé potřebují utajovat informace. Pro zajímavost budou žákům představeny dva historické příklady utajování zpráv. Pomocí těchto příkladů budou vysvětleny podobory kryptologie, tedy steganografie, kryptografie a kryptoanalýza. Poté budou zavedeny základní pojmy, které jsou nutností pro dobrou orientaci v oblasti šifrování, jako je šifra, otevřený a šifrový text, klíč a další. Děti se také dozví, co znamená substituční a transpoziční šifra, a budou jim představeny jednoduché šifrovací systémy, které lze řešit pouze pomocí tužky a papíru (například jednoduchá záměna, podle plotu, využití tabulek, …). Příprava obsahuje i informace a pokyny ke hře *Cesta za pokladem*.

Během výkladu bude žákům promítána prezentace pro lepší názornost a představu. Jednotlivé snímky prezentace jsou zobrazeny v příloze 9. V prezentaci byly vhodně použity animace, aby žáci měli čas na přemýšlení a formulaci odpovědí na zadávané

otázky. Informace, které jsou uvedeny v přípravě a prezentaci a budou přednášeny během výkladu, byly čerpány z bakalářské práce (Hájková, 2015).

Pro zpestření výuky a zvýšení zájmu žáků byla vytvořena pomůcka, která je vidět na obrázku 21. Pomůcka bude do vyučování vhodně zařazena, aby mohla žákům posloužit k lepšímu pochopení šifrovacího systému Skytala.

Obrázek 21 – Pomůcka pro děti (Skytala)

V rámci přípravy na vyučování byly také stanoveny cíle výuky, podle nichž bude žák schopen vysvětlit základní pojmy z oblasti kryptologie, uvést důvody šifrování, rozlišovat mezi pojmy šifrování, dešifrování a luštění, vyjmenovat některé možnosti šifrování či ukrývání textu, samostatně pracovat s některými uvedenými šifrovými systémy.

3.2.2 Průběh výuky

Výuka základů kryptologie probíhala v učebně s interaktivní tabulí, jak bylo předem domluveno s ředitelkou školy. Žáci nejprve obdrželi pracovní list s teorií a byli obeznámeni, jak s ním mají nakládat a že budou poznatky v něm uvedené ještě potřebovat. Potom, co zjistili, že si list mohou nechat, začali někteří po listu čmárat a malovat.

Následně byl zahájen výklad doprovázený prezentací. Žáci se aktivně hlásili a odpovídali na otázky. Správně jmenovali některé důvody šifrování, znali různé druhy neviditelných inkoustů (například citronovou šťávu) a možnosti, jak zviditelnit neviditelné písmo (zahřívání nad ohněm). Zkoušeli dešifrovat zprávu psanou pomocí Skytaly a většině se to podařilo. Žáky také zaujalo hledání textu skrytého v obrázku (viz snímek 9 v příloze 9) nebo možnosti ukrytí písmen zprávy do jiného textu.

Při probírání teorie (jako základní pojmy či dělení typů šifer) se děti soustředily méně. Někteří (většinou dívky) si doplňovali pojmy do pracovního listu, ale ostatní spíše některé části přeskočili a zkoušeli si například zašifrovat své jméno v prvním cvičení. Kvůli nedostatku času jsem byla nucena vynechat některé pojmy (kód, kódování, klíč), jejichž znalost nebyla pro plnění druhého pracovního listu tolik důležitá. Větší pozornost jsem věnovala tomu, aby žáci věděli, jak správně postupovat při šifrování

a dešifrování u jednoduchých substitučních a transpozičních šifer (například hledání znaků v převodové tabulce, čtení otevřeného textu v tabulce a další nezbytné kroky), neboť některé systémy těchto typů byly zařazeny do listu *Cesta za pokladem*.

Na konci výkladu měli žáci za úkol rozdělit se libovolně do dvojic a vymyslet název pro svůj tým. Vzniklo celkem devět dvojic. Po třídě koloval arch, kam žáci název týmu napsali (viz příloha 6). Po rozdělení byly děti seznámeny s pravidly hry, a sice se systémem úloh, s možnostmi nápověd, také bylo zdůrazněno, že k otevření truhly s pokladem potřebují trojciferné číslo. Žáci byli také upozorněni, že odměna je připravena pro každého z nich (na každé dítě vycházely dva pamlsky) a jak si mají počínat při vybírání svého podílu.

Společně se žáky jsme se dohodli, že mezi výkladem a hrou uděláme přestávku. Jak si skupinky počínaly při plnění úkolů, co jim dělalo největší potíže a co naopak, bude sepsáno v další kapitole, kde bude zmíněna i práce žáků sedmé třídy.

3.3 Vyhodnocení práce žáků

Po přestávce dostala každá dvojice pracovní list s názvem *Cesta za pokladem*. Většina žáků se zasekla již u první hádanky. Objevovaly se odpovědi jako tornádo, vítr, černá díra, tma. Na správnou odpověď přišly bezprostředně asi jen dvě dvojice, ostatní si braly nápovědu. Ty skupiny, které hádaly *noc* či *tmu*, měly sice špatnou odpověď, ale dostaly správný počet písmen, který potřebovaly v druhém úkolu. Nakonec ale všichni, kromě jedné dvojice, dospěli ke správné odpovědi.

Druhé cvičení bylo pro žáky velmi obtížné, neboť jim dělalo problém správně vyplnit šifrovou abecedu i přesto, že při výkladu byl zdůrazňován obdobný typ převodové tabulky (šifrová abeceda byla posunuta o sedm písmen doleva – viz sedmnáctý snímek v příloze 9). Proto jsem chodila mezi žáky a snažila se je navést na správnou cestu. Samotné dešifrování a hledání znaků otevřeného textu jim problém nedělalo, protože jsme společně několikrát opakovali směr orientace v tabulce při šifrování a dešifrování. Hledání písmenek v abecedě jim však trvalo velmi dlouho, zpráva na ně byla příliš dlouhá. V některých skupinkách si však vypomáhali tak, že jeden hledal znaky a druhý zapisoval. Žáky ale zpomalovalo i to, že si text nejprve psali na pomocný papír a potom ho přepisovali do pracovního listu. Cvičení ale dokončili všichni, až na dvě skupiny; jedna vůbec nezačala a druhá nedokončila.

Nad třetím úkolem všichni dlouho přemýšleli. Některé dvojice napadlo, že by mohly položky seřadit podle uvedených čísel nebo že čísla odkazují na nějaké písmeno v abecedě. Všichni ale nakonec dospěli ke správnému výsledku, pouze párkrát potřebovali poradit, že musí vynechat jednotky *kg* a *l*.

Se čtvrtou úlohou měli žáci překvapivě velké obtíže, ve většině případů je vůbec nenapadlo, že by mohli políčka vybarvovat. Jedné skupince nepomohla ani nápověda „Zkus pastelky“. Jedna dvojice zvolila sice špatný, ale velmi zajímavý postup; zmiňovaná políčka spojovala souvislou čarou. Dvě skupinky políčka křížkovaly, což

byl správný postup, ale výsledek nebyl příliš čitelný, proto žákům trvalo delší dobu, než na řešení přišli.

Až na jednu dvojici se všichni dobrali k nějaké odpovědi na páté cvičení. Nakonec pět týmů odpovědělo správně, dva týmy napsaly železnou bednu a jeden tým dřevěnou.

Poslední úloha byla pro žáky asi nejobtížnější. Kvůli časovému skluzu se k ní navíc některé dvojice vůbec nedostaly. Čtyři dvojice rozluštily první řádek psaný pozpátku a jedna dvojice dokázala rozluštit poslední řádek. Dívky z této skupiny dokonce správně zašifrovaly odpověď na pátou úlohu podle získaných pokynů, ale jejich řešení páté úlohy bylo špatné.

Protože už zbývalo jen pár minut do konce hodiny, dostaly všechny týmy skládanku. Nejrychleji obrázek složila opět dívčí dvojice (ta, která rozluštila poslední řádek šesté úlohy). Dívky potřebovaly pouze lehce napovědět, aby je napadlo, že obrázek skrývá odkazy na řešení úloh. Této dvojici se podařilo otevřít krabici s pokladem. Ostatní bohužel skládanku nestihli složit, proto jednotlivé dvojice obdržely lístečky s pořadovým číslem, podle kterých žáci následně přicházeli k truhle a vybírali si svou odměnu. Pořadí jim bylo přiřazeno podle počtu úloh, které se jim podařilo vyřešit, a podle toho, jak během hry pracovali.

Šesťáci se nebáli chodit pro nápovědy. Dva týmy využily plný povolený počet nápověd. Tři skupiny vyčerpaly pouze jednu nápovědu, mezi nimi byla i dvojice dívek, které řešily připravené úlohy samostatně a nejrychleji ze všech a úspěšně se dopracovaly až k odemčení truhly. Nejčastěji byla využita nápověda na první cvičení a nejméně si žáci brali nápovědu na čtvrtý úkol. Nápovědy využité jednotlivými týmy jsou zapsány v archu v příloze 6.

Sedmáci byli před začátkem hry také seznámeni s pravidly a byly jim vysvětleny pojmy *otevřený text* a *šifrový text*. Po zkušenostech s šestou třídou, byli také žáci sedmé třídy obeznámeni s existencí substitučních a transpozičních šifer a jejich stručným popisem. V sedmé třídě bylo vytvořeno celkem osm týmů.

Sedmá třída byla při řešení úloh o poznání výrazně rychlejší a nápaditější. Správnou odpověď na hádanku sice uhádly pouze dva týmy (opět se objevovala slova jako tornádo, vír, tma, ale i bagr, les a vesmír), ale všichni dokázali správně doplnit písmena do šifrové abecedy a dešifrovat text. I když se sedmáci nezdržovali psaním na pomocné papíry, hledání znaků v tabulce jim však také zabralo spoustu času.

O řešení třetího úkolu se tři dvojice vůbec nepokusily, ani nežádaly o nápovědu. Všichni ostatní nakonec ke správnému řešení došli, i když dva týmy potřebovaly „popostrčit“. Se čtvrtým úkolem nebyl žádný problém, všechny dvojice hned začaly vybarvovat nebo křížkovat, některé ani nepotřebovaly všechna písmenka.

Pátá úloha byla problémovější, dva týmy ji vůbec neřešily, další tři týmy vyzkoušely všechny odpovědi, dokud se nedobraly k té správné, a jeden tým dokonce odpověděl, že poklad není v žádné bedně.

K šesté úloze se dostaly pouze čtyři dvojice, z toho tři rozluštily první řádek a dvě dvojice i ten poslední. I sedmá třída měla svou dvojici „tahounů“, skládala se opět z dívek. Tato skupina byla nejrychlejší a povedlo se jí odevzdat lístek se zašifrovaným názvem bedny.

I když byli žáci sedmé třídy rychlejší, opět jsme se dostali do časového presu, a proto dostala skládanku pouze dívčí dvojice, která splnila všechny úkoly. Ostatní zase obdrželi lístečky s pořadím. Děvčatům se povedlo objevit číselný kód a otevřít truhlu.

Oproti šesté třídě sedmáci skoro vůbec nevyužívali nápovědy. O jednu nápovědu požádaly pouze tři týmy z osmi. Názvy všech týmů a využité nápovědy jsou uvedeny v příloze 7.

3.4 Hodnocení projektu žáky

Žáci šesté třídy dostali ještě krátký dotazník pro celkové zhodnocení projektu (viz příloha 10). Na základě vytvořeného dotazníku žáci anonymně hodnotili, co je na projektu nejvíce bavilo a naopak, co jim projekt přinesl a zda by se o kryptologii chtěli dozvědět více. V následujících odstavcích budou uvedeny některé z žákovských odpovědí.

Polovina třídy v různých formách uvedla, že nejvíce je na projektu bavila hra *Cesta za pokladem*. Někteří odpovídali obecně (například „*ta druhá část hodiny*“ nebo „*hra Cesta za pokladem*“), jiní byli konkrétnější („*dešifrování abecedy, hádání vět a skládačka*“, „*malování*“, „*abeceda*“, „*luštění*“, …). Tři žáky nejvíce bavilo vybírání a pojídání sladkostí a jednomu žákovi se líbilo, že odpadly hodiny, které měli mít původně.

Na otázku, co mě docela bavilo, se sešly odpovědi jako například „*luštění úkolů*“, „*pokoušet se vyhrát poklad*“, „*šifrování*“, objevily se ale také reakce „*jíst bonbony*“ a „*vybarvování čtverečků*“. Jednu z dívek docela bavila „*první část hodiny, konkrétně ty druhy, jak se to může skrýt*“. Šest žáků na tuto otázku nijak nereagovalo nebo napsali slovo „*nic*“.

Více jak polovina třídy různými slovy napsala, že je nejvíce nebavila prezentace a vyplňování prvního pracovního listu. Část respondentů opět odpověděla slůvkem „*nic*“, našla se ale i odpověď „*všechno mě bavilo*“.

Většina žáků se podle odpovědí v dotazníku díky projektu dozvěděla spoustu zajímavostí z kryptologie. Žáci zjistili, že existují různé druhy šifer a možnosti ukrytí vzkazů. Zaujal je například příběh Histiaia a jeho otroka s oholenou hlavou. Velmi zajímavé bylo přání jedné žačky, která napsala, že by chtěla ukrývání textu naučit někoho jiného (viz příloha 11).

Na otázku, co by žáci udělali jinak, se sešlo několik zajímavých návrhů. Děti by například provedly výuku zábavnější formou a zpomalily při přednášení, poskytly by více času na hru nebo by udělaly lehčí úlohy a změnily nápovědy. Někomu se také

zdálo, že v truhle bylo málo sladkostí. Velká část třídy ale nechala řádky u této otázky nepopsané.

Počet kladných a záporných odpovědí na otázku, zda by se děti chtěly o šifrování dozvědět více, byl vyrovnaný. Jeden z žáků se zdržel odpovědi a další žák připsal alternativu „*možná*“. U poslední otázky, zda by mělo být šifrování vyučováno ve škole, bylo vícekrát zakroužkováno *ano*, na jednom listu byly zakroužkovány obě odpovědi. Jeden z žáků reagoval na poslední dvě otázky podivně; zakroužkoval, že by se o šifrování nechtěl dozvědět více, na druhou stranu by ale chtěl, aby se šifrování vyučovalo ve škole.

Někteří žáci stihli při hodnocení projektu dokonce vybarvit smajlíky, které byly do dotazníku vloženy pro odlehčení. V příloze 11 a 12 si čtenář může prohlédnout odpovědi ze dvou vybraných dotazníků.

ZÁVĚR

Cílem diplomové práce bylo začlenit základní poznatky z oblasti kryptologie do výuky informatiky na druhém stupni základní školy. Z tohoto důvodu byl navržen projekt sestávající ze tří částí; empirického šetření, výuky základů kryptologie a pracovních listů pro žáky. Projekt byl uskutečněn na Základní škole Nasavrky, konkrétně v šesté a sedmé třídě (sedmá třída představovala kontrolní skupinu).

Diplomová práce je členěna na tři hlavní kapitoly, a sice teoretickou, empirickou a praktickou. V rámci teoretické části se čtenář nejprve seznamuje s několika druhy organizačních forem a metod výuky, zvláště pak s aktivizačními metodami. Část textu je také věnována pojmu myšlení a možnostem jeho kultivace.

Další kapitola této části přináší přehled základních pojmů z oblasti kryptologie, které jsou důležité pro správnou a efektivní manipulaci s šifrovými systémy. Následně je čtenář seznámen s vybranými jednoduchými šifrovými systémy, které jsou vhodné pro začátečníky a lze je využít za pomoci tužky a papíru. Jedná se o výběr ze substitučních, transpozičních a grafických šifer. Pro lepší představu byly do textu vloženy vhodné příklady a obrázky. Cílem teoretické části bylo mimo jiné popsat roli kryptologie ve vyučování informatiky a představit možnosti propojení kryptologie s dalšími předměty.

Pro účely výzkumu v rámci empirické části diplomové práce byl vytvořen dotazník vlastní konstrukce, který zjišťoval kompetence žáků šestého a sedmého ročníku pro zvládnutí učiva základů kryptologie.

Ze získaných výsledků vyplynul spíše neutrální, v některých případech až negativní, přístup k logickým úlohám, křížovkám a hlavolamům. Stejně tak tomu bylo i v případě projevení zájmu o výuku šifrování a dešifrování. Přestože nejvíce zastoupená odpověď byla kladná, celkové stanovisko všech respondentů bylo opět neutrální. Příčina tohoto přístupu byla interpretována jako nezkušenost a neschopnost utvořit si konkrétní představu o problematice kryptologie či řešení logických úloh. Nezájem dětí o křížovky a hlavolamy byl vysvětlen uspěchaností dnešní doby a velkým množstvím času, který děti tráví u počítače.

Možností vedoucí ke zdokonalení výzkumu do budoucna by mohlo být například zahrnutí otevřené otázky, která by navazovala na otázku 15 (viz příloha 1), kde by respondenti vysvětlili, z jakého důvodu volili svou odpověď. Takto by mohl být zjištěn pravý důvod nezájmu o výuku kryptologie.

V poslední, tedy praktické, části práce je popsána příprava a realizace projektu. V první řadě byly zhotoveny pracovní listy, podle kterých se následně odvíjela příprava na vyučování. Popis jednotlivých pracovních listů je obsažen v první kapitole praktické části. Cílem dalších kapitol bylo seznámit čtenáře s přípravou na vyučování, tedy obsahem výkladu, vytvořenými pomůckami a stanovenými cíli výuky, ale také s tím, jak výuka probíhala, jaké formy a metody byly využity a jak se při výkladu chovali žáci.

Po přečtení další části textu čtenář zjistí, jak si vedli žáci obou tříd při vyplňování pracovních listů, tedy při hře nazvané *Cesta za pokladem*. Při plnění jednotlivých úkolů

žáci bojovali hlavně s časem. Nejvíce času jim zabral druhý úkol, zašifrovaná zpráva byla příliš dlouhá. V důsledku nedostatku času nestihli žáci dořešit všechny úlohy a na skládanku se tedy buď nedostalo, nebo žáci nestihli obrázek složit. V obou třídách se ale našla dvojice (v obou případech dvojice dívek), která se dokázala propracovat všemi úlohami a otevřít krabici s pokladem.

Celkově si žáci sedmé třídy vedli lépe než šesťáci i přesto, že neabsolvovali přednášku o základech kryptologie. Šesťáci nad každou úlohou dlouze přemýšleli, sedmáci naopak ihned zkoušeli různé možnosti řešení. Tuto skutečnost bychom mohli vysvětlit tím, že u žáků sedmé třídy by již mělo být plně rozvinuto abstraktní myšlení, kdežto někteří šesťáci mohou stále potřebovat konkrétní představy pro řešení úloh a problémů.

Žákům šesté třídy byly ještě předloženy dotazníky, na jejichž základě žáci hodnotili, co se jim na projektu líbilo a nelíbilo či co by udělali jinak. Nejčastější odpovědi jsou sepsány v poslední kapitole praktické části.

Hlavní a důležitou změnou pro budoucí vylepšení projektu je zvýšení časové dotace pro výuku a obzvlášť pro hru. Do výuky by mělo být začleněno více pomůcek a konkrétních příkladů pro zvýšení aktivity a zájmu žáků. U jednotlivých úloh v pracovním listu *Cesta za pokladem* by měla být snížena náročnost nebo samotný počet úloh. Také nápovědy by měly být upraveny tak, aby hodnota jejich sdělení byla pro žáky přínosnější.

Začlenění kryptologie do výuky informatiky by znamenalo možnost rozvoje algoritmického, logického, tvořivého a samostatného myšlení u žáků, kultivace jejich dovedností a znalostí z hlediska dalších předmětů v rámci mezipředmětových vztahů, dále také možnost poučit žáky o počítačové bezpečnosti důkladněji a zábavnější formou, možnost zpestření vyučování nejen informatiky, ale i matematiky, dějepisu, a dalších předmětů.

Na druhé straně efektivní zavedení kryptologie do výuky není záležitost dvou hodin, problematika kryptologie je velmi rozsáhlá, a proto je nutné znalosti a dovednosti týkající se této oblasti soustavně rozšiřovat a zdokonalovat. Ne každá základní škola však má informatiku dostatečně časově dotovanou na to, aby se v jejím rámci mohly základy kryptologie vyučovat nebo se jim mohlo důkladně a dlouhodobě věnovat.

Stanovené cíle diplomové práce byly splněny. Byly zjištěny kompetence ke zvládnutí daného učiva a byl prozkoumán zájem žáků o šifrování. Došlo k začlenění jednoduchých šifrových systémů a základů z oblasti kryptologie do výuky informatiky v podobě přednášky a připravených pracovních listů. Došlo ke zhodnocení a interpretaci získaných výsledků a byly uvedeny výhody a nevýhody začlenění kryptologie do výuky informatiky na druhém stupni základní školy.

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM POUŽITÉ LITERATURY

BERRY, D. C., & MILLER, M. G. (2008). Crossword puzzles as a tool to enhance athletic training student learning: Part 2. *Athletic Therapy Today*, *13*(1), 32-34.

BITTO, Ondřej. *Historie kryptologie* [online]. [cit. 2016-11-05]. Dostupné z: http://www.fi.muni.cz/usr/jkucera/pv109/2003/xbitto.htm

CÁPAY, Martin, MAGDIN, Martin. Hlavolamy, kódy a šifry podporujúce algoritmické myslenie. In: *Alternativní metody výuky 2011: 9. ročník mezinárodní konference*. Hradec Králové: Gaudeamus, 2011. ISBN 978-80-7435-104-4.

Crypto-World [online]. [cit. 2016-11-05]. Dostupné z: http://crypto-world.info/

ČERNOCHOVÁ, Miroslava, KOMRSKA, Tomáš, NOVÁK, Jaroslav. *Využití počítače při vyučování: náměty pro práci dětí s počítačem*. 1. vyd. Praha: Portál, 1998, 165 s. ISBN 80-717-8272-6.

DOSEDĚL, Tomáš. *21 základních pravidel počítačové bezpečnosti*. 1. vyd. Brno: CP Books, 2005, 56 s. ISBN 80-251-0574-1.

FISHER, Robert. *Učíme děti myslet a učit se: praktický průvodce strategiemi vyučování*. 1. vyd. Praha: Portál, 1997, 176 s. Pedagogická praxe. ISBN 80-717-8120-7.

FOŘTÍKOVÁ, Jitka. Dílčí oblasti rozumových schopností a jak je rozvíjet: *Popis jednotlivých oblastí intelektu s výčtem vhodných aktivit pro jejich rozvoj* [online]. s. 11, 2016 [cit. 2016-11-05]. Dostupné z: http://lvicata.cvut.cz/system/files/skolka/dokumenty/oblasti_rozumovych_schopnosti.pdf

HÁJKOVÁ, S. *Luštění transpozičních šifer s podporou počítače*. Hradec Králové, 2015. Bakalářská práce na Přírodovědecké fakultě Univerzity Hradec Králové. Vedoucí bakalářské práce PhDr. Michal Musílek, Ph.D. 41 s.

CHYTRÝ, Vlastimil. *Logika, hry a myšlení*. 1. vyd. Ústí nad Labem: Univerzita J.E. Purkyně v Ústí nad Labem, 2015, 159 s. ISBN 978-80-7414-909-2.

JANEČEK, Jiří. *Gentlemani (ne)čtou cizí dopisy*. 1. vyd. Brno: BOOKS, 1998. 176 s. ISBN 80-85914-90-5.

JUKLOVÁ, Kateřina. *Základy obecné psychologie: studijní text*. 5. vyd. Hradec Králové: Gaudeamus, 2012, 56 s. ISBN 978-80-7435-221-8.

KALHOUS, Zdeněk, OBST, Otto a kol. *Školní didaktika*. 2. vyd. Praha: Portál, 2009, 447 s. ISBN 978-80-7367-571-4.

Logické úlohy. In: *E-rebus* [online]. [cit. 2016-11-05]. Dostupné z: http://www.e-rebus.cz/index.php?link=lu001

MAŇÁK, Josef. Aktivizující výukové metody. In: *Metodický portál: inspirace a zkušenosti učitelů* [online]. 2011 [cit. 2017-01-28]. Dostupné z: http://clanky.rvp.cz/clanek/c/o/14483/AKTIVIZUJICI-VYUKOVE-METODY.html/

MAŇÁK, Josef. *Nárys didaktiky*. 3. vyd. Brno: Masarykova univerzita v Brně, 2003, 104 s. ISBN 80-210-3123-9

MELICHAR, Jan, SVOBODA, Josef. *Rozvoj matematického myšlení I pro studium učitelství pro mateřské školy*. 1. vyd. Ústí nad Labem: Univerzita Jana Evangelisty Purkyně, 2003, 62 s. ISBN 80-704-4512-2.

MUSÍLEK, Michal. *Kapitoly z dějin informatiky*. 1. vyd. Univerzita Hradec Králové: Gaudeamus, 2011. 193 s. ISBN 978-80-7435-129-7.

MUSÍLEK, Michal, HUBÁLOVSKÝ, Štěpán. Počítačová bezpečnost ve výuce informatiky: (1. část - Tvorba hesel a steganografie). *Matematika, fyzika, informatika* [online]. 2010, **20**(3) [cit. 2017-01-29]. Dostupné z: http://mfi.upol.cz/old/MFI_20_pdf/INF_20_03.PDF

MUSÍLEK, Michal, HUBÁLOVSKÝ, Štěpán. Počítačová bezpečnost ve výuce informatiky: (7. část - snadné transpoziční šifry a výuka programování). *Matematika, fyzika, informatika* [online]. 2013, **22**(1), [cit. 2017-02-13]. Dostupné také z: http://mfi.upol.cz/index.php/mfi/article/view/9/7

PAZOUREK, Karel. *Rekreační šifrování: Šifry Školní šifrovací soutěže 2013-2014* [online]. 2014 [cit. 2016-11-05]. Dostupné z: http://www.gymtrebon.cz/UserFiles/pazourek/sifra1415/Prirucka3.pdf

PELÁNEK, Radek. *Hlavolamikon: Sbírka hlavolamů, hádanek, šifer a logických úloh*. 1. vyd. Brno: Computer Press, 2014. 240 s. ISBN 978-80-251-4303-2.

PIPER, Fred, MURPHY, Sean. *Kryptografie: Průvodce pro každého*. 1. vyd. Praha: Dokořán, 2006. 158 s. ISBN 80-7363-074-5.

SEHNALOVÁ, Vladimíra. *Rozvoj logického myšlení s ICT* [online]. 2013, 34 [cit. 2016-11-05]. Dostupné z: http://www1.osu.cz/~sehnalova/publikace/2013sehlog.pdf

SINGH, Simon. *Kniha kódů a šifer: Tajná komunikace od starého Egypta po kvantovou kryptografii*. 2. vyd. Praha: Dokořán a Argo, 2009. 382 s. ISBN 978-80-7363-268-7 (Dokořán) a 978-80-257-0144-7 (Argo).

SOTONA, Jiří. *Milovníci slovíčkaření aneb Proč máme tak rádi křížovky*. In: *Novinky.cz* [online]. 2016 [cit. 2016-11-05]. Dostupné z: http://www.novinky.cz/zena/styl/396706-milovnici-slovickareni-aneb-proc-mame-tak-radi-krizovky.html

SPITZER, Manfred. *Digitální demence: jak připravujeme sami sebe a naše děti o rozum*. Brno: Host, 2014. ISBN 978-80-7294-872-7.

Technoplaneta [online]. [cit. 2016-11-15]. Dostupné z: http://technoplaneta.cz/

TŮMA, Jiří. *Transpozice*. [online]. [cit. 2016-11-05]. Dostupné z: http://www.karlin.mff.cuni.cz/~tuma/ciphers/Sifry4.pdf

VONDRUŠKA, Pavel. *Kryptologie, šifrování a tajná písma*. 1. vyd. Praha: Albatros, 2006. 344 s. ISBN 80-00-01888-8.

ZORMANOVÁ, Lucie. *Obecná didaktika: Pro studium a praxi*. 1. vyd. Praha: Grada Publishing, 2014, 240 s. ISBN 978-80-247-4590-9.

ZOUBEK, Vilém. *Šifry*. In: *Podskaláček* [online]. 1998 [cit. 2017-01-31]. Dostupné z: http://www.zoubek.cz/homepage/sifry/

SEZNAM PŘÍLOH

PŘÍLOHA 1 – Dotazník vlastní konstrukce

KRYPTOLOGIE NA ZÁKLADNÍ ŠKOLE - dotazník

Ahoj,

jsem studentka Přírodovědecké fakulty Univerzity Hradec Králové a v rámci své diplomové práce (to je takový hóódně dlouhý referát) chci zjistit, jaký význam bude mít vyučování kryptologie (to jsou různé druhy šifer a hádanek) v hodinách informatiky. A proto přichází na řadu dotazník, který právě držíš v ruce. Díky němu získám větší přehled o tom, jestli mám vůbec šanci s výukou šifer uspět a jak je pro Tebe tato výuka důležitá.

Vyplnění dotazníku ti zabere jen pár minut. Dotazník je anonymní, to znamená, že se nemusíš podepisovat. Chci tě ale poprosit, abys na otázky odpovídal/a podle pravdy. Stačí zakřížkovat správnou odpověď, asi takto: ☒
Pokud si svou odpověď rozmyslíš, zaškrtnutý čtvereček zabarvi a zakřížkuj novou možnost: ■→ ☒
U některých otázek můžeš také odpovídat vlastními slovy.

Tak se pusť do toho!

1. Luštíš křížovky (např.: švédská křížovka, klasická křížovka – s legendou mimo obrazec, osmisměrka, kris-kros, doplňovačka s tajenkou, ...)? Jak často?

   ☐ Několikrát týdně
   ☐ Jednou týdně
   ☐ 1 až 3x měsíčně
   ☐ Několikrát za rok
   ☐ Nikdy

2. Jestliže jsi v předchozí otázce odpověděl „nikdy", tuto otázku přeskoč. Jaký typ křížovek luštíš nejradši? Zde můžeš zakroužkovat více možností.

   ☐ Švédská křížovka
   ☐ Osmisměrka
   ☐ Kris-kros
   ☐ Klasická křížovka – s legendou mimo obrazec
   ☐ Doplňovačka s tajenkou
   ☐ Jiné – napiš jaké: _____

3. Už jsi někdy luštil/a osmisměrku? Jakým způsobem ji řešíš?

   ☐ Hledám postupně všechna slova z nabídky
   ☐ Ve změti písmen hledám smysluplné slovo, potom se přesvědčím, že je uvedeno v nabídce

4. Máš rád/a hádanky?

   ☐ Určitě ne
   ☐ Spíše ne
   ☐ Nevím
   ☐ Spíše ano
   ☐ Určitě ano

5. Baví tě řešit logické matematické úlohy a hlavolamy?

   ☐ Určitě ne
   ☐ Spíše ne
   ☐ Nevím
   ☐ Spíše ano
   ☐ Určitě ano

6. Je pro tebe řešení logických úloh a hlavolamů obtížné?

   ☐ Určitě ne
   ☐ Spíše ne
   ☐ Nevím
   ☐ Spíše ano
   ☐ Určitě ano

7. Kde se s hlavolamy, hádankami a logickými úlohami nejčastěji setkáváš?

   ☐ Ve škole
   ☐ Doma
   ☐ V kroužku nebo klubu
   ☐ Jinde – napiš kde: _____

8. Setkal/a jsi se někdy s nějakou formou utajení textu (např.: neviditelný inkoust, přeházená písmenka, ...)?

   ☐ Ne
   ☐ Nevím
   ☐ Ano

9. Jestliže jsi v předchozí otázce odpověděl „ano“, napiš, o jakou formu utajení se jednalo:

   _____

10. Používáš sám/sama nějakou formu utajení zprávy? Pokud ano, napiš jakou.

    ☐ ne
    ☐ ano – napiš jakou: _____

11. Znáš nějaký způsob šifrování? Pokud ano, napiš jaký.

    ☐ Ne
    ☐ Ano – napiš jaký: _____

12. Zkus správně přiřadit definici k pojmu:

Transpoziční šifra	Forma ukrývání textu.
Substituční šifra	Změna pořadí písmen v textu.
Steganografie	Písmena v textu jsou zaměněna za jiná písmena nebo znaky podle určitého pravidla.

13. Víš, co znamená slovo „anagram“?

    ☐ Ne
    ☐ Ano

14. Pokud jsi v předchozí otázce odpověděl „ano“, napiš nějaký příklad anagramu:

    _____

15. Chtěl/a bys, aby se v informatice vyučovaly způsoby šifrování a dešifrování?

    ☐ Určitě ne
    ☐ Spíše ne
    ☐ Nevím
    ☐ Spíše ano
    ☐ Určitě ano

16. Máte ve školním časopise křížovky a hlavolamy?

    ☐ Ne
    ☐ Nevím
    ☐ Ano

17. Řešíš křížovky a hlavolamy ve Vašem školním časopise?

    ☐ Ne
    ☐ Ano

18. Uvítal/a bys ve Vašem školním časopise více křížovek, hlavolamů a podobných úloh na zamyšlení?

    ☐ Určitě ne
    ☐ Spíše ne
    ☐ Nevím
    ☐ Spíše ano
    ☐ Určitě ano

Jsi na konci!

Děkuji Ti za pomoc při psaní mé diplomové práce!

PŘÍLOHA 2 – Pracovní list Základy kryptologie

ZÁKLADY KRYPTOLOGIE – pracovní list

Kryptologie = nauka o _____.

Důvody, proč šifrujeme:

- Ochrana dat a tajných informací – např.: _____
  _____
- Tajná korespondence – např.: _____
  _____

První pokusy o šifrování se objevily již v ___ st. _____. Jednalo se spíše o utajení samotné existence tajných zpráv.

Například příběh o Histiaiovi, který nechal svému poslovi _____ _____, vytetoval mu tam tajnou zprávu, nechal mu dorůst _____ a poslal ho za svým zetěm Aristagorem.

Skytala je označení pro _____, na kterou se navinul pruh látky či papyru a na něj se zapsala tajná zpráva. Odvinutý pruh se mohl použít jako _____. Příjemce zprávy musel proužek _____ na _____ o stejném _____, aby si mohl zprávu přečíst.

Odvětví kryptologie - Přiřaď k definici správný pojem:

Kryptoanalýza	Utajování existence zpráv. Metody: _____ _____ _____
Steganografie	Luštění tajných zpráv bez znalosti šifrovacího klíče a pravidel.
Kryptografie	Souhrn metod pro změnu podoby textu tak, aby byl pro nepovolaného člověka nečitelný.

Základní pojmy

_____ = nahrazování písmen zprávy jinými písmeny, číslici nebo znaky

_____ = slovo, číslo nebo symbol, které nahrazuje jiné slovo nebo skupinu slov

_____ = text po zašifrování, jeví se jako náhodná kombinace znaků

_____ = srozumitelný text psaný v běžném jazyce, který chceme zašifrovat

_____ = souhrn pravidel, podle kterých probíhá šifrování

_____ = postup vytváření šifrového textu

_____ = převést šifrový text na otevřený, příjemce musí znát klíč i algoritmus

_____ = převést otevřený text na šifrový pomocí šifrovacího algoritmu a klíče

_____ = převod šifrového textu na otevřený bez znalosti klíče a pravidel šifrování

_____ = převod textu do podoby vhodné pro vysílání elektrických, zvukových či optických signálů

Typy šifer – nehodící se škrtni:

Záměna znaků otevřeného textu za znaky šifrové abecedy: substituční š. transpoziční š.

Změna pořadí znaků v otevřeném textu dle určitých pravidel: substituční š. transpoziční š.

Úloha 1

K dispozici máš substituční tabulku šifry atbaš. Zašifruj pomocí této tabulky své křestní jméno.

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A

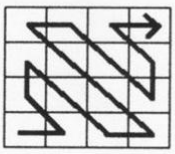
OT: _____ (tvoje jméno)

ŠT: _____

Jednoduché transpoziční šifry – pozpátku, ob dvě písmena, střídání první a poslední pozice, „podle plotu", transpoziční tabulky, ...

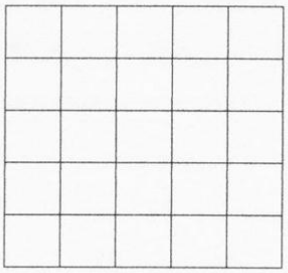
Úloha 2

Kamarád ti poslal tajnou zprávu. Předem jste se domluvili, že budete šifrovat pomocí tabulky, která je uvedena na obrázku. Dešifruj jeho zprávu.



Tajná zpráva: KHRNI SROOE EAYVZ STNSE NAAJJ

Otevřený text: _____



PŘÍLOHA 3 – Pracovní list Cesta za pokladem (verze pro 6. třídu) s řešením

CESTA ZA POKLADEM

1. **Hádanka na zahřátí:**

   Všechno žere, všechno se v něm ztrácí, stromy, květy, zvířata i ptáci; hryže kov i pláty z ocele, tvrdý kámen na prach semele; města rozvalí a krále skolí, vysokánské hory svrhne do údolí. Co je to?

   Řešení: ČAS

2. **Přítel ti posílá tajnou informaci. Dešifruj zprávu, jestliže víš, že odesílatel při šifrování posunul šifrovou abecedu doleva o tolik písmen, kolik jich má odpověď na předchozí hádanku.**

OT:	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
ŠA:	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

   Šifrový text: SUHVPBFNB MVRX GYRMLFH VORY NWHUD PDML VWHMQD SLVPHQD DOH MLQDN XVSRUDGDQD QDSULNODG SRVWHO D OHSRVW

   Otevřený text: PŘESMYČKY JSOU DVOJICE SLOV KTERÁ MAJÍ STEJNÁ PÍSMENA ALE JINAK USPOŘÁDANÁ NAPŘÍKLAD POSTEL A LEPOST

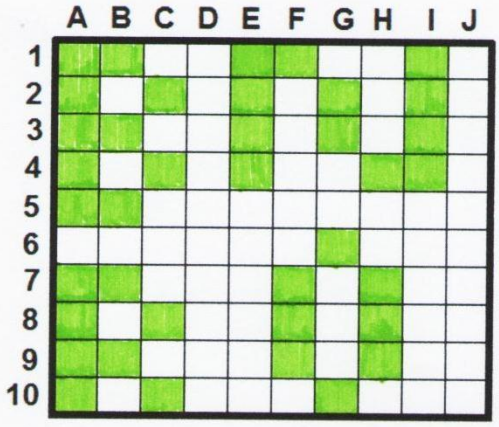
3. **Co zapomněla koupit paní Nováková?**

   Nákupní seznam

   3 cibule
   2 kg brambor
   4 jogurty
   1 salátová okurka
   7 mandarinek
   3 konzervy pro kočky
   4 l mléka
   2 ryby

   Řešení: BRUSINKY

4. **Ve kterém městě se odehrává bitva?**



Tajemné souřadnice:

1A	1B	2A	2C	3A	3B
4A	4C	5A	5B	7A	7B
8A	8C	9A	9B	10A	10C
1E	1F	1I	2E	2G	2I
3E	3G	3I	4E	4H	4I
6G	7F	7H	8F	8H	9F
9H	10G				

Řešení: BRNO

5. **Ve které bedně je poklad?**

Na každé bedně jsou dva nápisy. Na jedné bedně jsou oba nápisy pravdivé, na druhé jeden pravdivý a jeden nepravdivý, na třetí oba nepravdivé.

Železná bedna: „Zde není poklad.“ (P), „Poklad je v dřevěné bedně.“ (N)

Dřevěná bedna: „Poklad není v železné bedně.“ (P), „Poklad je v papírové bedně.“ (P)

Papírová bedna: „Zde není poklad.“ (N), „Poklad je v železné bedně.“ (N)

Odpověď: PAPÍROVÁ BEDNA

6. **Do rukou se ti dostala tajná zpráva od nepřátel. Pokus se ji rozluštit.**

Šifrový text: EJUTS IXEME DALKO PSAND EB

KDMEIRHYORBJSRJITYIENKD (1 3 5 7 ...)

OECNTULPTEUETOMSNCSLYO (2 4 6 8 ...)

SOIPUPRURALEVOSNHMOUYUZCOAKDSYPIAOFOVRDEUEDJVNPZAODPMEAOJTC

Otevřený text: BEDNA S POKLADEM EXISTUJE K ODEMČENÍ TRUHLY POTŘEBUJEŠ TROJMÍSTNÝ ČÍSELNÝ KÓD SPRÁVNOU ODPOVĚĎ NA PÁTOU ÚLOHU ZAŠIFRUJ POMOCÍ PŘESMYČKY A ODEVZDEJ

ČÍSELNÝ KÓD: 3 8 2

PŘÍLOHA 4 – Pracovní list Cesta za pokladem (verze pro 7. třídu)

CESTA ZA POKLADEM

1. **Hádanka na zahřátí:**

   Všechno žere, všechno se v něm ztrácí, stromy, květy, zvířata i ptáci; hryže kov i pláty z ocele, tvrdý kámen na prach semele; města rozvalí a krále skolí, vysokánské hory svrhne do údolí. Co je to?

   Řešení:_____

2. **Přítel ti posílá tajnou informaci. Dešifruj zprávu, jestliže víš, že odesílatel při šifrování posunul šifrovou abecedu doleva o tolik písmen, kolik jich má odpověď na předchozí hádanku.**

   Převodová tabulka:

Otevřený text	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Šifrová abeceda				G	H		J			M	N	O		Q			T	U		W		Y	Z		B	

   Šifrový text: SUHVPBFNB MVRX GYRMLFH VORY NWHUD PDML VWHMQD SLVPHQD DOH MLQDN XVSRUDGDQD QDSULNODG SRVWHO D OHSRVW

   Otevřený text: _____

   _____

   _____

3. **Co zapomněla koupit paní Nováková?**

   Nákupní seznam

   3 cibule

   2 kg brambor

   4 jogurty

   1 salátová okurka

   7 mandarinek

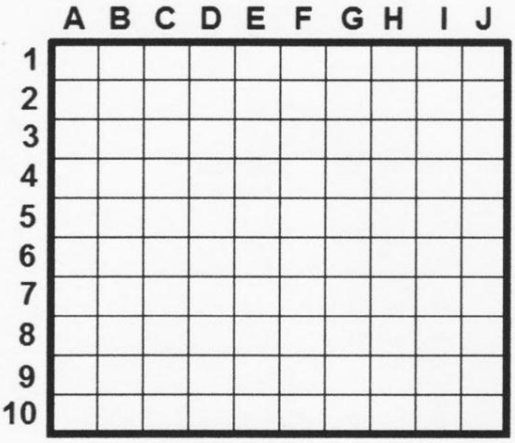
   3 konzervy pro kočky

   4 l mléka

   2 rybí pomazánky

   Řešení: _____

4. **Ve kterém městě se odehrává bitva?**



Tajemné souřadnice:

1A	1B	2A	2C	3A	3B
4A	4C	5A	5B	7A	7B
8A	8C	9A	9B	10A	10C
1E	1F	1I	2E	2G	2I
3E	3G	3I	4E	4H	4I
6G	7F	7H	8F	8H	9F
9H	10G				

Řešení: _____

5. **Ve které bedně je poklad?**

Na každé bedně jsou dva nápisy. Na jedné bedně jsou oba nápisy pravdivé, na druhé jeden pravdivý a jeden nepravdivý, na třetí oba nepravdivé.

Železná bedna: „Zde není poklad.“, „Poklad je v dřevěné bedně.“

Dřevěná bedna: „Poklad není v železné bedně.“, „Poklad je v papírové bedně.“

Papírová bedna: „Zde není poklad.“, „Poklad je v železné bedně.“

Odpověď: _____

6. **Do rukou se ti dostala tajná zpráva od nepřátel. Pokus se ji rozluštit.**

Šifrový text: EJUTS IXEME DALKO PSAND EB

KDMEIRHYORBJSRJITYIENKD OECNTULPTEUETOMSNCSLYO

SOIPUPRURALEVOSNHMOUYUZCOAKDSYPIAOFOVRDEUEDJVNPZAODPMEAOJTC

Otevřený text: _____

_____

_____

PŘÍLOHA 5 – Nápovědy k jednotlivým úkolům

NÁPOVĚDY

1. úkol

Nemá křídla, ale letí, nemá nohy, ale běží. Na vysoké hradní věži hodiny ho přísně střeží.

2. úkol

OT:	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
ŠA:	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Verze pro 7. třídu: Přítel použil substituci, to znamená, že zaměnil znaky textu za znaky šifrové abecedy.

3. úkol

Číslo nemusí znamenat pouze počet nebo množství, má i více významů.

4. úkol

Zkus pastelky.

5. úkol

Poklad není v železné bedně.

6. úkol

Nepřátelské skupině unikla informace, že každý řádek zprávy zašifrovali jiným typem transpozice.

Verze pro 7. třídu: Nepřátelské skupině unikla informace, že zprávu zašifrovali pomocí transpozice, tj. přeházeli písmenka zprávy podle různých pravidel, např. ob jedno písmeno, pozpátku, první a poslední, ... Každý řádek, jiná transpozice.

7. úkol

Řešení úloh.

KÓD ZÁMKU: ___ ___ ___

PŘÍLOHA 6 – Přehled týmů 6. třídy

PŘEHLED TÝMŮ – 6. TŘÍDA

Čas zahájení: 11:50

Jméno týmu	Využité nápovědy	Čas
THE LOST PENGUIN	1.,5.,6.	45 min
X Azeret a ša idot	4,3,5,6	45 min
Gripe a QZPFY	1.3.	-"-
PLÁČAČKY	5.	-"-
TYKVE	2.	-"-
Slimáci	1.	-"-
class	2.,5.,6	-"-
X dementi	1.,3.,2.,4.	-"-
pokémoni	1.,3.,6.	-"-

PŘÍLOHA 7 – Přehled týmů 7. třídy

PŘEHLED TÝMŮ – 7. TŘÍDA

Čas zahájení: 11:00

Jméno týmu	Využité nápovědy	Čas
PRINCESSUNICORN		40 min.
DOMA	6.	-11-
DANGER STRIPERS	1.	-11-
FICHTLAŘI	6.	-11-
dva spolužáci a 1 kamarád		-11-
KOZY		-11-
Justmenky		-11-
PTÁČCI - PANI		-11-

PŘÍLOHA 8 – Obsah přednášky o základech kryptologie

ZÁKLADY KRYPTOLOGIE – příprava na vyučování

Na začátku rozdat pracovní listy!!!

Co vás napadne, když se řekne kryptologie? Čím se asi zabývá?

Kryptologie je nauka o šifrování.

Co se vám vybaví pod slovem šifrování?

Šifrovat znamená převést text do takové podoby, která je pro nepovolaného člověka zcela nesrozumitelná a nečitelná.

Důvody šifrování

Proč podle vás lidé používají různé metody šifrování?

Šifrování umožňuje ochránit citlivé či tajné informace před očima nepovolaných lidí. Velmi často se v praxi zabezpečují data o osobách (např. přístup k registrům s osobními údaji je zabezpečen a i samotné údaje jsou převedeny do bezpečného formátu), vědci zase šifrují své objevy, aby je nikdo nemohl vydávat za své nebo je nějakým způsobem zneužít (např. výroba výbušnin)). Ale i my každý den něco utajujeme, pomocí hesla zabezpečujeme přístup do počítače nebo k různým účtům.

Šifruje se ale i za účelem tajné korespondence. Děti na táborech a ve školách si posílaly tajná psaníčka a šifrovaly jejich obsah, aby si je nemohli ostatní přečíst. Šifrují se ale i vážnější a důležitější zprávy, například válečné depeše o strategiích boje či informacích o nepříteli.

Pohled do historie

Kdy podle vás lidé začali používat různé formy utajení textu?

První pokusy o utajení textu se objevili už v pátém století před naším letopočtem. Jednalo se ale spíš o utajení existence zprávy než jejího obsahu. Například v Persii chtěl Histiaios poslat vzkaz svému zeti Aristagorovi Milétskému a tak oholil svému otroku hlavu, vytetoval na ni svůj vzkaz, a když otroku dorostly vlasy, poslal ho do Řecka. Aristagoras mu musel vlasy zase oholit, aby si mohl vzkaz přečíst.

Dalším příkladem je Skytala, což je nejstarší šifrovací systém, který používali v Persii. Skytala se jmenuje podle dvou holí, neboli *skytalé*, jednu měl odesílatel a druhou příjemce zprávy. Odesílatel na hůl navinul nějaký pruh látky či papyru, napsal na něj zprávu a poslal ji po svém poslovi. Ten mohl pásek použít jako opasek a tím zamaskovat existenci tajné zprávy. Příjemce musel pásek navinout na hůl o stejném průměru.

Nechat kolovat pomůcku!!

Odvětví kryptologie

Už jsme se dozvěděli, že můžeme buď pozměnit obsah textu, nebo samotný text ukrýt. S tím souvisí jednotlivá odvětví kryptologie, a sice kryptografie, steganografie a kryptoanalýza.

Do kterého odvětví podle vás spadá utajování existence zprávy (např. oholení hlavy, ...)?

Steganografie

Název steganografie je odvozen od slov steganos (= skrytý, schovaný) a graphein (=psát).

O jakých steganografických metodách jsme se již bavili? (Histiaios, Skytala – použití jako opasku)

Znáte nějaké další metody ukrývání textu?

Například neviditelný inkoust (uv-fixy, mléko, citronová šťáva).

Ukrytí textu ve změti písmen či v jiném textu. Příklady v prezentaci: první příklad – změna velikosti písmen, druhý příklad – první písmeno v každém slově. Je mnoho dalších možností, např. čísla, propíchnutí špendlíkem, změna fontu, první písmena na začátku řádků a další.

Zmenšení textu do obrázku – vrátit se k předchozímu slidu.

Kryptografie

Souhrn metod, které umožňují utajit obsah zprávy tak, aby byla pro nepovolaného člověka nečitelná. K takovému utajování se používá šifrování, účastnící komunikace si domluví určitá pravidla, podle kterých změní podobu textu.

O jakém šifrovacím systému jsme se už zmínili? (Skytala – domluvené pravidlo: tyč stejného průměru)

Kryptografií a způsoby šifrování se budeme později zabývat více.

Kryptoanalýza

Je opakem kryptografie. Kryptoanalytici se snaží šifru rozluštit a přečíst si její pravý obsah i přesto, aniž by znali klíč, pomocí kterého byla zpráva zašifrována. Pro úspěšné luštění tajných zpráv je nutná dobrá znalost jazyka (například výskyt některých písmen v českém jazyce, apod.), trpělivost a také znalost světa kryptologie.

Luštění je poměrně náročné, a proto se jím dnes zabývat nebudeme.

Základní pojmy

K tomu, abychom mohli efektivně pracovat se šiframi, musíme se seznámit s některými základními pojmy.

- **Šifra** = nahrazování písmen zprávy jinými písmeny, číslici nebo znaky (př. v prezentaci)
- **Kód** = slovo, číslo nebo symbol, které nahrazuje jiné slovo nebo skupinu slov (př. heslo IRENA v Černém jestřábu)
- **Otevřený text** = srozumitelný text psaný v běžném jazyce, který chceme zašifrovat
- **Šifrový text** = text po zašifrování, jeví se jako náhodná kombinace znaků (vrátit se na předchozí slide a ukázat OT a ŠT)
- **Klíč** = souhrn pravidel, podle kterých probíhá šifrování (např. které znaky budeme používat při šifrování, jaký směr šifrování využijeme, atd.), je nutné, aby klíč znali oba účastníci komunikace a aby byl pečlivě utajen; klíč je velmi důležitý, protože kdybychom jen OT převedli například do Morseovy abecedy, mohl by si text přečíst každý, protože Morseova abeceda je veřejně známá, účastníci komunikace se však mohou domluvit, že obrátí tečky a čárky, což je vlastně šifrovací klíč (i když velmi slabý)

- **Šifrovací algoritmus** = postup vytváření šifrového textu
- **Zašifrovat** = převést OT na ŠT pomocí šifrovacího algoritmu a klíče
- **Dešifrovat** = převést ŠT na OT, příjemce má k dispozici stejný klíč a pravidla šifrování, ale musí použít opačný algoritmus, klíč musí být bezpečně střežen
- **Luštění** = převedení ŠT na OT bez znalosti klíče a pravidel šifrování
- **Kódování** = převod textu do podoby vhodné pro vysílání elektrických, zvukových či optických signálů (např.: Morseova abeceda, binární kód, ...)

Základy šifrování

Nyní už se dostaneme k jednotlivým typům šifer a zkusíme společně šifrovat i dešifrovat. My budeme dnes používat pouze jednoduché šifrové algoritmy na krátkých textech.

Znáte nějaký způsob šifrování (kromě steganografických metod)?

Podle způsobu, jakým šifrujeme, rozdělujeme šifry na dva základní typy – substituční a transpoziční.

Napadá někoho, co znamená substituční šifra a jaké metody u ní používáme?

Substituční šifry jsou nejznámější a nejpoužívanější. Jedná se o záměnu znaků otevřeného textu za znaky jiné šifrové abecedy, což může být například posunutá abeceda, nebo souhrn číslic nebo symbolů.

Napadá vás, jak je to s transpozičními šiframi?

U transpozičních šifer dochází ke změně pořadí znaků otevřeného textu podle určitého klíče a pravidel. Počet a tvar znaků OT je tedy stejný jako u ŠT.

Substituční šifry

Při šifrování můžeme použít různé způsoby, např. na celý text použijeme jedinou šifrovací abecedu nebo na každý znak OT použijeme jinou šifrovací abecedu, atd. My se budeme zabývat **jednoduchou záměnou**, kde se používá pouze jedna šifrovací abeceda.

Pro zjednodušení používáme převodovou tabulku. V prvním řádku jsou uvedeny znaky otevřeného textu a v druhém řádku znaky šifrové abecedy. Například tabulka šifry **atbaš**, která ukazuje, že první písmeno abecedy zaměníme za poslední atd.

Vysvětlit zkratky OT, ŠT, ŠA!!

Zdůraznit, že nepoužíváme háčky, čárky, písmeno CH a mezery!!

Pomocí této tabulky jsem zašifrovala své jméno. *Jaké písmenko zaměním za S?*

Př: Zašifrovat vlastní jméno na pracovním listě. SPOLEČNĚ

Na dalším slidu jsou další příklady převodových tabulek. První tabulka zobrazuje šifrovou abecedu, která je posunuta oproti obyčejné abecedě o 7 písmen doleva. Druhá šifrová abeceda má náhodně zvolené pořadí písmen. Třetí tabulka je šifrou **albam**, u které bychom mohli použít pouze poloviční tabulku. Poslední substituce zaměňuje písmena za symboly (písmo Wingdings 3).

Dešifrování probíhá obdobně. V tabulce hledáme tentokrát v dolním řádku a přiřazujeme písmena v prvním řádku.

Transpoziční šifry

Jak již bylo řečeno, jedná se o změnu pořadí znaků OT, to znamená, že ŠT má stejné znaky jako OT, ale jsou „přeházená" podle určitého pravidla.

Př.: v prezentaci moje příjmení pozpátku

Napadá někoho, podle kterého pravidla bylo slovo zašifrováno?

Další šifrovací systém zapisuje střídavě znaky OT na první a poslední pozice do předem připraveného řádku ŠT. Příklad v prezentaci.

Lze využít i systém, který na předem připravený řádek zapisuje znaky OT ob libovolný počet pozic. Příklad v prezentaci.

Oblíbený šifrovací systém se nazývá „podle plotu". Znaky OT se zapisují do dvou nebo více řádků podle plotu, ŠT se pak čte po řádcích. Příklad v prezentaci.

Mohou být ale využity i tabulky, do kterých se text zprávy zapisuje podle předem dohodnutého pravidla, např. do spirály, cik-cak, apod. Fantazii se meze nekladou. Šifrový text se čte po řádcích. Příklad tabulek a šifrování v prezentaci.

Jelikož příjemce ví, podle jakých pravidel byla zpráva zašifrována, je dešifrování snadné. U jednoduchých transpozic příjemce pouze čte zprávu pozpátku no podle jiného dohodnutého pravidla. U tabulek a systému podle plotu si musí připravit tabulku, do které po řádcích vepisuje ŠT. OT potom čte dohodnutým směrem, například po spirále.

Př.: Příklad dešifrování v prezentaci – společně na pracovním listě.

AKTIVITA

! Vytvořit dvojice! Dvojice si vymyslí jméno, to se zapíše do tabulky! Do dvojice rozdat pracovní listy a čisté papírky.

Každá dvojice může využít 4 nápovědy – důkladně rozmyslet! Pro získání nápovědy musí dvojice odevzdat papírek s číslem úlohy a jménem týmu, na kterou chtějí nápovědu.

!Nesmí se křičet, napovídat!

Po odevzdání papírku se zašifrovaným názvem bedny, dostanou skládanku a papírek na číselný kód.

Na konci čeká sladká odměna pro všechny (pro každého dva mlsky).

Každý po získání odměny obdrží ještě smajlíkový dotazník.

! VYBRAT PRACOVNÍ LISTY + NÁPOVĚDY + SKLÁDANKY!!! !

PŘÍLOHA 9 – Snímky prezentace použité ve výuce

ZÁKLADY KRYPTOLOGIE

KRYPTOLOGIE

= nauka o šifrování

Důvody šifrování

- zabezpečení dat a tajných informací (choulostivá data o osobách, vědecké objevy, hesla, ...)
- tajná korespondence (např. válečné depeše, milostná psaníčka, ...)

Pohled do historie

Skytala

Odvětví kryptologie

- Kryptografie
- Steganografie
- Kryptoanalýza

Steganografie

- *steganos* = schovaný, *graphein* = psát
- utajování existence tajných zpráv
- př.: Histiaios a oholená hlava; použití zprávy jako opasku, ...

Některé steganografické metody

Neviditelný inkoust

Některé steganografické metody

Ukrytí textu ve změti písmen:

- Skákal pes přes oves, přes zelenou louku, šel za ním myslivec, péro na klobouku.

(kapesník)

- Martin Olbracht ušel kus Ameriky.

(mouka)

Některé steganografické metody

Ukrytí textu do obrázku

Kryptografie

- *kryptos* = skrytý
- změna podoby textu
- domluvená pravidla šifrování účastníků komunikace

- př.: Skytala (tyče o stejném průměru)

Kryptoanalýza

- luštění tajných zpráv bez znalosti šifrovacího klíče
- nutná výborná znalost jazyka, poznatků z oblasti kryptologie, dostatek trpělivosti

Základní pojmy

- **šifra** = nahrazování písmen textu jinými písmeny, číslicemi nebo znaky
- např.: SOBOTA → 1814114190
- **kód** = slovo, číslo nebo symbol, které nahrazuje nějaké jiné slovo nebo skupinu slov
- **otevřený text** = srozumitelný text psaný v běžném jazyce, který chceme zašifrovat

Základní pojmy

- **šifrový text** = text po zašifrování, jeví se jako náhodná kombinace znaků
- **klíč** = souhrn pravidel, podle kterých probíhá šifrování; musí ho znát příjemce a odesílatel; před ostatními ale musí být bezpečně utajen
- např.: užití symbolů: ✔ 🚲⬜⛊🛍🛒⬛🚙ⓘ🛩
- **šifrovací algoritmus** = postup vytváření šifrového textu

Základní pojmy

- **šifrování** = převedení otevřeného textu pomocí klíče a šifrovacího algoritmu na šifrový text
- **dešifrování** = převedení ŠT na OT, příjemce zprávy musí znát klíč i algoritmus, který použil odesílatel
- **luštění** = převedení ŠT na OT bez znalosti klíče a pravidel
- **kódování** = převod textu do podoby vhodné pro vysílání elektrických, zvukových nebo optických signálů (Morseovka, binární kód)

Základy šifrování

SUBSTITUČNÍ ŠIFRY

- nejrozšířenější
- záměna znaků OT za znaky šifrové abecedy (písmena, čísla, symboly, ...)

TRANSPOZIČNÍ ŠIFRY

- změna pořadí znaků v OT podle určitých pravidel
- počet a tvar znaků OT je stejný jako u ŠT

Substituční šifry

- Jednoduchá záměna = jediná šifrovací abeceda
- Převodová tabulka:

OT:	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
ŠA:	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A

- př.: OT: Sabina
  ŠT: HZYRMZ

Substituční tabulky

OT:	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
ŠA:	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G

OT:	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
ŠA:	X	S	A	D	Z	R	F	P	J	W	C	Q	T	E	Y	M	B	K	H	N	O	U	G	L	V	I

OT:	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
ŠA:	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M

OT:	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
ŠA:	⇨	⇘	⇩	⇙	⇦	←	→	↑	↓	↖	↗	↙	↘	↔	↕	▲	▼	△	▽	◀	▶	◁	▷	◣	◢	◤

Dešifrování

- Stejný princip jako u šifrování, ale opačný postup hledání znaků

OT:	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
ŠA:	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G

- př.: ŠT: WVKWHYLGLT
  OT: PODPAREZEM → pod pařezem

Transpoziční šifry

- Text psaný pozpátku
- př.: OT: HAJKOVA
  ŠT: AVOKJAH
- Střídání první a poslední pozice
- př.: OT: heslo je klokan → 13 pozic
  ŠT: H S O E L K N A O K J L E

Transpoziční šifry

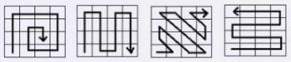
- Zápis „ob tři" pozice:
  OT: TRANSPOZICE → 11 pozic
  ŠT: T N O C R S Z E A P I
- Šifrovací systém podle plotu:
  OT: hledej kolem studny

H				E				L				T				Y
	L		D		J		O		E		S		U		N	
		E				K				M				D		

ŠT: HELTY LDJOE SUNEK MD

Další transpoziční tabulky

- Zápis znaků OT do tabulky po směru šipek → ŠT čteme po řádcích



- př.:

L	O	J	E
S	T	A	O
E	U	N	R
H	G	N	A

ŠT: LOJES TAOEU NRHGNA

Dešifrování

- u jednoduchých transpozic čteme text podle dohodnutého pravidla
- u tabulkových transpozic musíme nejprve připravit vhodnou tabulku, zapsat do ní ŠT po řádcích a OT přečíst podle předem dohodnutého pravidla

Dešifrování

- př.: ŠT: KHRNI SROOE EAYVZ STNSE NAAJJ

→ 25 znaků → tabulka 5x5

K	H	R	N	I
S	R	O	O	E
E	A	Y	V	Z
S	T	N	S	E
N	A	A	J	J

OT: naše tajná skrýš je v ohrožení

Zdroje

- PELÁNEK, Radek. *Hlavolamikon: [sbírka hlavolamů, hádanek, šifer a logických úloh]*. Brno: Computer Press, 2014. ISBN 978-80-251-4303-2.
- HÁJKOVÁ, S. *Luštění transpozičních šifer s podporou počítače*. Hradec Králové, 2014. Bakalářská práce na Přírodovědecké fakultě Univerzity Hradec Králové. Vedoucí bakalářské práce PhDr. Michal Musílek, Ph.D. 41 s.

PŘÍLOHA 10 – List pro hodnocení projektu

HODNOCENÍ PROJEKTU

Nejvíc mě bavilo: _____

_____

_____

Docela mě bavilo: _____

_____

_____

Nejvíc mě nebavilo: _____

_____

_____

Co mi projekt přinesl: _____

_____

_____

Co bych udělal/a jinak: _____

_____

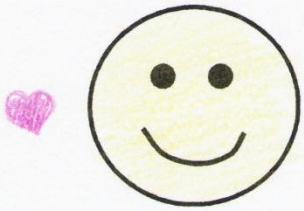
_____

Chtěl/a bych se o šifrování dozvědět víc: ano ne

Chtěl/a bych, aby se šifrování vyučovalo ve škole: ano ne

PŘÍLOHA 11 – Vyplněný list s hodnocením projektu I

HODNOCENÍ PROJEKTU



Nejvíc mě bavilo: Ta druhá část hodiny. Ten list byl opravdu zábavný. S kamarádkou nám to šlo.

Docela mě bavilo: První část hodiny. Konkrétně ty druhy jak se to může skrýt.

Nejvíc mě nebavilo: Vysvětlování co to znamená a tak podobně. Vím, že bych se bez toho možná neobešla, ale to nevadí.

Co mi projekt přinesl: Umím různě skrýt vzkazy, které nechci, aby si někdo přečetl. Snad je nezapomenu. Třeba bych to mohla naučit někoho jiného.

Co bych udělal/a jinak: Dala bych více sladkostí do krabičky ☺. Možná bych dala trochu více času na ten druhý pracovní list.

Chtěl/a bych se o šifrování dozvědět víc: (ano) ne

Chtěl/a bych, aby se šifrování vyučovalo ve škole: (ano) ne

PŘÍLOHA 12 – Vyplněný list s hodnocením projektu II

HODNOCENÍ PROJEKTU

Nejvíc mě bavilo: jíst ten poklad, který byl u "truhle s pokladem"

Docela mě bavilo: Řešení toho papíru šifer, který nás měl dovést k pokladu

Nejvíc mě nebavilo: Vyplňovat ten papír, podle textu, který byl na interaktivní tabuli

Co mi projekt přinesl: Nové poznatky o nauce kryptologie → různých šifer, hesel a hádanek

Co bych udělal/a jinak: Asi skoro nic, měla to připravené bezky, ale ty úlohy byly těžké

Chtěl/a bych se o šifrování dozvědět víc: (ano) ne

Chtěl/a bych, aby se šifrování vyučovalo ve škole: (ano) ne