

Oponentní posudek na diplomovou práci

Autor/ka DP: Hana Vacatová
Studijní program/obor: N1101 Matematika
Název práce: Sbírka úloh k šifrování
Oponentka práce: Ing. Jindra Drábková, Ph.D.

Hodnoticí kritéria	Splňuje bez výhrad	Splňuje s drobnými výhradami	Splňuje s výhradami	Nesplňuje
A. Obsahová				
V práci jsou vymezeny základní a dílčí cíle, které jsou v koncepci práce patřičně rozpracovány. Cíle jsou adekvátně naplňovány.	☐	☒	☐	☐
Práce splňuje cíle zadání.	☐	☐	☒	☐
Studující využívá a kriticky vybírá sekundární a/nebo primární literaturu.	☐	☐	☒	☐
Práce má vymezen předmět, je využito odpovídajících metodologických postupů.	☐	☒	☐	☐
Výstupy výzkumných částí jsou adekvátně syntetizovány a je o nich diskutováno.	☐	☒	☐	☐
V práci je využita odborná terminologie a jsou vysvětleny hlavní pojmy.	☐	☐	☒	☐
V práci jsou formulovány jasné závěry, které se vztahují ke koncepci práce a ke stanoveným cílům.	☐	☒	☐	☐
V průběhu zpracování tématu studující pracoval/a v součinnosti s vedoucím/vedoucí práce.	☐	☐	☐	☐
B. Formální				
Práce vykazuje standardní poznámkový aparát a jednotný způsob citací v rámci práce, je typograficky jednotná.	☐	☐	☒	☐
Studující dodržuje jazykovou normu, text je stylisticky jednotný.	☐	☒	☐	☐
Text je soudržný, srozumitelný a argumentačně podložený.	☐	☐	☒	☐
C. Přínos práce				
Tvůrčí přístup studujícího, kompilační hodnota, využití pro praxi.	☐	☒	☐	☐



Celkové hodnocení práce (max. 1700 znaků):

Cílem diplomové práce bylo vytvořit sbírku příkladů na téma šifrování pro žáky základních i středních škol. V teoretické části jsou popsány základy dělitelnosti a úvod do šifrování. Součástí popisu jednotlivých šifer jsou i řešené příklady. Součástí praktické části je sbírka úloh na téma šifrování včetně výsledků. Jednotlivé kapitoly práce jsou přehledně členěny, po formální stránce je práce na dobré úrovni, v práci se občas vyskytují překlepy, gramatické (Další typy Caesarovi šifry) a typografické chyby (záměna spojovníku za pomlčku, nesprávné používání tří teček, mezery před interpunkčními znaménky).

Celkově je diplomová práce na nízké úrovni. Některé pojmy nejsou dostatečně odborně vysvětleny. Vytvořená sbírka je podle mého názoru nepoužitelná, protože v ní nejsou řešené příklady ani žádný teoretický úvod. Použitá literatura s jedenácti položkami, z toho pěti z Technické univerzity v Liberci je pro diplomovou práci nedostatečná. Autorka v práci vůbec necituje, takže není zřejmé, co je převzaté a co je její dílo.

Některá řešení příkladů, která jsou v teoretické části, nejsou zřetelně vysvětlena a některá obsahují i chyby. Tabulka 3, kde je Vigenèrův čtverec, je rozdělena na dvě stránky, takže se velmi těžko příklad kontroluje (vhodnější by bylo opakovat na druhé stránce záhlaví nebo přeformulovat text tak, aby tabulka byla na jedné stránce). Ve sbírce v kapitole Permutační šifra není vhodné použít u většiny příkladů stejný počet písmen u slova, které se má zašifrovat, jako u transpozičního klíče

Přes uvedené připomínky práci doporučuji k obhajobě.

Práce splňuje požadavky na udělení akademického titulu magistr:	ANO
Práci doporučuji k obhajobě:	ANO
Návrh klasifikačního stupně:	dobře

Náměty pro obhajobu (max. 1500 znaků):

- 1) Vysvětlíte příklad na str. 18 dole, zašifrování na str. 32 a 43.
- 2) Proč někde písmeno ch považujete za dva znaky a někde za jeden?
- 3) Odkud jste čerpala informace pro tabulku 6 (Četnost znaků v českém jazyce)?
- 4) Vysvětlíte frekvenční analýzu četnosti znaků na str. 53.

Datum: 29. 1. 2015

Podpis:

