Posudek diplomové práce

předložené na katedře matematiky
Pedagogické fakulty Jihočeské univerzity v Českých Budějovicích

posudek **oponentky diplomové** práce

Autor: **Alena Košáková**

Název práce: **Matematika v moderních šifrovacích metodách**
Posudek vyhotovil(a): **doc. RNDr. Helena Koldová, Ph.D.**

Odborná úroveň práce: **velmi dobrá**

Popsání cílů a metod: **autorka cíle práce nedefinuje, jen je zmiňuje v kapitole Závěr. Cílem DP bylo seznámit zájemce i širokou veřejnost s problematikou šifrování a využití matematiky v této oblasti, jak uvádí autorka. V první části práce zavádí základní teoretická východiska související s šifrováním, uvádí některé typy kryptosystémů a to jednak z pohledu matematiky a také z pohledu nejnovějších poznatků.**

Kvalita teoretické části práce: **velmi dobrá; autorka v teoretické části práce (kapitoly 1-6) vymezuje základní pojmy, související se zpracováním diplomové práce a s naplněním jejích cílů. Vymezuje pojem šifrování z pohledu matematiky, zavádí pojem symetrické šifrování, asymetrické šifrování, RSA, šifrování hybridní a uvádí jejich způsoby využití. Tato část je velmi podrobná a přináší výbornou inspiraci pro učitele matematiky, kteří budou téma šifrování zařazovat do své výuky matematiky jak na základní, tak na střední škole. Velmi oceňuji doplňující vizualizace, které vytvořila autorka (např. obr. 1-10, tabulka 4, 5, 8 aj.) a které usnadňují čtení, porozumění textu. Celkově má práce velmi pěknou grafickou úpravu, text je pěkně členěn a význam sdělení je oddělován. Nerozumím na str. 12 velikosti písma odkazu**

příjemce se nejprve domluví na klíči (tedy na sekvenci znaků), odesílatel zprávu ašifruje, zašle ji příjemci a ten ji přijme a rozšifruje. (https://www.napocitaci.cz/33/symetricke-a-asymetricke-sifrovani-iqueidgOkE4NvrWuNY54vrLeM677jX7sp3Lu-ZpLpGVMy1prA/, 7. 7. 2020) *Symetrická šifra je taková šifra, kde pro*

Není čitelný (stejně např. na str. 60).
Je zřejmé, že diplomantka prostudovala velké množství související literatury, její sdělení jsou podložená a práce je tak velmi cenným materiálem.
Na str. 17 však například postrádám zdroj pro tak odborné tvrzení: *Spory o jeho odolnosti se vedou již od let, kdy byl tento algoritmus přijat ve standardu. Podrobné popsání těchto diskusí je možné si přečíst v mnoha pracích, které se týkají kryptografie. Později bylo jasné, že všechny tyto zápory vedou k jedné jediné věci, a to k velikosti klíče. Toto se jevilo jako největší slabina algoritmu DES, a proto na něj byly uskutečněny útoky. Slabina byla zřejmá až v devadesátých letech minulého století.*
Kapitola 3.4-3.7 není ozdrojována vůbec. Stejně tak úvod kapitoly 4, apod.

Rozsah praktické složky práce: **v DP není praktická část. Za sebe bych jako praktickou část označila např. kapitolu 4.4.1. Geometrická interpretace eliptických křivek nad polem T, která obsahuje podrobné vysvětlení a rozpracování tématu s vizualizacemi, nebo také kap. 4.4.2.2. Operace sčítání na eliptické křivce. Praktickou částí, kapitolou s praktickým významem, by mohla být i kapitola 6. Pojednává o využití šifrování. Hledala jsem zde zmínku o kryptoměnách, bohužel, ačkoli je v seznamu literatury uvedena publikace Stroukal, D. a Skalický, J. (2018): Bitcoin a jiné kryptopeníze budoucnosti: historie, ekonomie a technologie kryptoměn, stručná příručka pro úplné začátečníky. Praha: Grada Publishing a. s, je na ní odkazováno jen v úvodu DP a problematiku kryptoměn v práci nenajdeme. To však nemá vliv na rozsah a obsah zpracování DP, práce je velmi obsáhlá a má výbornou vypovídající hodnotu.**

Grafická, jazyková a formální úroveň: **dobrá. Citace odpovídají zvolené normě. Velké množství citovaných publikací v textu svědčí o tom, že autorka prostudovala dostatečné množství odborné literatury.**

Věcné chyby, chyby psaní a překlepy:
nejsou

Přínos práce:
Diplomová práce představuje text, který by mohl sloužit učitelům matematiky na střední nebo na základní škole jako podpůrný či motivační materiál pro výuku nestandardních aplikačních problémů.

Otázky pro obhajobu a náměty do diskuze:
Jak byste vyučovala popisovanou problematiku ve škole? Myslíte si, že jsou učebnice matematiky v ČR pro výuku tématu šifrování připravené? A je to téma okrajové?

Práci **doporučuji** k obhajobě.

Navrhuji hodnocení stupněm: velmi dobře

Místo, datum a podpis: České Budějovice, 17. 5. 2021