Posudek diplomové práce

předložené na katedře matematiky
Pedagogické fakulty Jihočeské univerzity v Českých Budějovicích

posudek **oponenta diplomové** práce

Autorka: Kateřina Boučková

Název práce: *Šifry ve výuce matematiky na 1. stupni základní školy*

Posudek vyhotovil: **prof. RNDr. Pavel Tlustý, CSc.**

Po tisíce let spoléhali lidé na komunikační systémy, které jim umožňovaly předávání tajných informací. Problémem takové komunikace vždy bylo riziko vyzrazení, které mohlo mít až tragické následky. Předložená diplomová práce se zbývá vybranými matematickými metodami ochrany dat od jejich počátků ve starověku až do současnosti.

Práce sledovala dva hlavní cíle. Jednak seznámit širší okruh zájemců, zejména pedagogů na 1. stupni základní školy, s tímto zajímavým tématem a jeho možným využitím, jak v hodinách matematiky samotných, tak i jako motivačního a aktivizačního prostředku pro zvýšení zájmu o matematiku. Autorka kladla důraz zejména na šifrovací techniky a postupy využívajících takových matematických postupů, které jsou zvládnutelné žáky základní školy a nevyžadující použití složitého softwaru a výpočetní techniky. Dalším cílem bylo vytvoření sady pracovních listů, pomocí kterých se děti seznámí zábavnou formou s různými druhy šifer z minulosti, ale i současnosti a naučí se, jak daný text správně zašifrovat a dešifrovat. Sadu pracovních listů autorka následně ověřovala na vybrané základní škole. Domnívám se, že se podařilo oba cíle beze zbytku splnit.

Tematicky je práce rozdělena do několika hlavních kapitol, z nichž některé se dále člení na řadu podkapitol. Po nezbytném úvodu je podán stručný, avšak pro další pochopení použitých metod dostatečný přehled základních pojmů a principů šifrování. Autorka řeší především otázky, které vznikají při zašifrování a dešifrování textu. Problematika prolomení dané šifry, bezpečnosti jednotlivých šifer, atd. je i s ohledem na předpokládanou skupinu čtenářů zmíněna jen okrajově. Podrobněji jsou zmíněny některé konkrétní šifrovací techniky (Cardanova mřížka, mono-alfabetická šifra, afinní šifra, šifra Playfair, atd.) Poslední kapitola je věnována pracovním listům, popisu řešení a vyhodnocení. K vlastnímu ověření pracovních listů došlo na Základní a mateřské škole v Chlumu. V řadě pracovních listů se vyskytují i další zajímavé informace z historie, jazykovědy, Braillovo písmo, atd., což je názornou demonstrací mezipředmětových vztahů.

Celkově lze konstatovat, že předložená diplomová práce je psána srozumitelně a má odpovídající grafickou úroveň. Domnívám se tedy, že splňuje všechny požadavky, které jsou na ni kladené. DOPORUČUJI proto, přijmout práci k obhajobě a navrhuji známku VÝBORNĚ.

V Českých Budějovicích, 5. května 2021

prof. RNDr. Pavel Tlustý, CSc.