

Příloha k protokolu o SZZ č.

Vysoká škola: JU Pedagogická fakulta

Katedra: matematiky

Datum odevzdání posudku: 26. 4 .2018

Diplomant: Eva Milichovská

Aprobace: Mn-Dn-SZn

Vedoucí diplomové práce:
prof. RNDr. Pavel Tlustý, CSc.

POSUDEK DIPLOMOVÉ PRÁCE

Historie šifrovacích metod a jejich aplikace

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 poloviny 20. století.

Práce sledovala dva hlavní cíle. Navázat a podstatným způsobem rozšířit bakalářskou práci autorky o další možné postupy šifrování zpráv bez použití výpočetní techniky. V tomto případě byl důraz kladen na šifrovací techniky využívajících takových matematických postupů, které jsou zvládnutelné žáky základní školy. Druhým cílem práce bylo vytvoření pracovních listů do zájmových kroužků matematiky a pro šikovné žáky posledních ročníků základní školy a jejich následné ověření na vybrané základní škole. Domnívám se, že se autorce podařilo oba cíle beze zbytku splnit.

Tematicky je práce rozdělena do sedmi hlavních kapitol, z nichž některé se dále člení na řadu podkapitol. Po nezbytném úvodu je ve druhé kapitole podán stručný, avšak pro další pochopení použitých metod dostatečný přehled základních pojmů a principů šifrování. Autorka řeší současně všechny tři základní otázky, které vznikají při šifrování – šifrování textu, dešifrování textu a metody prolomení dané šifry, tedy zabývá se i problematikou bezpečnosti jednotlivých šifer. Ve třetí kapitole je podán soupis matematických definic a vět, které jsou nezbytné pro další pochopení uvedených šifrovacích postupů. Ve čtvrté kapitole nás autorka postupně seznamuje s několika konkrétními šifrovacími technikami (Fleissnerova mřížka, monoalfabetická šifra, afinní šifra, šifra Playfair, atd. Poslední tři kapitoly jsou věnovány pracovním listům, popisu řešení a vyhodnocení. K vlastnímu ověření pracovních listů došlo na základní škole Evžena Rošického v Jihlavě v rámci Matematického kroužku. Veškeré šifrované texty v pracovních listech představují ukázky ze známých literárních děl, což je názornou demonstrací mezipředmětových vztahů.

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

prof. RNDr. Pavel Tlustý, CSc.

Návrh na klasifikaci diplomové práce: Výborně



Podpis vedoucího diplomové práce

V Č. Budějovicích dne 26. 4. 2018

Stupeň	výborně	velmi dobře	dobře	nevyhověl
--------	---------	-------------	-------	-----------