

Příloha k protokolu o SZZ č.

Vysoká škola: JU Pedagogická fakulta

Katedra: matematiky

Datum odevzdání posudku: 12. 5 .2016

Diplomant: Eva Milichovská

Aprobace: Mu-Hu-SZU

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

POSUDEK BAKALÁŘSKÉ PRÁCE

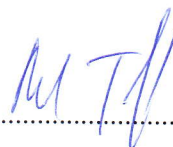
Vybrané šifrovací metody

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. Bakalářská práce se zabývá vybranými matematickými metodami ochrany dat od jejich počátků ve starověku až do poloviny 20. století.

Tematicky je práce rozdělena do pěti 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 metodami luštění šifer, tedy zmiňuje i problematiku 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 autorka provádí chronologický přehled šifrovacích metod od Skytale (užívané ve Spartě v 7. století př. n. l) až po Hillovu šifru, kterou užívalo námořnictvo Spojených států během 2. světové války. Pátá kapitola je věnována základním metodám kryptoanalýzy, tedy vědy, která se zabývá luštěním šifer.

Celkově lze konstatovat, že předložená bakalářská 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.

Návrh na klasifikaci bakalářské práce: Výborně



Podpis vedoucí bakalářské práce

V Č. Budějovicích dne 12. 5. 2016

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