Posudek diplomové práce

předložené na katedře matematiky
Pedagogické fakulty Jihočeské univerzity v Českých Budějovicích

posudek **vedoucího diplomové** práce

Autorka: Bc. Alena Košáková

Název práce: *Matematika v moderních šifrovacích metodách*

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 moderními matematickými používanými od druhé poloviny 20. století do současnosti.

Cílem diplomové práce bylo připravit souhrnný materiál, ve které nalezne případný zájemce základní orientaci v problematice moderního šifrování. Vzhledem k tomu, že autorka klade důraz na využití pokročilejších matematických metod, tak jen některé z uvedených postupů jsou zvládnutelné žáky základní školy. Všechny pasáže textu budou plně srozumitelné čtenářům s dobrou matematickou průpravou zejména v oblasti teorie čísel. Na druhou stranu tento přístup umožňuje ukázat konkrétní praktické realizace kryptografických postupů v každodenním reálném životě. Domnívám se, že se autorce podařilo stanovený cíl v zásadě splnit.

Tematicky je práce rozdělena do šesti 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 matematických pojmů a vztahů, jejichž znalost je nezbytná pro použité šifrovací metody. Autorka řeší současně všechny tři základní otázky, které vznikají při šifrování – šifrování textu, rozšifrování textu i prolomení dané šifry, tedy zabývá se i problematikou bezpečnosti jednotlivých šifer. Třetí kapitola je věnována symetrickým kryptosystémům – AES, R, DES, Akelarre, Anubis, Blowfish, atd. Ve čtvrté kapitole se čtenář dozvídá o tzv. šifrách s veřejným (RSA, El-Gamal, kryptografie na bázi eliptických křivek). U každé z šifer je uvedena stručná historie, jak se tvoří a jaká je její bezpečnostní úroveň. Vše je doplněno o názorné příklady s konkrétními čísly, která čtenářům pomohou problematiku šifrování ještě hlouběji pochopit. Krátce je zmíněna i technika hybridního šifrování (viz kapitola 5.). V poslední kapitole jsou příklady konkrétních realizací šifrovacích metod z reálného života – digitální podpis, systém AACS sloužící k ochraně optických disků, standard SSL definující bezpečnost elektronické komunikace, autentizační protokol Kerberos, platební protokol 3D Secure pro internetové platby kartou, atd.

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

V Českých Budějovicích, 3. 5. 2021

prof. RNDr. Pavel Tlustý, CSc.