Příloha k protokolu o SZZ č.

Vysoká škola: Pedagogická fakulta JU v Č. Budějovicích

Katedra: matematiky

Datum odevzdání posudku: 17.5.2007

Diplomantka: Pavla Sirotková
Aprobace: M-F/SŠ

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

Posudek diplomové práce

„Matematika a širfování“

Po tisíce let spoléhali lidé komunikacní systémy, které jim umoňovaly předávání tajných informací. Problémem takové komunikace bylo riziko vyzrazení, které mohlo mít až tragické následky. Diplomová práce se zbývá matematickými metodami ochrany dat.

Tématicky je práce rozdělena do sedmi kapitol, z nichž některé se dále člení na řadu podkapitol. V první části je uveden prehled šifrovacích metod od staroveku po soucasnost. Dále jsou shrnuty matematické poznatky, které v dalších kapitolách slouží jednak k šifrování pomocí algoritmu RSA, ale také k ruzným druhum dešifrování. Z moderních šifrovacích metod se autorka věnovala podrobně algoritmu označovaném jako RSA. Tento algoritmus byl představuje základ dnešní kryptologie a byl první, který používal k zašifrování zprávy jiný klíc než k jejímu dešifrování. Dnes je jedním z prvku zabezpecení našich e-mailu, platebních karet, elektronických podpisu ci ruzných prístupových hesel. Práce obsahuje několik nepřesností či chyb, z nichž jen některé uvádím:

1. ve větě 3.10 jsou špatně indexy
2. věta 3.11 je nepřesně
3. str. 29 - postrádám zdůvodnění, proč nemůže existovat taková „polynomická formule“
4. věta 3.15 není větou ve smyslu matematiky
5. V definici 3.16 jsou zaměněny pojmy definice - věta
6. věta 3.16 je zcela špatně, zejména výraz (3.3)
7. v posledním odstavci na str. 53 jsou gramatické chyby

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

Návrh na klasifikaci diplomové práce: dobře

.....
Podpis vedoucího diplomové práce

V Č. Budějovicích dne : 17.5.2007

Stupeň klasifikace	výborně	velmi dobře	dobře	nevyhověl