Posudek oponenta

bakalářské práce Jindřicha Kinského

„Kódování jako ochrana přenášených informací“

Předložená bakalářská práce je napsána na téma, jehož význam a aktuálnost autor přibližuje v předmluvě a první kapitole své práce. Cílem bylo „uvedení do základní problematiky kódování jako procesu, při němž konkrétní kryptografická metoda převádí originální (otevřený) text na text šifrovaný“. S potěšením konstatuji, že tento cíl se podařilo v práci na vynikající úrovni naplnit.

Práce odpovídá svým obsahem a rozsahem zadání. Text je adekvátně strukturován do kapitol, subkapitol a odstavců. Za výbornou je možno označit celkovou grafickou a jazykovou úroveň předložené práce (nalezl jsem pouze několik drobných chyb; zmínil bych snad jen nejednotnost u českého vyjádření pojmu: „autentifikace“ – na str.4, „autentizace“ – na str.29 a jinde; dále se přiznám, že rozpaky u mě vzbuzuje zavádění slova „enkrypce“ – str.30).

Co se týče použité literatury, je třeba ocenit její mimořádný rozsah (pět desítek položek) a vyváženost – autor pracoval jak s významnými monografiemi, tak s aktuálními články domácí a zahraniční provenience. Nechybí adekvátní citace v textu a bibliografické záznamy použitých elektronických pramenů.

Z obsahového hlediska nemám k práci zásadních výhrad. Autorovi se podařilo zpracovat velmi pěkný a hlavně fundovaný přehled kryptografických metod, zejména novějších, v současnosti při ochraně informací běžně používaných. Autor nevynechal ani velmi obtížná témata jako např. kvantovou kryptografii.

Z popisu jednotlivých algoritmů je patrné, že se s nimi autor důkladně seznámil. Přesto mu do textu vniklo pár nepřesností, speciálně v některých matematických formulacích, např. ve třetím řádku na str.14 by mělo být „původní nezměněné uspořádání prvků množiny“, na str. 22 a dalších by bylo vhodné využít termín „nesoudělná čísla“, na str. 23-4 má zřejmě namísto slova „skupina“ být termín „grupa“, na str. 24 je pro prvočísla chybně uvedeno, že „p“ je násobkem „q“.

Předložená bakalářská práce prokazuje schopnost zpracovat velmi obtížné téma a podat čtivý ucelený výklad. Zmíněné nedostatky nepovažuji za závažné. Při obhajobě bych autora poprosil o podrobnější popis algoritmu Triple DES, jeho vlastností a možností jeho použití.

Bakalářskou práci s radostí doporučuji k obhajobě a hodnotím ji známkou výborně.

V Praze dne 11.6.2010

Doc. RNDr. Jiří Ivánek, CSc.