OPONENTSKÝ POSUDEK BAKALÁŘSKÉ PRÁCE

Autor práce: Jiří Mareš
Název: Srovnání algoritmů pro kryptografii s veřejným klíčem
Vedoucí: David Stanovský

Předložená práce srovnává tři běžně používané algoritmy pro šifrování pomocí veřejného klíče, konkrétně jde o RSA, Rabinův a ElGamalův algoritmus. Vedle popisu a stručného teoretického zdůvodnění obsahuje text teoretický odhad časové složitosti jak šifrovacích tak dešifrovacích částí algoritmů. Těžiště práce tvoří výsledky měření autorových implementací všech tří algoritmů.

Text je napsán přístupnou formou a velmi dobře se čte. Ačkoli téma nekladlo vysoké nároky na teoretické znalosti, vyžadovalo od studenta funkční implementace a následně měření na rozsáhlejším souboru vstupů. Prezentace i objasnění výsledků měření jsou v textu zpracovány velmi pečlivě. Žádné významnější věcné ani jazykové nedostatky oponent v práci nenalezl. Nepříliš funkčním se u podobného textu zdá být autorem použitý systém poznámek pod čarou, většina poznámek by mohla být bez jakýchkoli dalších úprav zařazena do hlavního textu. Kromě toho by odůvodnění, proč dešifrovací část RSA a ElGamalova algoritmu funguje, jehož vynechání je komentováno v poznámkách 2 a 7, práci nijak významně neprodloužilo.

Předložená práce Jiřího Mareše *Srovnání algoritmů pro kryptografii s veřejným klíčem* splnila zadání, doporučuji ji proto uznat jako bakalářskou a po jistém rozvažování, způsobeném především nižší obtížností zvoleného tématu, ji navrhuji ohodnotit známkou **výborně**.

v Praze 18.1.2011 Jan Žemlička