Jiří Mareš: Srovnání algoritmů pro kryptografii s veřejným klíčem

posudek vedoucího práce

Jde o prakticky zaměřenou práci, v jejímž rámci byly implementovány tři z nejpoužívanějších číselněteoretických kryptosystémů s veřejným klíčem (RSA, Rabin, ElGamal, v několika variantách) a tyto algoritmy byly srovnány z hlediska efektivity. Práce obsahuje popis každého algoritmu, poznámky o jeho implementaci, teoretický odhad složitosti v závislosti na délce a měření rychlosti šifrování a dešifrování na náhodných datech pro různé délky klíčů. Výsledky měření jsou pečlivě diskutovány, srovnány jsou jak varianty jednotlivých algoritmů, tak algoritmy mezi sebou navzájem.

Práce byla zpracována zcela samostatně a poměrně pečlivě. Prokazuje studentovu orientaci v tématu, schopnost efektivně programovat matematické algoritmy a provádět věrohodnou analýzu jejich běhu.

Předloženou práci doporučuji uznat jako bakalářskou a ohodnotit stupněm **výborně.**

V Praze 14.1.2011
David Stanovský