Posudek vedoucího na bakalářskou práci

Veronika Heglasová: Kryptografie založená na eliptických křivkách

Předložená práce se věnuje kryptografickým systémům, které jsou založené na eliptických křivkách. Po stručném představení teoretických základů jsou popsány úpravy známých kryptosystémů pro eliptické křivky: eliptická varianta Diffie-Helmanova schématu na výměnu klíče, Massey-Omurův kryptosystém a kryptosystém ElGamal. Posledně jmenovanému se autorka věnuje podrobněji a šifrování a dešifrování je implementováno v programu Mathematika.

Práce je napsaná srozumitelně a čtivě. K hodnocení výborně chybí zpracování nějakého obtížnějšího teoretického tématu, případně praktické testování a srovnání různých přístupů, apod. Práci proto **doporučuji k obhajobě** a navrhuji hodnocení **velmi dobře**.

V Praze dne 17.6.2010

Mgr. Libor Barto, Ph.D.