Posudek vedoucího diplomové práce

Bc. Pavla Miky

„Aplikace kryptografie v informačních systémech“

Cílem diplomové práce bylo popsat a porovnat nejrozšířenější šifrovací algoritmy využívané v informačních systémech. Tento cíl se podařilo autorovi na velmi dobré úrovni naplnit. Vycházel přitom z adekvátně vybrané literatury, která je řádně citována v textu.

Z obsahového hlediska se autorovi podařilo zpracovat velmi pěkný přehled problematiky, včetně podrobného popisu hlavních kryptografických algoritmů, které jsou v informačních systémech aktuálně používány. Text je přehledně strukturován do šesti kapitol, v nichž jsou zachycena všechna témata informační bezpečnosti avizovaná v zadání diplomové práce.

Přínosná je zejména část věnovaná hodnocení algoritmů z různých hledisek a porovnání bezpečné délky klíčů. Diplomant zde shromáždil výsledky různých analýz, které jsou tak na jednom místě přístupným způsobem prezentovány.

Předložená diplomová práce prokazuje široký přehled autora v tématu a dostatečnou erudovanost v jeho zpracování. Diplomant pracoval velmi samostatně, prostudoval potřebné prameny a adekvátně zachytil současný stav aplikace kryptografie v informačních systémech.

Diplomovou práci P. Miky doporučuji k obhajobě a navrhuji známku velmi dobře.

V Praze dne 5. 9. 2013

Prof. RNDr. Jiří Ivánek, CSc.