

## Posudek

vedoucího

diplomové

Autorka: Marcel Šebek

Název práce: Deniable encryption

Jméno vedoucího: Jiří Tůma

Matematická úroveň:

vynikající

Grafická, jazyková a formální úroveň:

velmi dobrá

Výsledky:

originální

Použité metody:

standardní

Aplikovatelnost:

přínos pro praxi i teorii

Věcné chyby:

téměř žádné

Tiskové chyby:

vzhledem k rozsahu a pojednávanému tématu přiměřený počet

Celková úroveň práce:

vynikající

Práci

doporučuji

uznat jako diplomovou. Návrh klasifikace přikládám na zvláštním papíru.

Připomínky a vyjádření vedoucího: Jde o vynikající diplomovou práci, které lze málo vytknout. Je psána se znalostí věci, autora téma zjevně velmi zajímá. I když se některé pasáže nepodařilo probrat dostatečně podrobně (kapitola 4), celkový záběr práce je široký a obsah dobře promyšlený.

Ocenit je třeba také naprostou samostatnost, se kterou autor téma zpracoval, zvládnutí velkého množství literatury až po nejnovější články k tématu. Také podrobné prověřování publikovaných důkazů a odhalení chyb v navržených schématech popíratelného šifrování resp. v důkazech, že skutečně zajišťují ty kryptografické služby, které zajistit mají.

Práce zcela naplňuje požadavky kladené na diplomovou práci.

Místo, datum, podpis vedoucího:

