

POSUDEK OPONENTA DIPLOMOVÉ PRÁCE

Student: Bc. Tomáš Novosád

Oponent: Ing. Jiří Hološka, Ph.D.

Studijní program: **Inženýrská informatika**

Studijní obor: **Informační technologie**

Akademický rok: **2013/2014**

Téma diplomové práce: **Aplikace symetrické kryptografie**

Hodnocení práce:

V teoretické části, autor popisuje jednotlivá šifrovací témata formou, která je dobře čitelná i pro čtenáře s minimální znalostí v oboru kryptografie. Formální stránka práce je v pořádku, práce je psána srozumitelně a bez výrazných pravopisných či faktických chyb.

Praktická část je zpracována v jazyce C#, pro výukové potřeby by bylo vhodnější použít syntakticky přívětivější jazyk například Python.

Práce s literaturou je adekvátní povaze diplomové práce, kladně hodnotím zejména zdroje z Národního institutu pro standardy a technologie (NIST) a články Bruce Schneiera.

K práci nemám žádné zásadní připomínky, práce je zpracována pečlivě, prokazuje že autor je schopen samostatně řešit problematiku, která má komplexní charakter. Zvolené téma hodnotím jako těžké a plně vyhovující požadavkům na diplomovou práci. Práci doporučuji k obhajobě.

Otázka k obhajobě:

V praktické části jste použil kódování Windows-1250, nebylo by vhodnější použít Unicode ?

Celkové hodnocení práce:

Známku uvede oponent dle svého uvážení dle klasifikační stupnice ECTS:

A – výborně, B – velmi dobře, C – dobře, D – uspokojivě, E – dostatečně, F – nedostatečně.

Stupeň F znamená též „nedoporučuji práci k obhajobě“.

Předloženou diplomovou práci doporučuji k obhajobě a navrhuji hodnocení

A - výborně.

V případě hodnocení stupněm „F – nedostatečně“ uveďte do připomínek a slovního vyjádření hlavní nedostatky práce a důvody tohoto hodnocení.

Datum 27.5.2014

Podpis oponenta diplomové práce