

POSUDEK OPONENTA DIPLOMOVÉ PRÁCE

Student: BC. ADAM VOLF

Oponent: Ing. Jaromír Švejda, Ph.D.

Studijní program: **Inženýrská informatika**

Studijní obor: **Učitelství informatiky pro SŠ**

Akademický rok: **2017/2018**

Téma diplomové práce: **Testy odolnosti kryptografických metod**

Hodnocení práce:

Diplomová práce je velmi dobře technicky zpracovaná. Text je napsán přehledně a srozumitelně.

Jazyková úroveň práce je však trochu slabší, kvůli občasnému výskytu gramatických chyb (zejména čárky ve větách). Kapitola 2 obsahuje nevhodnou strukturovanost dokumentu, neboť v jejím obsahu se nevyskytují podkapitoly 2. úrovně – všechny podkapitoly jsou sníženy na úroveň 3. Totéž se týká kapitol 3, 5 a 6.

Technicky je však práce, až na výše zmíněné nedostatky, na velmi dobré úrovni. Diplomant splnil většinu bodů zadání. Jediným otazníkem v této oblasti je 4. bod zadání, ke kterému se vztahuje jeden z dotazů k obhajobě.

Otázky k obhajobě:

1. V závěru uvádíte, že Microsoft Bitlocker je dle testů software s nejsilnější kombinací kryptografických metod ve Vámi testované skupině, je však určen pouze pro OS Windows. Kdyby bylo nutné vybrat vhodný šifrovací SW pro jiné OS (Mac OS, Linux), který z Vámi testovaných SW byste místo Microsoft Bilockeru vybral?
2. Na kterých vzorcích databáze (viz zadání bod 4) jste otestoval vybrané metody kryptografie?

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

B - velmi dobře.

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

Datum 1. 6. 2018

Podpis oponenta diplomové práce