

## Hodnocení vedoucího bakalářské práce

**Student:** Jakubík Samuel

**Téma:** Útok na šifrování dokumentů OpenDocument s využitím GPU (id 19884)

**Vedoucí:** Hranický Radek, Ing., UIFS FIT VUT

### 1. Informace k zadání

Práce souvisí s projektem MVČR TARZAN. Cílem bylo rozšířit systém Fitcrack o podporu šifrovaných souborů formátu Open Document Format (ODF). Ačkoli standard specifikuje více použitelných způsobů kryptografického zabezpečení, dostupné nástroje pro práci s dokumenty ODF podporují pouze šifrování algoritmy Blowfish a AES. Pro obě varianty student implementoval rozšiřující modul pro výpočet jak na CPU, tak na GPU. Použitelnost výsledného řešení pan Jakubík experimentálně ověřil a porovnal s existujícími nástroji.

### 2. Práce s literaturou

Student využil jak doporučené literatury, tak dalších relevantních materiálů, které si sám dohledal.

### 3. Aktivita během řešení, konzultace, komunikace

Student byl při řešení aktivní a na domluvené konzultace docházel připraven.

### 4. Aktivita při dokončování

Při dokončování došlo k mírné prodlevě při ladění kódu pro GPU. To se však nakonec zdárně podařilo a student hotovou práci ke kontrole předložil v řádu několika dní před odevzdáním. Mé připomínky student následně zapracoval.

### 5. Publikační činnost, ocenění

není

### 6. Souhrnné hodnocení

**dobře (C)**

Veškeré obtíže, na které pan Jakubík při řešení narazil, se podařilo úspěšně vyřešit. Zadání považuji ve všech bodech za splněné. Oceňuji především podrobné a přehledné experimentální vyhodnocení výsledného řešení. Z pohledu vedoucího práci hodnotím jako "lepší C".

Prohlášení: Uděluji VUT v Brně souhlas ke zveřejnění tohoto hodnocení v listinné i elektronické formě.

V Brně dne: 22. května 2017

.....  
podpis