Univerzita
Pardubice
Fakulta elektrotechniky
a informatiky

Posudek vedoucího diplomové práce

Autor diplomové práce: **Josef ŠENFELD, Bc.**

Název diplomové práce: **Rainbow tables a jejich využití k prolomení hašovací funkce**

1. **Zadání odborného problému a použití metod řešení v rámci diplomové práce**

   Cílem práce bylo podrobně popsat hašovací funkce, sestavení a využití raindow table k jejich prolomení a vytvoření grafické simulace fungování rainbow table předem omezené velikosti.

2. **Konkrétní výsledky diplomové práce**

   Předložená práce má dva konkrétní výstupy. Tím prvním je precizně zpracovaná problematika hašovacích funkcí a raindow tables. Druhým konkrétním výstupem je plně funkční simulace fungování rainbow tables, jež je využitelná nejen v rámci vzdělávání, ale i pro simulaci náročnosti vytvořeného heše v závislosti na délce hesla a jeho dekódování s využitím rainbow tables.

3. **Prokázání správnosti navrženého řešení problému**

   Autor práce podrobně představil využití hašovací funkce, ukládání uživatelských hesel a autentizace. Na základě těchto informací pak přesně a jednoznačně představil principy rainbow tables, kde využil teoretických principů představených v předchozích kapitolách. Tyto principy jsou názorně ukázány v grafické simulaci využití rainbow tables a to včetně testování.

4. **Splnění cílů diplomové práce**

   Student splnil všechny vytyčené cíle.

5. **Kvalita textu diplomové práce**

   Text je zpracován na úrovni odpovídající diplomové práci, bez závažných chyb a nedostatků.

6. **Připomínky a dotazy k diplomové práci**

   Vedoucí práce nemá připomínky k předložené práci.

Doporučení práce k obhajobě: **ano**

Navržený klasifikační stupeň: **výborně**

Posudek vypracoval:

Jméno, tituly: Josef Horálek, Mgr., Ph.D.
Zaměstnavatel: Univerzita Pardubice, FEI

V Pardubicích dne: 27. 5. 2015 Podpis: