Univerzita
Pardubice
Fakulta elektrotechniky
a informatiky

Posudek oponenta 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**

   Zadaný odborný problém spočívá v realizaci návrhu, implementaci a ověření softwarového nástroje pro simulaci metody prolamování hesel omezené velikosti pomocí Rainbow tables.

2. **Konkrétní výsledky diplomové práce**

   Diplomant popsal ve své teoretické části práce mechanismus Rainbow tables a vytvořil grafickou aplikaci demonstrující názorně tuto činnost. Zároveň byla navržena vhodná redukční funkce omezující kolize.

3. **Prokázání správnosti navrženého řešení problému**

   Správnost řešení byla ověřena výše zmíněnou grafickou aplikací. Práci doplňuje vzájemné porovnání vhodnosti použití metody Rainbow tables a Brute force.

4. **Splnění cílů diplomové práce**

   Cíle diplomové práce byly splněny v plném rozsahu.

5. **Kvalita textu diplomové práce**

   V práci jsou dodrženy zásady DTP. Práce je zpracována přehledně, obsahuje všechny potřebné náležitosti a je v požadovaném rozsahu.

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

   U obhajoby diplomové práce doporučuji popsat, proč jsou současné hašovací funkce slabé a jaké jsou lepší vlastnosti hashovacích funkcí NMAC a HMAC?

Doporučení práce k obhajobě: **ano**

Navržený klasifikační stupeň: **výborně**

Posudek vypracoval:

Jméno, tituly: Soňa Neradová, Ing.
Zaměstnavatel: Univerzita Pardubice, FEI

V Pardubicích dne: 20. 5. 2015 Podpis: