

## Posudek vedoucího diplomové práce

Jméno studenta: Bc. Marek Farkas  
Téma práce: Implementace RNG pomocí dostupných zdrojů entropie v systémech Linux a Windows  
Autor posudku: Mgr. Tomáš Hudec, KIT FEI UPa

### Cíl práce:

Teoretická část vysvětlí pojmy týkající se entropie, hustoty informací a náhodnosti, popíše známé metodiky hodnocení kvality generátorů náhodných čísel a bude rozšířena o využití entropie v praxi, zejména v oblasti zabezpečení (kryptografie, kryptografické algoritmy a protokoly).

Na základě výsledků výše uvedené BP bude pomocí dostupných zdrojů entropie implementován generátor náhodných čísel (RNG). Jeho výstup pak bude posouzen pomocí vhodných metod popsanych v teoretické části.

### 1. Uplatnění metod (příslušejících navazujícímu magisterskému studiu)

Student využil znalosti a metody zejména z předmětů týkajících se počítačích systémů a programování.

### 2. Produkt vytvořený při vypracování DP

Výsledků práce je několik, zejména přehled možných zdrojů entropie v systémech osobních počítačů a serverů pod operačními systémy Linux a Windows, dále pak popis hodnotících metod generátorů náhodných čísel a zejména pak samotný program generátoru náhodných čísel používající ke generování dříve popsané zdroje entropie v systému.

### 3. Prokázání správnosti navrženého řešení problému

Výsledný program generátoru byl podroben testům pomocí hodnotících metod RNG, které byly rovněž v práci popsány. Dle výsledků testů lze vytvořený RNG považovat za kvalitní.

### 4. Naplnění uložených cílů

Všechny cíle byly splněny.

### 5. Kvalita textu z hlediska jeho struktury, srozumitelnosti, jazykové a typografické úrovně

Struktura textu a logické členění do kapitol jsou v pořádku, v práci je však množství gramatických a typografických chyb. Z nejzávažnějších: Kapitoly nezačínají na samostatné stránce, chyby v interpunkci, ve shodě (i/y), nečeské uvozovky.

### 6. Nejasnosti v DP, které je třeba objasnit při obhajobě, a doplňující otázky

Ve kterých oblastech IT najde vámi vytvořený generátor náhodných čísel uplatnění?

Práci doporučuji k obhajobě.

Navržená výsledná známka: výborně minus

V Pardubicích, dne: 29. 5. 2017

-----  
podpis