Posudek diplomové práce pana Bc. Marka Farkase nazvané „I*mplementace RNG pomocí dostupných zdrojů entropie v systémech Linux a Windows*“
Oponent doc. Dr. Ing. Tomáš Brandejský

Diplomová práce se zabývá přínosným tématem především pro oblast zabezpečení dat. Práce má rozsah 55 stran plus přílohy. Je organizována přehledně a systematicky. Diplomant se seznámil se základními pojmy, zavedl pojem entropie. Prostudoval využitelné zdroje entropie v dnešních PC a navrhl SW implementaci RNG.
První dvě kapitoly se představují základní pojmy a jsou s menšími modifikacemi převzaty z práce bakalářské (!), na kterou tato práce navazuje. Třetí kapitola nazvaná entropie v praxi přináší příklady využití generátorů náhodných čísel v kryptografii. Jedná se o zajímavý průřez uplatněním kryptografie v lidských dějinách. Rovněž ve čtvrté kapitole nazvané zdroje entropie autor uvádí, že vznikla přepracováním a rozšířením textu bakalářské práce. V kapitole 5 pak popisuje vlastní implementaci RNG v jazyce JAVA.
Text práce je čtivý a bez výraznějších stylistických, nebo dokonce pravopisných chyb.Po typografické stránce je práce rovněž v pořádku.
Diplomant ověřil generátor vycházející ze sledování uživatelských aktivit ve třech pokusech, které v závěru práce popsal a dokumentoval. Ne, že by s jeho aplikací nebylo možno tyto pokusy rekonstruovat, přesto je škoda, že diskutované datové soubory na CD přiloženy nebyly, adresář, kam měly být zřejmě umístěny zůstal prázdný.
Mimo zásad pro vypracování práce neobsahuje explicitně definované cíle, což bych ale v tomto případě nebral jako příliš důraznou výtku, protože implicitní cíl práce je nasnadě.
Dle mého názoru se autor dokázal zorientovat v obtížné oblasti a i když ji udržel na úrovni nevyžadující znalost vyšší matematiky, přesto prokázal schopnost zorientovat se v matematiky náročnějších problémech. Rovněž tak vytvořil příslušnou ukázkovou SW aplikaci demonstrující základní myšlenky publikované v textu.

Připomínky:
Str. 15: Neexistuje žádná Monte Carlova hodnota, nebo metoda pojmenovaná po nějakém panu Monte Carlovi. Metoda Monte Carlo je nazváná podle jistého města s blízkým vztahem k náhodným procesům a vytvořili ji především pánové Marcim Ulam a John Von Neumann.
Kap. 3.1: hovoří se o třech různých kryptosystémech, neuvádí se o kterých. Prosím uveďte.
Kap. 3,1: Starověcí Číňané,… například Čingischán – ale Čingischán byl Mongol.
Obtížná čitelnost – např. Str. 33: Twofish je šifra... Twofish je rychlý…
Kap. 3.2.2, str. 36: vysvětlete pojem „Krátké klávesy“ - není nikde definován.
Kap. 4.1, str. 40: Nebyli bychom rádi, pokud bychom museli dnes používat displeje s rozlišením jednotek tisící obrazových bodů – to nabízelo např. ZX Spectrum (320x240 bodů)
Kap. 5: Součástí jazyka C++ je od standardu verze 10/11 také knihovna <random>implementující m.j. i nedeterministický „True random number generator“. Mohl byste ho porovnat se svým řešením?

*Práci hodnotím **B -velmi dobře** a doporučuji k obhajobě*

V Pardubicích dne 26.5.2017