

Posudek práce

předložené na Přírodovědecké fakultě JU

☐ posudek vedoucího
☐ bakalářské práce

☒ posudek oponenta
☒ diplomové práce

Autor/ka: Bc. Stanislav Pecka

Název práce: Návrh a implementace generátoru náhodných čísel

Studijní program a obor: Aplikovaná informatika

Rok odevzdání: 2018

Jméno a tituly vedoucího/opponenta: Ing. Jiří Jelínek, CSc.

Pracoviště: ÚAI

Kontaktní e-mail: jjelinek@prf.jcu.cz

Odborná úroveň práce:

☐ vynikající ☐ velmi dobrá ☒ průměrná ☐ podprůměrná ☐ nevyhovující

Věcné chyby:

☐ téměř žádné ☒ vzhledem k rozsahu přiměřený počet ☐ méně podstatné četné ☐ závažné

Výsledky:

☐ originální ☒ původní i převzaté ☐ netriviální kompilace ☐ citované z literatury ☐ opsané

Rozsah práce:

☐ veliký ☒ standardní ☐ dostatečný ☐ nedostatečný

Grafická, jazyková a formální úroveň:

☐ vynikající ☐ velmi dobrá ☒ průměrná ☐ podprůměrná ☐ nevyhovující

Tiskové chyby:

☐ téměř žádné ☒ vzhledem k rozsahu a tématu přiměřený počet ☐ četné

Celková úroveň práce:

☐ vynikající ☐ velmi dobrá ☒ průměrná ☐ podprůměrná ☐ nevyhovující

Slovní vyjádření, komentáře a připomínky vedoucího/oponenta:

Cílem předložené práce je dle zadání návrh a implementace několika druhů hardwarových generátorů skutečně náhodných čísel a jejich porovnání. Kritéria porovnání jsou rovněž stanovena v zadání a jsou jimi míra náhodnosti generovaných dat, rychlost generování, náročnost implementace a masovost rozšíření. Preferováno bylo využití moderních i mobilních technologií. Téma práce je bezpochyby aktuální.

Práce je rozvržena do devíti věcných kapitol s nerovnoměrnou úrovní členění. V úvodu práce autor naznačuje motivaci souvislostí s moderními nástroji komunikace.

Cíle práce jsou podrobněji popsány v kapitole 2 a odpovídají zadání.

V kapitole 3 autor občas používá poněkud nevhodnou formulaci (kryptografie vyžadující vysoký stupeň zabezpečení), nesoulad v podřízenosti kapitol lze najít v kapitolách 3.4 a 3.5. V podkapitole 3.3 se autor věnuje útokům na existující generátory, což však není předmětem práce. Popis šifrování vybočuje z rámce zadání a k základnímu tématu práce má pouze okrajový vztah. Kapitola 3.6 se věnuje kritériím kvality generátorů náhodných čísel a očekával bych členění dle zadání práce a v něm definovaných kritérií hodnocení kvality generátorů. Kritický obor W definovaný v kapitole 3.6.4 a 3.6.5 je kompletním oborem reálných čísel.

Kapitola 4 je zaměřena na stávající řešení generátorů skutečně náhodných čísel. U konkrétních realizací bych opět očekával informace o jejich kvalitě s využitím definovaných kritérií (viz zadání práce). Uvedené implementace jsou však pouze popsány, a to ještě na velmi vysoké úrovni obecnosti. V kapitole 4.4 je nutno upozornit na základní předpoklad využití technologií založených na chování uživatele a tím je, jak sám autor uvádí, "různorodá obsluha PC". V případě využívání konkrétního technického prostředku jediným člověkem je obtížné vstupní data považovat za náhodně generovaná.

Kapitola 5 se zabývá použitými vývojovými nástroji, přičemž popis systému Android či jazyka Java považuji v daném rozsahu za nadbytečný.

Kapitola 6 se již zabývá navrhovanými implementacemi generátoru náhodných čísel. Ve vzorci 6.1 není uvedeno, z jakého intervalu pochází generované číslo RND. Hodnota C je navržena pouze empiricky. Není jasné, zda u přístupů založených na chování uživatele byla zajištěna výše uvedená různorodá obsluha.

Kapitola 7 ukazuje možnou implementaci Vernamovy šifry. Ta byla provedena pouze pro jeden typ navrhovaného generátoru, pro hlavní téma práce jde pouze o okrajovou ukázkou praktického použití.

V kapitole hodnocení dat (8.3) autor poukazuje na jím špatně zvolenou metodiku při zvolení hodnoty HM, na tento nedostatek však nereaguje. Grafy v této kapitole rovněž ukazují, že použité techniky nevedly k dodržení jedné ze základních premis skutečného generátoru náhodných čísel, a tedy rovnoměrného rozložení generovaných výstupů. Ze vstupních grafů také vyplývá, že řada z použitých metod je silně závislá na konkrétním experimentu a neposkytuje tedy vyrovnané výstupní hodnoty entropie. Závěr o jiném rozložení náhodných hodnot než rovnoměrném je potvrzen rovněž v kapitole 8.5. Autor však z těchto výstupů nečiní žádné další závěry. Souhrnné hodnocení je uvedeno v tabulce 28 (která neobsahuje všechna kritéria definovaná v zadání), přičemž tato tabulka nerespektuje váhu jednotlivých testovacích metod pro výsledné hodnocení generátoru. Na problematiku váhy jednotlivých kritérií upozorňuje sám autor při diskusi ohledně započtení kritéria rychlosti generování. Ve vyhodnocení také zcela chybí porovnání se standardními generátory skutečných náhodných čísel i například využití stejných zobrazovacích technik, které autor uvádí u popisu náhodných čísel hned v úvodu práce (obr. 1 a 2). Celkově lze tak metodiku vyhodnocení považovat za poněkud účelovou a nesystémovou. Diskutabilní jsou rovněž finální závěry autora a je otázka, zda některý z jím navrhovaných generátorů by byl prakticky využitelný jako generátor skutečně náhodných čísel. Sporný je i názor autora, že jeho cílem nebylo vytvořit plnohodnotný generátor náhodných čísel, což poněkud odporuje zadání.

V práci se vyskytuje rovněž určitý počet gramatických chyb a je dostatečně dokumentována z hlediska grafických komponent (grafy, tabulky, obrázky). Ne vždy jsou však tyto komponenty využity dostatečně efektivně. V citované literatuře autor uvádí celkem 49 titulů, přičemž např. titul 3 a 30 se opakují (z uvedeného odkazu nelze rozlišit, zda se jedná o různé zdroje). Příložené CD obsahuje jak naměřená data, tak zdrojové kódy jednotlivých generátorů a rovněž text práce.

Vzhledem k výše uvedeným připomínkám navrhuji práci k obhajobě s hodnocením 2 až 3, a to podle průběhu obhajoby.

Případné otázky při obhajobě a náměty do diskuze:

1. Můžete uvést do souvislosti obsah kap. 3.6 a kritéria uvedená v zadání?
2. Byla při generování čísel zajištěna "různorodá obsluha" zmiňovaná v textu?
3. Proč byla volena hodnota C ve vzorci 6.1 uvedeným způsobem?
4. Jaké závěry vyvozujete ze sběru a hodnocení dat v kap. 8?
5. Proč nebyly do hodnocení v tab. 28 implementovány váhy kritérií?
6. Porovnejte používané generátory skutečně náhodných čísel s vašimi návrhy a implementacemi.

Práci

☒ doporučuji

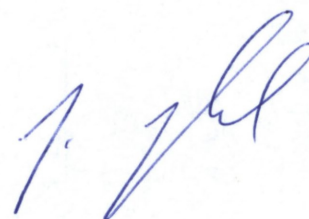
☐ nedoporučuji

uznat jako diplomovou/bakalářskou.

Navrhuji hodnocení stupněm:

☐ výborně ☐ velmi dobře ☒ dobře ☐ neprospěl/a

Místo, datum a podpis vedoucího/oponenta:
V Českých Budějovicích, 8. 1. 2019



Posudek práce

předložené na Přírodovědecké fakultě JU

☐ posudek vedoucího
☐ bakalářské práce

☒ posudek oponenta
☒ diplomové práce

Autor: Bc. Stanislav Pecka
Název práce: Návrh a implementace generátoru náhodných čísel
Studijní program a obor: Aplikovaná informatika
Rok odevzdání: 2018

Jméno a tituly vedoucího/opponenta: Libor Dostálek
Pracoviště: UAI
Kontaktní e-mail: dostalek@prf.jcu.cz

Odborná úroveň práce:

☐ vynikající ☐ velmi dobrá ☒ průměrná ☐ podprůměrná ☐ nevyhovující

Věcné chyby:

☐ téměř žádné ☒ vzhledem k rozsahu přiměřený počet ☐ méně podstatné četné ☐ závažné

Výsledky:

☐ originální ☐ původní i převzaté ☒ netriviální kompilace ☐ citované z literatury ☐ opsané

Rozsah práce:

☐ veliký ☐ standardní ☒ dostatečný ☐ nedostatečný

Grafická, jazyková a formální úroveň:

☐ vynikající ☐ velmi dobrá ☒ průměrná ☐ podprůměrná ☐ nevyhovující

Tiskové chyby:

☐ téměř žádné ☒ vzhledem k rozsahu a tématu přiměřený počet ☐ četné

Celková úroveň práce:

☐ vynikající ☐ velmi dobrá ☒ průměrná ☐ podprůměrná ☐ nevyhovující

Slovní vyjádření, komentáře a připomínky vedoucího/oponenta:

Z grafů 2 až 6 je zjevné, že výstupy všech implementovaných generátorů pseudonáhodných čísel nemají rovnoměrné rozdělení. Což bylo i potvrzeno pomocí testu Kolmogorov-Smirnov. Podle mého názoru, tím pádem další testování již postrádalo smyslu. Tato informace měla být vytěžena k tomu, že implementované generátory jsou pro praktické využití nevhodné a jejich využití může přinést bezpečnostní rizika. Zejména pokud se využijí pro generování kryptografického materiálu.

Škodou je, že nebyl učiněn pokus výstupy generátorů transformovat tak, aby měly rovnoměrné rozdělení.

Případné otázky při obhajobě a náměty do diskuze:**Práci**

☒ doporučuji

☐ nedoporučuji

uznat jako diplomovou/bakalářskou.

Navrhuji hodnocení stupněm:

☐ výborně ☒ velmi dobře ☐ dobře ☐ neprospěl/a

Místo, datum a podpis vedoucího/oponenta:
V Českých Budějovicích

