Posudek práce

předložené na Přírodovědecké fakultě JU

❑ posudek vedoucího ☑ posudek oponenta
☑ bakalářské práce ❑ diplomové práce

Autor/ka:	Petr Kopecký
Název práce:	**Praktická implementace Vernamovy šifry**
Studijní program a obor:	**Aplikovaná Informatika**
Rok odevzdání:	**2011**

Jméno a tituly vedoucího/oponenta:	Ing. Václav Novák
Pracoviště:	Ústav aplikované informatiky PřF JCU
Kontaktní e-mail:	vacnovak@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:

Práce je vysoce specializována na jeden typ šifry a její implementaci. Jedná se o Vernamovu šifru. Jsou zde tři části. V první části je popsán současný náhled na Vernamův algoritmus v kontextu dnešních požadavků. V druhé části je diskutována kvalita šifry za pomoci Dieherdtových testů. No a ve třetí části jsou shrnuty výsledky testů a doporučení pro další rozvoj.
Práce však bohužel obsahuje, jak formální, tak faktické chyby či nepřesnosti.

K faktickým chybám lze řadit:

1. Citace [11] – je použita Wikipedia – nedůvěryhodný zdroj
2. Strana 23, 7 řádek. Má následovat výpis, ale následuje vysvětlení
3. Na obrázcích 4,5,6 chybí popis os a celková plocha grafu neodpovídá 100%

K formálním patří např.:

1. Strana 3, 13 řádek shora. Nejasné slovní spojení: „Pro dešifrovací postup byl stejný jako šifrovací …“
2. Strana 18, 7 řádek shora. Chybí konec závorky.
3. Strana 25. Závěr je nedostatečný není zde shrnuto hodnocení co a do jaké míry bylo dosaženo. Byly splněny cíle práce ?

V práci zcela chybí odkazy na čerpanou literaturu, ta je pouze v příloze a není jasno v jakém kontextu je použita.

Případné otázky při obhajobě a náměty do diskuze:

1. Student navrhuje v kapitole 9 vytvoření vlastního generátoru náhodných čísel. Proč?
2. Vysvětlete vztah na straně 16. Zejména pojem w-kritický obor?

Celkově práce působí rozpačitě, ale student odvedl jistě příslušné penzum práce a prokázal porozumění problematice.

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 12.1.2012

Václav Novák