Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

OPONENTSKÝ POSUDEK BAKALÁŘSKÉ PRÁCE

Student: **NEDBAL JAN** **Oponent:** **Ing. Milan Oulehla, Ph.D.**

Studijní program: **Inženýrská informatika**
Studijní obor / specializace: **Softwarové inženýrství**
Akademický rok: **2022/2023**

Téma bakalářské práce: **Postkvantové algoritmy se zaměřením na homomorfní šifrování**

Hodnocení práce:		**A**	**B**	**C**	**D**	**E**	**F**
		Hodnocení: A – nejlepší; F - nevyhovující					
1.	Aktuálnost řešeného tématu	☐	☐	☒	☐	☐	☐
2.	Obtížnost zadaného úkolu	☐	☐	☐	☒	☐	☐
3.	Splnění všech bodů zadání	☐	☐	☐	☐	☒	☐
4.	Vhodnost zvolené metody řešení	☐	☐	☐	☐	☒	☐
5.	Logické členění práce	☐	☐	☐	☐	☒	☐
6.	Úroveň jazykového zpracování	☐	☐	☐	☐	☒	☐
7.	Formální úroveň práce	☐	☐	☐	☐	☒	☐
8.	Práce s literaturou a její citace	☐	☐	☐	☐	☒	☐
9.	Úroveň zpracování teoretické části	☐	☐	☐	☐	☒	☐
10.	Kvalita zpracování praktické části	☐	☐	☐	☐	☒	☐
11.	Dosažené výsledky práce	☐	☐	☐	☐	☒	☐
12.	Přínos práce a její využití	☐	☐	☐	☐	☒	☐

Celkové hodnocení práce:
Výsledná známka není průměrem výše uvedených hodnocení. Známku uvede oponent dle svého uvážení dle klasifikační stupnice ECTS:
A – výborně, B – velmi dobře, C – dobře, D – uspokojivě, E – dostatečně, F – nedostatečně.
Stupeň F znamená též „nedoporučuji práci k obhajobě“.

Předloženou bakalářskou práci doporučuji k obhajobě a navrhuji hodnocení

E - dostatečně.

V případě hodnocení stupněm „F – nedostatečně“ uveďte do připomínek a slovního vyjádření hlavní nedostatky práce a důvody tohoto hodnocení.

Otázky k obhajobě:
Otázka 1:
V podkapitole 3.1 Výhody kvantových šifer uvádíte:
„Další výhodou kvantové kryptografie je, že může poskytnout zabezpečení proti počítačovým útokům. Tradiční metody šifrování jsou citlivé na výpočetní výkon útočníka, který dokáže šifru prolomit pomocí velmi výkonné počítačové technologie. Kvantová kryptografie je na druhou stranu vůči těmto útokům imunní.“

- Co považujete za tradiční metody šifrování?
- Můžete popsat „citlivost na výpočetní výkon útočníka“ u šifry AES?

Otázka 2:
Je kód, který uvádíte v 6.3.3 Ověření prvočísla vhodný pro testování prvočíselnosti velkých čísel?

Další připomínky, vyjádření, náměty k obhajobě práce (možno pokračovat i na další stránce):
Teoretická část bakalářské práce vykazuje po odborné stránce značné nedostatky. Jedná se například o:

- neúplné nebo nepřesné popisy šifrovacích algoritmů,
- špatné nebo nevhodné používání některých pojmů,
- tvrzení, která nejsou podpořena citacemi literárních pramenů,
- apod.

V praktické části práce jsou ukázky zdrojových kódů, jejichž popis je příliš stručný nebo nepřesný. Kompletní kódy nejsou k práci přiloženy, takže nebylo možné ověřit jejich funkčnost.

Práce obsahuje i řadu jazykových a formálních nedostatků, které ale nepovažuji za zásadní.

Celkově je práce na samé hranici klasifikačního stupně E, obhajoba před komisí, bude proto zásadní.

Datum 1. 6. 2023 Podpis oponenta bakalářské práce