Univerzita Hradec Králové
Fakulta informatiky a managementu

POSUDEK VEDOUCÍHO BAKALÁŘSKÉ PRÁCE

Jméno studenta: Matěj Boura

Název práce: Zabezpečení certifikátů Eliptických křivek

Autor posudku: Ing. Hana Švecová

Cíl práce: Cílem práce je analýza zabezpečení certifikátů Eliptických křivek a možnosti jejich využití v praxi.

Povinná kritéria hodnocení práce	**Stupeň hodnocení** (známka)					
	A	**B**	**C**	**D**	**E**	**F**
Práce svým zaměřením odpovídá studovanému oboru	☒	☐	☐	☐	☐	☐
Vymezení cíle a jeho naplnění	☐	☒	☐	☐	☐	☐
Zpracování teoretických aspektů tématu	☐	☒	☐	☐	☐	☐
Zpracování praktických aspektů tématu	☐	☒	☐	☐	☐	☐
Adekvátnost použitých metod, způsob jejich použití	☐	☒	☐	☐	☐	☐
Hloubka a správnost provedené analýzy	☐	☒	☐	☐	☐	☐
Práce s literaturou	☐	☒	☐	☐	☐	☐
Logická stavba a členění práce	☐	☒	☐	☐	☐	☐
Jazyková a terminologická úroveň	☐	☐	☒	☐	☐	☐
Formální úprava a náležitosti práce	☐	☒	☐	☐	☐	☐
Vlastní přínos studenta	☐	☒	☐	☐	☐	☐
Využitelnost výsledků práce v teorii (v praxi)	☐	☐	☒	☐	☐	☐

Vyjádření k výsledku anti-plagiátorské kontroly

Anti plagiátorská kontrola eVSKP identifikovala celkovou podobnost: 7 %.

Dílčí připomínky a náměty:

Stran stylistiky práce obsahuje drobné gramatické chyby v podobě využití neformálních slov např. str. 1 „ohledně“, str. 4 „dojít“, str. 21 „Zajímavé je…“ **.**

Celkové posouzení práce a zdůvodnění výsledné známky:

Bakalářská práce se zabývá analýzou a využitím Eliptických křivek v moderních kryptografických systémech. V první části práce autor charakterizoval Teorii eliptických křivek, v další části autor analyzoval možnosti zabezpečení eliptických křivek, a v poslední praktické části se zaměřil na využití Eliptických křivek v praxi (SSH, Bitcoin, Elektronický podpis aj).
Autor při zpracovávání své bakalářské práce vše aktivně konzultoval, a obratem zapracovával připomínky ze strany vedoucího práce.
Zvolené téma kvalifikační práce bylo velmi náročné na zpracování, a i přes dílčí drobné gramatické nedostatky je nutné ocenit autorovu snahu toto náročné téma zpracovat.
Práce splňuje požadavky kladené na bakalářskou práci a práci doporučuji k obhajobě.

Otázky k obhajobě:

1) Charakterizujte Bitcoin a jeho využití v praxi.
2) Vysvětlete využití ECC u elektronického podpisu (kvalifikovaného certifikátu).

Práci doporučuji k obhajobě.

Navržená výsledná známka: B

V Hradci Králové**, dne 13. května 2022**

podpis