Univerzita Hradec Králové
Fakulta informatiky a managementu

POSUDEK OPONENTA BAKALÁŘSKÉ PRÁCE

Jméno studenta: Daniel Havrda

Název práce: Analýza vybraných kryptografických algoritmů

Autor posudku: Josef Horálek, Ph.D.

Cíl práce: Cílem práce bylo navrhnout a provést testy pro analýzu vybraných šifer s důrazem na výpočetní výkon a porovnat výsledky.

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

Antiplagiátorská kontrola eVSKP identifikovala celkovou podobnost: 0%.

Dílčí připomínky a náměty:

Autor práce měl grafy 4.4 a 4.5 uvést ve větším rozlišení, tak aby byla maximalizována jejich vypovídající hodnota.

Celkové posouzení práce a zdůvodnění výsledné známky:

Předložená práce svojí logickou strukturou, rozsahem a zpracováním zcela splňuje požadavky kladené na bakalářskou práci.
V teoretické části práce prokazuje znalost principů kryptografie, využívaných algoritmů a možnosti využití kryptografie pro zajištění integrity a autentizace.
V praktické části práce pak autor seznamuje s vybraným způsobem testování a výsledky realizovaných testů. Výsledky jsou zpracovány za využití grafů a relevantním komentářem.
Autorovi lze doporučit v dané problematice pokračovat se naměřením na využití eliptických křivek.

Otázky k obhajobě:

Nejsou.

Práci doporučuji k obhajobě.

Navržená výsledná známka: A

V Hradci Králové**, dne 30. srpna 2019**

podpis