Univerzita Hradec Králové
Fakulta informatiky a managementu

POSUDEK VEDOUCÍHO BAKALÁŘSKÉ PRÁCE

Jméno studenta: Daniel Havrda

Název práce: Analýza vybraných kryptografických algoritmů

Autor posudku: Vladimír Soběslav

Cíl práce: Analyzovat problematiku kryptografických algoritmů a srovnat vybrané symetrické šifry s důrazem na výpočetní výkon.

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

Dle anti-plagiátorské kontroly je zde nulová shoda.

Dílčí připomínky a náměty:

V bakalářské práci bylo možné hlouběji analyzovat využití jednotlivých druhů kryptografie a šifer ve světě, např. za pomoci relevantních zdrojů, respektive statistik a přehledů.

Celkové posouzení práce a zdůvodnění výsledné známky:

Bakalářská práce je zaměřena na problematiku šifrovacích algoritmů. Jedná se o etablované téma s dostatečným množství zdrojů.
Závěrečnou práci je možné rozdělit do dvou logických celků, teoretickou analýzu symetrické a asymetrické kryptografie. Teoretickou část reprezentuje první až třetí kapitola. Autor v této části jednoznačně deklaroval cíle diplomové práce, dále pak stručně, avšak správně, představil základní teoretická východiska. V následující části autor provedl srovnání s využitím dvou základních knihoven. Čtvrtá a pátá kapitola pak velmi přehledně reprezentují rychlosti jednotlivých šifer a v reálných testech.
Celkově jedná o zajímavou závěrečnou práci, která může čtenáři posloužit pro rychlou orientaci v problematice nejpoužívanějších kryptografických algoritmů a jejich výpočetní náročnosti.

Otázky k obhajobě:

1) Původní předpoklad podobnosti při výpočtech se nepotvrdil, pokuste se představit zmiňované optimalizace na úrovni procesorových instrukcí, jež zásadně ovlivňují rychlost zpracování šifrování.

Práci doporučuji k obhajobě.

Navržená výsledná známka: B

V Hradci Králové**, dne 5. září 2019**

podpis