Posudek vedoucího bakalářské práce

Student:	Ondřej Ruml
Číslo studenta:	E22422
Název bakalářské práce:	Porovnání vybraných kryptografických algoritmů a jejich využití v praxi
Cíl práce:	Popsat a porovnat vybrané kryptografické algoritmy a vyhodnotit jejich efektivitu a aplikovatelnost v kyberprostoru.
Vedoucí práce:	Mgr. Libor Koudela, Ph.D.
Studijní program:	B0688A140004 Informatika a systémové inženýrství
Akademický rok:	2024/2025

Náročnost tématu

	výborně	velmi dobře	vyhovující	nevyhovující	nelze hodnotit
Teoretické znalosti	☒	☐	☐	☐	☐
Vstupní údaje a jejich zpracování	☐	☒	☐	☐	☐
Použité metody	☒	☐	☐	☐	☐

Kritéria hodnocení práce

	výborně	velmi dobře	vyhovující	nevyhovující	nelze hodnotit
Stupeň splnění cíle práce	☒	☐	☐	☐	☐
Původnost zapracování tématu	☐	☒	☐	☐	☐
Adekvátnost použitých metod	☒	☐	☐	☐	☐
Hloubka provedené analýzy (ve vztahu k tématu)	☐	☒	☐	☐	☐
Logická stavba práce a rozsah	☒	☐	☐	☐	☐
Práce s českou a zahraniční literaturou včetně citací	☒	☐	☐	☐	☐
Formální úprava práce (text, grafy, tabulky)	☒	☐	☐	☐	☐
Jazyková úroveň (styl, gramatika, terminologie)	☐	☒	☐	☐	☐

Využitelnost výsledků práce

	vysoká	střední	nízká	nelze hodnotit
Pro teorii	☐	☒	☐	☐
Pro praxi	☒	☐	☐	☐

Ostatní připomínky k práci

Autor se zabývá porovnáním vybraných kryptografických algoritmů a jejich využitím v praxi. První kapitola pojednává o vybraných pojmech a poznatcích z kryptologie a teorie informačních systémů a těch partií matematiky, které mají význam z hlediska šifrování. Druhá kapitola uvádí klasifikaci a přehled základních šifrovacích algoritmů s ilustračními příklady. Ve třetí kapitole jsou porovnány vybrané kryptografické algoritmy na základě stanovených kritérií. Čtvrtá kapitola uvádí podklady pro výběr vhodného kryptografického algoritmu a příklady praktického využití některých algoritmů.
Autor prokázal dobré zvládnutí studované problematiky, což dokládají i přiložené ukázky kódů v programovacím jazyce Python.
Při porovnávání kryptografických algoritmů vychází autor ze standardů organizací NIST a NÚKIB. Práce může dobře posloužit nejen jako základ pro orientaci v dané problematice, ale i jako vodítko při řešení rozhodovacího problému týkajícího se zabezpečení citlivých dat.
Po formální stránce má práce dobrou úroveň; překlepy a opomenutí v interpunkci v textu jsou, ale nejsou nijak časté.
Cíl práce byl splněn, práci doporučuji k obhajobě.

Vyjádření k výstupům ze systému Theses

Nejvyšší míra podobnosti uvedená v systému Theses je 2 %, o plagiát se nejedná.

Otázky a náměty k obhajobě

Velmi citlivou záležitostí je zadávání údajů o platební kartě v internetovém prostředí. Můžete uvést, jaké metody šifrování využívají běžné platební brány? Jakých rizik by si měl být uživatel při zadávání takových údajů vědom?

Závěrečné hodnocení

Práci **doporučuji** k obhajobě.
Tuto bakalářskou práci navrhuji hodnotit známkou: **A**

V Pardubicích 16.5.2025

Podpis .....