

POSUDEK VEDOUCÍHO DIPLOMOVÉ PRÁCE

Student: Bc. Baslar Jan

Vedoucí práce: Ing. Petr Žáček, Ph.D.

Studijní program: Informační technologie
Specializace: Kybernetická bezpečnost
Akademický rok: 2024/2025

Téma diplomové práce: Vzorová implementace pokročilých kryptografických algoritmů

Hodnocení práce:

	A	B	C	D	E	F
	Hodnocení: A – nejlepší; F - nevyhovující					
1. Splnění všech bodů zadání	☒	☐	☐	☐	☐	☐
2. Vhodnost zvolené metody řešení	☒	☐	☐	☐	☐	☐
3. Členění práce (kapitoly, podkapitoly, odstavce)	☒	☐	☐	☐	☐	☐
4. Práce s literaturou a její citace	☒	☐	☐	☐	☐	☐
5. Úroveň jazykového zpracování	☒	☐	☐	☐	☐	☐
6. Formální úroveň práce	☒	☐	☐	☐	☐	☐
7. Kvalita zpracování teoretické části	☒	☐	☐	☐	☐	☐
8. Kvalita zpracování praktické části	☒	☐	☐	☐	☐	☐
9. Dosažené výsledky práce	☒	☐	☐	☐	☐	☐
10. Přínos práce a její využití	☒	☐	☐	☐	☐	☐
11. Spolupráce autora s vedoucím práce	☒	☐	☐	☐	☐	☐

Výsledek kontroly plagiátorství:

Práce byla posouzena z hlediska plagiátorství s výsledkem 100% shodnosti, ale pouze v konfiguračních souborech u kterých to lze očekávat. Práce není plagiát.

Celkové hodnocení práce:

Výsledná známka není průměrem výše uvedených hodnocení. Známkou uvede vedoucí 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 diplomovou práci doporučuji k obhajobě a navrhuji hodnocení

A - výborně.

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

Další připomínky, vyjádření, náměty k obhajobě práce (možno pokračovat i na další stránce):

K této diplomové práci nemám výhrad, student si téma zvolil sám, její praktický přesah pro firmu MONET+ jen nezpochybnitelný. Velmi kvalitně zpracovaná práce. Níže příkládám a cituji vyjádření k práci z firmy:

"Divize Elektronických plateb společnosti MONET+ využívá ve svých systémech rozsáhlé množství aplikované kryptografie pro zabezpečení poskytovaných služeb. Tyto služby jsou ve většině případů chráněny pomocí HSM (Hardware Security Module), nicméně v rámci vývoje, integrace a ladění nestandardních stavů je často nezbytné ověřovat kryptografické operace manuálně.

V současnosti k těmto účelům používáme sadu různorodých interních nástrojů, které však mají omezenou uživatelskou přívětivost a často vyžadují hlubší technické znalosti k jejich správnému použití.

Z těchto důvodů jsme společně s kolegou Janem Baslarem zahájili práci na nové platformě, která by sloužila jako jednotné prostředí pro všechny kryptografické nástroje. Zde musím vyzdvihnout Janův přístup, kdy navrhl systém pro centrální správu testovacích klíčů. Tento návrh výrazně zjednodušuje práci s nástroji, umožňuje snadnější integraci navazujících operací a podporuje opakované využití již vytvořených klíčových struktur.

Dalším silným aspektem aplikace je uživatelské rozhraní, které je moderní, přehledné a dostupné napříč platformami. Díky tomu je aplikace využitelná pro široké spektrum týmů v rámci naší společnosti a významně přispívá ke zvýšení efektivity práce.

Za Divizi Elektronických plateb MONET+"

Nejen na základě výše uvedeného, lze konstatovat splnění všech bodů zadání, a proto doporučuji práci k obhajobě a navrhuji klasifikovat stupněm A - výborně.

Datum 9.6.2025

Podpis vedoucího diplomové práce