

POSUDEK OPONENTA DIPLOMOVÉ PRÁCE

Student: Bc. Jan Baslar

Oponent: Ing. Michal Šmiraus, Ph.D.

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

Téma diplomové práce: Vzorová implementace pokročilých kryptografických algoritmů

Hodnocení práce:

Předložená diplomová práce se zabývá návrhem a realizací multiplatformní aplikace zaměřené na implementaci kryptografických algoritmů s důrazem na potřeby firmy Monet. Práce v teoretické části detailně a přehledně popisuje principy klasických i bankovních kryptografických algoritmů, včetně DES, AES, MAC a PIN Block, přičemž ukazuje dobré porozumění problematice. Praktická část se věnuje návrhu a vývoji uživatelsky přívětivé aplikace, včetně validace vstupů, podpory různých platforem a bezpečné správy klíčů, což demonstduje velmi solidní praktické zvládnutí moderního přístupu při vývoji softwaru.

Menší výhrady lze mít ke stylistické stránce textu, místy se vyskytují překlapy a nedůslednosti v sazbě, případně nejednotný jazyk odborných pasáží. Přesto se jedná o nadprůměrně zpracovanou práci, která prokazuje jak odborné znalosti autora, tak schopnost vytvořit funkční nástroj, který může být firmou dále využíván a rozšiřován – práci **doporučuji k obhajobě**.

Otázky k obhajobě:

1. Jak je v aplikaci technicky řešeno generování MAC podle normy ISO 9797 a jaký vliv má volba paddingu a typu MAC na výslednou autentizaci zprávy ?
2. Jaké rozdíly v implementaci a bezpečnosti jste zaznamenal mezi provozními režimy ECB, CBC a CTR u algoritmů DES a AES ?

Celkové hodnocení práce:

Známku uvede oponent 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.

Datum

8.6. 2025

Podpis oponenta diplomové práce