Univerzita Hradec Králové
Fakulta informatiky a managementu

POSUDEK VEDOUCÍHO DIPLOMOVÉ PRÁCE

Jméno studenta: Bc. Zdeněk Hejzlar

Název práce: Aplikační podpora výuky kryptografie s využitím PHP frameworku

Autor posudku: Mgr. Jana Medková, Ph.D.

Cíl práce: Cílem diplomové práce je vytvoření webové aplikace pro podporu výuky kryptografie. Aplikace bude sloužit jako interaktivní nástroj pro studium vybraných kryptografických metod. Hlavními úkoly jsou pečlivé nastudování principů kryptografických algoritmů a vlastní implementace těchto algoritmů, která umožní uživateli aplikace krokování metod a analýzu jednotlivých kroků uvnitř algoritmů. Dalším cílem je návrh moderního uživatelského prostředí s využitím PHP frameworku. Součástí práce je otestování aplikace z hlediska správnosti implementovaných algoritmů a její uživatelské přijatelnosti a použitelnosti.

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

Práce vykazuje 2 % podobnost s dostupnými texty. Se všemi texty je podobnost vždy méně než 1 %. Podobnost je většinou v dílčích frází v popisu šifer a nastavení jejich parametrů. Dále je tu podobnost s materiály vydanými Národním úřadem pro kybernetickou bezpečnost, které jsou řádně citovány.

Dílčí připomínky a náměty:

Praktická část práce je na velmi dobré úrovni. Webová aplikace je plně funkční a uživatelsky přívětivá. Navíc její plná verze je k dispozici ve dvou jazycích, češtině a angličtině. Kapitola 5, která popisuje implementační část, je srozumitelně popsána, poskytuje smysluplný a čtivý popis všech použitých nástrojů a vysvětluje, proč byly vybrány právě tyto nástroje. Zvláště ocenitelný je detailní popis implementace jednotlivých algoritmů a navržených tříd a metod.

Teoretická část, i přestože stylisticky a jazykově mírně zaostává za praktickou částí, stále nabízí kvalitní popisy implementovaných algoritmů a zdůvodnění jejich výběru pro aplikaci. Zde by však mohl být prostor pro drobné vylepšení, zejména co se týče hlubší literární rešerše aktuálního použití algoritmů.

Celkové posouzení práce a zdůvodnění výsledné známky:

Práce navazuje na bakalářskou práci autora, ale obohacuje stávající řešení v mnoha směrech: vlastní implementace kryptografických algoritmů umožňuje jejich krokování, přehledná schémata usnadňují jejich pochopení a nová architektura výrazně zvyšuje úroveň aplikace. Projekt využívá technologie jako PHP 8.3, Laravel 9.19, GMP knihovnu, Sentry, PSalm, Docker a další. Text práce je ucelený a dobře strukturovaný. Testování prokázalo správnost algoritmů a uživatelskou přívětivost. Celkově lze práci hodnotit jako velmi kvalitní. Aplikace bude využita jako doplňkový studijní materiál při výuce kryptografie na FIM UHK.

Otázky k obhajobě:

Jaké další kryptografické algoritmy by bylo vhodné implementovat do webové aplikace? Jaké již implementované třídy nebo metody by bylo možné využít pro implementaci dalších algoritmů do aplikace?

Práci doporučuji k obhajobě.

Navržená výsledná známka: A

V Hradci Králové**, dne 14. května 2024**

podpis