



POSUDEK OPONENTA BAKALÁŘSKÉ PRÁCE

Jméno studenta: Zdeněk Hejzlar

Název práce: Zabezpečení TLS

Autor posudku: Mgr. Josef Horálek, Ph.D.

Cíl práce: Cílem bakalářské práce je analýza aktuálně využívaných kryptografických algoritmů s následnou komparací, návrhem a vytvořením výukové aplikace pro výuku kryptografie.

Povinná kritéria hodnocení práce	Stupeň hodnocení (známka)					
	A	B	C	D	E	F
Práce svým zaměřením odpovídá studovanému oboru	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Vymezení cíle a jeho naplnění	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Zpracování teoretických aspektů tématu	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Zpracování praktických aspektů tématu	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Adekvátnost použitých metod, způsob jejich použití	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Hloubka a správnost provedené analýzy	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Práce s literaturou	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Logická stavba a členění práce	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Jazyková a terminologická úroveň	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Formální úprava a náležitosti práce	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Vlastní přínos studenta	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Využitelnost výsledků práce v teorii (v praxi)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Vyjádření k výsledku anti-plagiátorské kontroly

Anti-plagiátorská kontrola eVSKP identifikovala celkovou podobnost: 0 %.

Dílčí připomínky a náměty:

Autor v práci nedostatečně popisuje principy fungování kryptografických algoritmů, které jsou aplikovány v praktické části práce a je tedy nedostatečně zpracována analytický část práce. Webová aplikace je sice plně funkční, ale chybí detailnější popis jednotlivých algoritmů, což snižuje využitelnost vytvořeného výstupu. Jako slabou lze také označit práci se zdroji, kde autor v celé práci uvádí pouze devět zdrojů, což je pro řešenou oblast nedostatečné.

Celkové posouzení práce a zdůvodnění výsledné známky:

Předložená práce je rozdělena do sedmi kapitol včetně úvodu a závěru. Samotná teoretická část, která obsahuje analýzu a popis kryptografických algoritmů je v kapitole třetí. Jak již bylo popsáno výše, autor zde zůstává na povrchu dané problematiky a text neobsahuje odpovídající popis principů jednotlivých algoritmů, ani není uveden základní matematický aparát v oblasti výpočtu šifer, jejich náročnosti a odolnosti vůči útokům hrubou silou.

Kapitola čtvrtá pak obsahuje obecný popis vytvořené aplikace, která je plně funkční, avšak chybí základní UML diagram, popis služeb apod. Celkový rozsah práce je pak na spodní hranici akceptovatelnosti, což plyne z výše uvedených nedostatků. Přes výše uvedené nedostatky však práce, hlavně její praktická část, má vysoký potenciál využitelnosti jako jeden z možných podpůrných

nástrojů ve výuce. Po doplnění popisu principů a ukázek kódu jednotlivých kryptografických algoritmů, je práce plně využitelná. Právě z tohoto důvodu práci doporučuji k obhajobě.

Otázky k obhajobě:

Představte principy blokových a proudových šifer.

Představte kód, který řeší Vigenèrovu šifru.

Představte logické blokové schéma pro šifrování DES, AES a RSA.

Popište principy veřejného a privátního klíče a jeho využití v moderní kryptografii.

Práci doporučuji k obhajobě.

Navržená výsledná známka: C

V Hradci Králové, dne 16. května 2022

podpis