



POSUDEK VEDOUCÍHO BAKALÁŘSKÉ PRÁCE

Jméno studenta: Zdeněk Hejzlar

Název práce: Zabezpečení TLS

Autor posudku: Ing. Hana Švecová

Cíl práce: Cílem bakalářské práce byla 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 checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Zpracování teoretických aspektů tématu	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Zpracování praktických aspektů tématu	<input checked="" type="checkbox"/>	<input 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 checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Práce s literaturou	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input 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 type="checkbox"/>	<input checked="" 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 checked="" type="checkbox"/>	<input 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 checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Vyjádření k výsledku anti-plagiátorské kontroly

Anti plagiátorská kontrola eVSKP identifikovala celkovou podobnost: 5 %.

Dílicí připomínky a náměty:

Kvalifikační práce je zpracována v rozsahu 36 stran. Teoretická část je rozpracována na 10 stranách, praktická část je rozpracována cca na 12 stranách. Cílem kvalifikační práce byl návrh a vytvoření výukové aplikace pro výuku kryptografie. Vytvořená aplikace je velmi hezky zpracována včetně anglické verze, avšak celkový rozsah celé kvalifikační práce by mohl být více rozpracován v obou dvou částech (teoretické a praktické).

Celkové posouzení práce a zdůvodnění výsledné známky:

Kvalifikační práce je zaměřena na analýzu aktuálně využívaných kryptografických algoritmů včetně komparace s cílem navrhnout a vytvořit výukovou aplikaci pro výuku kryptografie na Fakultě informatiky a managementu Univerzity Hradec Králové.

Autor práci rozdělil do dvou částí, do části teoretické a do části praktické. V teoretické části je zpracován úvod do kryptografie – základní rozdělení kryptografie, druhy šifrovacích systémů, a dále jsou charakterizovány dílčí typy šifer.

V praktické části je představena výuková aplikace, která je dobře zpracována. URL pro výukovou aplikaci je <https://edu.uhk.cz/~hejzlzd1/>

Autor při zpracovávání své bakalářské práce vše aktivně konzultoval, a obratem zapracovával připomínky ze strany vedoucího práce.

Práce splňuje požadavky kladené na bakalářskou práci a práci doporučuji k obhajobě.

Otázky k obhajobě:

- 1) Charakterizujte Kryptoanalýzu.
- 2) Vysvětlete principy zabezpečení TLS.

Práci doporučuji k obhajobě.

Navržená výsledná známka: B

V Hradci Králové, dne 16. května 2022

podpis