Univerzita Hradec Králové
Fakulta informatiky a managementu

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	☒	☐	☐	☐	☐	☐
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

Anti plagiátorská kontrola eVSKP identifikovala celkovou podobnost: 5 %.

Dílčí 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