Posudek oponenta diplomové práce

Student:	Bc, Jaromír SMOLA
Číslo studenta:	E140049
Název diplomové práce:	Archivace digitálních dokumentů v organizaci
Cíl práce:	Zmapovat současný stav procesu nakládání s digitálními dokumenty v organizaci.
Vedoucí práce:	doc. Ing. Stanislava Šimonová, Ph.D.,
Oponent práce:	prof. Ing. Jan Čapek, CSc.,

Náročnost tématu

	výborně	velmi dobře	vyhovující	nevyhovující	nelze hodnotit
Teoretické znalosti	☐	☒	☐	☐	☐
Vstupní údaje a jejich zpracování	☒	☐	☐	☐	☐
Použité metody	☐	☒	☐	☐	☐

Kritéria hodnocení práce

	výborně	velmi dobře	vyhovující	nevyhovující	nelze hodnotit
Stupeň splnění cíle práce	☒	☐	☐	☐	☐
Původnost zapracování tématu	☐	☒	☐	☐	☐
Adekvátnost použitých metod	☐	☒	☐	☐	☐
Hloubka provedené analýzy (ve vztahu k tématu)	☐	☒	☐	☐	☐
Logická stavba práce a rozsah	☒	☐	☐	☐	☐
Práce s českou a zahraniční literaturou včetně citací	☐	☒	☐	☐	☐
Formální úprava práce (text, grafy, tabulky)	☐	☐	☒	☐	☐
Jazyková úroveň (styl, gramatika, terminologie)	☒	☐	☐	☐	☐

Využitelnost výsledků práce

	vysoká	Střední	nízká	nelze hodnotit
Pro teorii	☐	☒	☐	☐
Pro praxi	☐	☒	☐	☐

Ostatní připomínky k práci

Nečitelné obrázky: 2, 13, 14, 19, 23 a 24.Text na str 23 neodpovídá obr č. 4 text je až příliš zjednodušený, pro čtenáře kteří neznají princip činnosti algoritmů RSA, resp. DSA těžko pochopitelný. Na str. 23 píšete: „*Vytvoření elektronického podpisu probíhá tak, že vezmeme elektronický dokument (v podstatě jedno velmi velké číslo) a místo jedinečného podpisu vezmeme soukromý klíč (tajné podepisovací číslo).“* V případě RSA číselná velikost zprávy (dokumentu) M nesmí překročit číslo m, pro které platí $0 \leq m \leq n-1$, kde $n=pq$. Tedy ne jedno velmi velké číslo Je-li dokument obsáhlý, zpravidla se dělí na bloky. Soukromým klíčem nic nepodepisujeme, dokument jen zašifrujeme.
V práci mě chybí alespoň zmínka o dalších algoritmech (EL Gamal, Eliptické křivky), Dále by práci prospěl příklad krátkého dokumentu, jak se mění od prvotního vytvoření do podoby vhodné pro uložení do archivu.
Str. 57 nahoře: „*Dokumenty, které je třeba nově pečetit, vznikají na různých aplikačních serverech ve vizualizovaném serverovém prostředí“* správně: Dokumenty, které je třeba nově pečetit, vznikají na různých aplikačních serverech ve virtualizovaném serverovém prostředí.

Otázky a náměty k obhajobě

Pokud se k podpisu používá DSA algoritmus, dochází k šifrování?

Závěrečné hodnocení

Práci **doporučuji** k obhajobě.
Tuto diplomovou práci navrhuji hodnotit známkou: **C - Velmi dobře**

V Pardubicích 6.1.2019

Podpis .....