Univerzita
Pardubice
Fakulta elektrotechniky
a informatiky

Posudek vedoucího bakalářské práce

Jméno studenta:	Tomáš MANDYS
Téma práce:	Elektronické průkazy totožnosti
Cíl práce:	Popis a charakteristika vybraných druhů elektronických průkazů totožnosti, použitých technologií a algoritmů. Rozbor vybraného algoritmu.

Náročnost zadání bakalářské práce na:

teoretické znalosti	střední
praktické zkušenosti	nižší
podkladové materiály (vstupní data) a jejich zpracování	střední

A: Slovní hodnocení:

Naplnění cíle práce:

Obsah práce je částečně v souladu se zadáním. Práce je zpracována přehledně. Po odborné stránce mám k práci tyto výhrady:

u symetrické a nesymetrické kryptografie je uvedeno málo příkladů šifer
slabý rozbor algoritmu RSA

Práce je v celé míře teoretická.

Úvodní kapitoly student věnoval hiostorii kryptografie. Další kapitoly se již zabývají elektronickými průkazy totožnosti - občanským pasem, cestovním pasem a elektronickým podpisem. V sedmé závěrečné kapitole pak autor provádí rozbor algoritmu RSA.

Autor práci vytvořil zcela sám, dané cíle téměř (slabá implementační část) splnil.

Logická stavba a stylistická úroveň práce:

V práci jsou dodrženy zásady DTP (kromě drobných chyb). Práce obsahuje všechny potřebné náležitosti a je v požadovaném rozsahu. Práce má dobrou grafickou úpravu.

Po jazykové a stylistické stránce nemám k práci téměř žádné připomínky.

Využití záměrů, námětů a návrhů v praxi:

Práci je možné v praxi využít jako základní text pro zájemce o kryptografii a o elektronické průkazy totožnosti v oblasti ochrany dat.

Případné další hodnocení (připomínky k práci):

Autor se nevyvaroval několika hrubých gramatických chyb.

B: Kriteriální hodnocení:

Nápovědu k vyplnění vybraného pole je možné zobrazit klávesou F1, stručně je uvedena i ve stavovém řádku.

Kriteria hodnocení práce:	Úroveň	Připomínky
Úroveň dokumentu		
logická stavba práce	průměrné	
stylistická úroveň	průměrné	
práce s literaturou včetně citací	průměrné	
formální úprava práce (text, grafy, tabulky)	průměrné	
Teoretická část		
rozsah a úroveň zpracování rešerše	průměrné	
formulace teoretických východisek pro praktickou část	průměrné	
odborné zvládnutí problematiky	průměrné	
Praktická část – produkt (řešení)		
adekvátnost použitých metod, SW, postupů	nelze hodnotit	pokus o teoretický rozbor algoritmu RSA
kvalita návrhu řešení	nelze hodnotit	
komplexnost řešení	částečná	
návrh datových struktur	nelze hodnotit	
uživatelské rozhraní	nelze hodnotit	
odborné zvládnutí problematiky	nelze hodnotit	
rozpracovanost	rozpracováno	
využitelnost praktické části v praxi	nevyužitelné	
Praktická část - popis		
popis řešení v bakalářské práci	nelze hodnotit	
ostatní přílohy (tabulky, grafy, výpočty, …)	nelze hodnotit	
uživatelská příručka	nelze hodnotit	
Uložení dokumentu/ů bakalářské práce na CD	ano	
Uložení výsledku praktické části na CD	ne	
Stupeň splnění cíle práce	částečně	

C: Otázky k obhajobě (max 2):

1. **Co je to problém faktorizace v RSA algoritmu?**
2. **Co je to SSL, využití?**

Doporučení práce k obhajobě: **ano**

Navržený klasifikační stupeň: **dobře**

Posudek vypracoval:

Jméno, tituly: Zdeněk Šilar, Ing.
Zaměstnavatel: Univerzita Pardubice, FEI

V Pardubicích dne: 31. 8. 2009 Podpis: