Univerzita
Pardubice
Fakulta elektrotechniky
a informatiky

Posudek vedoucího bakalářské práce

Jméno studenta:	Lukáš Marian
Téma práce:	Informační bezpečnost a kryptologie
Cíl práce:	Cílem práce je popsat kryptologii jako jednu z metod informační bezpečnosti. V teoretické části autor vyjde z prostudované odborné literatury a na základě získaných znalostí souhrně popíše požadavky na model konvenčního kryptosystému včetně charakteristiky tohoto systému. V práci bude mimo jiné podrobně popsán princip veřejného klíče a možnosti jeho použití. Dále budou popsány sysmetrické a asymetrické šifry a hashovací funkce a jejich vazby. Praktickým výstupem bakalářské práce budou laboratorní úlohy pro demonstraci využití vybranných kryptografických technik.

Náročnost zadání bakalářské práce na:

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

A: Slovní hodnocení:

Naplnění cíle práce:

Autor ve své práci představil kryptologie a její praktické použití . Představen je model konvenčního kryptosystému, jeho charakteristiku a základní metody šifrování. Popsány jsou principy symetrického a asymetrického šifrování, hašovacích funkcí, digitálního podpisu a proces hodnocení moderního kryptosystému. Nastíněny jsou základní možnosti kryptoanalytických útoků a možnosti obrany proti těmto útokům. Praktická část je rozdělena do dvou laboratorních úloh. První se věnuje programu PGP, který se používá pro šifrování emailové komunikace a je zde popsána a předvedena instalace a konfigurace na platformách Windows a Linux. V druhé laboratorní úloze je předvedena a popsána konfigurace autentizační metody CHAP na sériové lince mezi dvěma směrovači.

Logická stavba a stylistická úroveň práce:

Práce má celkově komplexní a dobře provázanou náplň. Na základě představených teoretických znalostí autor realizoval praktické úlohy.

Využití záměrů, námětů a návrhů v praxi:

Způsob zpracování bakalářské práce ověřil připravenost autora na propojení teoretických znalostí s praktickou realizací šifrovacích technik.

Případné další hodnocení (připomínky k práci):

Autor využil svých získaných znalostí a dovedností v rámci studia oboru Informačních technologií.
Pro zvládnutí tématu bakalářské práce bylo nutné rozšířit a doplnit si znalosti z oblasti praktické realizace šifrovacích metod..

Autor ve své práci pracoval s relevantními zdroji v rozsahu vhodném pro bakalářskou práci.

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	nelze hodnotit	
formulace teoretických východisek pro praktickou část	průměrné	
odborné zvládnutí problematiky	nadprůměrné	Studium kryptografie nad rámec počítavých sítí IPS1 - IPS4.
Praktická část – produkt (řešení)		
adekvátnost použitých metod, SW, postupů	nadprůměrné	
kvalita návrhu řešení	průměrné	
komplexnost řešení	komplexní	
návrh datových struktur	nelze hodnotit	
uživatelské rozhraní	nelze hodnotit	
odborné zvládnutí problematiky	nadprůměrné	
rozpracovanost	dokončeno	
využitelnost praktické části v praxi	ve větší míře	
Praktická část - popis		
popis řešení v bakalářské práci	nadprůměrné	
ostatní přílohy (tabulky, grafy, výpočty, …)	průměrné	
uživatelská příručka	nelze hodnotit	
Uložení dokumentu/ů bakalářské práce na CD	ano	
Uložení výsledku praktické části na CD	ano	
Stupeň splnění cíle práce	splněn	

C: Otázky k obhajobě (max 2):

1. **Jaké bezpečnostní cíle zajišťuje elektronický podpis?**
2. **Popište základní principy algoritmus MD5.**

Doporučení práce k obhajobě: **ano**

Navržený klasifikační stupeň: **výborně**

Posudek vypracoval:

Jméno, tituly: Soňa Neradová, Ing.
Zaměstnavatel: UPCE, FEI

V Pardubicích dne: 28. května 2012 Podpis: