Univerzita
Pardubice
Fakulta elektrotechniky
a informatiky

Posudek vedoucího bakalářské práce

Jméno studenta:	Michal Indra
Téma práce:	Šifrovací algoritmy
Cíl práce:	Cílem práce byl teoretický popis vybraných šifrovacích algoritmů, jejich praktická implementace a vytvoření praktických a ukázkových programů pro demonstraci vybraných šifrovacích metod.

Náročnost zadání bakalářské práce na:

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

A: Slovní hodnocení:

Naplnění cíle práce:

Hlavní cíle práce byly splněny. Pouze jeden dílčí cíl, požadující zhodnocení dostupných knihoven pro podporu šifrování, byl splněn pouze částečně.

V teoretické části práce se autor věnuje popisu základních pojmů a principů z oblasti kryptologie. Dále je uveden teoretický popis vybraných šifrovacích algoritmů a stručný popis využití šifrování ve vybraných komunikačních protokolech.

V praktické části autor implementoval vybrané šifrovací metody (Cesarova šifra, Mono-alfabetická substituční šifra s náhodnou transformací, Vernamova šifra, RC4 a RSA). Při implementaci RSA využil dostupné knihovny java.security a javax.crypto.

Implementované algoritmy použil ve vytvořené ukázkové aplikaci, demonstrující činnost jednotlivých metod šifrování. Rovněž vytvořil (k jednodušším metodám šifrování) ukázkovou aplikaci pro prolomení daných šifrovacích metod.

Logická stavba a stylistická úroveň práce:

Práce je správně rozčleněna do kapitol, které na sebe logicky navazují. Práce obsahuje všechny potřebné náležitosti. Stylistická úroveň textu je průměrná, čitelnost v některých částech je ztížena použitím příliš komplikovaných souvětí.

V textu práce se (v nezanedbatelné míře) vyskytují překlepy a gramatické chyby.

Práce je vytištěna oboustranně, což není pro tento typ práce zcela standardní. Při tomto typu tisku by měly hlavní kapitoly začínat vždy na pravé (liché) straně. Žádné z těchto pravidel není v práci dodrženo.

V teoretické části zcela chybí odkazy na literaturu, ze které autor dané informace čerpal.

Není vhodné současně v jednom textu používat pojmy Byte a bajt, navíc slovo Byte je často skloňováno ("zbylé byty").

V některých případech není mezi ukázkový zdrojový kód a následující text vložena žádná meziodstavcová mezera.

V některých kapitolách, které popisují implementaci, jsou identifikátory proměnných vkládány do uvozovek. Tento způsob není příliš vhodný. Navíc tento způsob zápisu není jednotný v celé práci a neodpovídá ani konvencím, uvedeným na straně 10.

V práci je použita jako jednotka času vteřina.

Využití záměrů, námětů a návrhů v praxi:

Teoretická část práce je využitelná jako úvodní studijní materiál z oblasti kryptologie. Praktická část byla od začátku koncipována jako ukázková implemntace, demonstrující principy fungování vybraných šifrovacích

algoritmů. Využití praktické části pro studium je částečně ztíženo nekomentovaným kódem a chybějící programátorskou dokumentací.

Případné další hodnocení (připomínky k práci):

Při podrobném studiu dané problematiky z různých zdrojů autor nalezl několik nesrovnalostí, týkajících se odlišného popisu některých šifrovacích metod v jednotlivých studovaných zdrojích. Na tyto rozpory upozornil v textové části práce.

V teoretické části jsou uvedeny některé nepřesnosti, např.: "Úprava otevřených dat na šifrovaná data se nazývá kódování." nebo "Privátní klíč mají k dispozici pouze komunikující, …". Rovněž je v textu (str. 23) uvedeno, že: "V českém jazyce je nejčetnějším znakem 'a'…", což je v rozporu s tabulkou 2 (str. 22).

V práci není uvedeno, zda se autor pokusil o vlastní implementaci RSA bez použití externích knihoven. Vzhledem k tomu, že se práce zabývá především ukázkovými implementacemi daných algoritmů, bylo by vhodné vytvořit i čistě vlastní implementaci. Výkonnostní srovnání těchto dvou rozdílných řešení by bylo jistě zajímavé.

V práci chybí podrobnější popis použitých hotových knihoven.

V práci chybí popis aplikace Záškodník.

V samotné aplikaci nefunguje přizpůsobení velikosti (výšky) textových polí velikosti formuláře tak, aby byla maximálně využita plocha formuláře.

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	podprůměrné	Bylo použito velké množství zdrojů, ale nejsou uvedeny odkazy v textu.
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	nadprůměrné	
Praktická část – produkt (řešení)		
adekvátnost použitých metod, SW, postupů	průměrné	
kvalita návrhu řešení	průměrné	
komplexnost řešení	komplexní	
návrh datových struktur	nelze hodnotit	
uživatelské rozhraní	průměrné	
odborné zvládnutí problematiky	průměrné	
rozpracovanost	dokončeno	V práci není zmíněno, jak byla aplikace testována.
využitelnost praktické části v praxi	částečná	
Praktická část - popis		
popis řešení v bakalářské práci	průměrné	
ostatní přílohy (tabulky, grafy, výpočty, …)	nelze hodnotit	
uživatelská příručka	podprůměrné	Uživatelská příručka je součástí textové části práce. Programátorská dokumentace chybí. Částečně je popis uveden v kapitole 5. Kód není komentován.
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. **Vysvětlete rozdíl mezi kódováním a šifrováním.**
2. **Existují nějaká další dostupná hotová řešení (knihovny), implementující moderní šifrovací algoritmy, která jsou vhodná pro programovací jazyk Java?**

Doporučení práce k obhajobě: **ano**

Navržený klasifikační stupeň: **velmi dobře**

Posudek vypracoval:

Jméno, tituly: Ing. Petr Veselý
Zaměstnavatel: KST, FEI, Univerzita Pardubice

V Pardubicích dne: 29. května 2014 Podpis: