FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Hodnocení vedoucího závěrečné práce

Student: Hana Svobodová
Vedoucí: práce: Ing. Josef Kokeš
Název práce: Algoritmy pro sdílení tajemství
Obor: Bezpečnost a informační technologie

Datum vytvoření: 19. 5. 2019

Hodnotící kritérium:	*Způsob hodnocení – následující škálou 1 až 4:*
1. Splnění zadání	***1=zadání splněno,*** *2=zadání splněno s menšími výhradami,* *3=zadání splněno s většími výhradami,* *4=zadání nesplněno*

Popis kritéria:
Posuďte, zda předložená ZP dostatečně a v souladu se zadáním obsahově vymezuje cíle, správně je formuluje a v dostatečné kvalitě naplňuje. V komentáři uveďte body zadání, které nebyly splněny, posuďte závažnost, dopady a případně i příčiny jednotlivých nedostatků. Pokud zadání svou náročností vybočuje ze standardů pro daný typ práce nebo student případně vypracoval ZP nad rámec zadání, popište, jak se to projevilo na požadované kvalitě splnění zadání a jakým způsobem toto ovlivnilo výsledné hodnocení.

Komentář:

Práce je zaměřena prakticky: cílem bylo nastudovat známé algoritmy pro sdílení tajemství a některé z nich naimplementovat v podobě vhodné pro praktické použití. Toto studentka splnila dle požadavků.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
2. Písemná část práce	*100 (A)*

Popis kritéria:
Zhodnoťte přiměřenost rozsahu předložené ZP vzhledem k obsahu, tj. zda všechny části ZP jsou informačně bohaté a ZP neobsahuje zbytečné části. Dále posuďte, zda předložená ZP je po věcné stránce v pořádku, případně vyskytují-li se v práci věcné chyby nebo nepřesnosti. Zhodnoťte dále logickou strukturu ZP, návaznosti jednotlivých kapitol a pochopitelnost textu pro čtenáře. Posuďte správnost používání formálních zápisů obsažených v práci. Posuďte typografickou a jazykovou stránku ZP, viz Směrnice děkana č. 26/2017, článek 3. Posuďte, zda student využil a správně citoval relevantní zdroje. Ověřte, zda jsou všechny převzaté prvky řádně odlišeny od vlastních výsledků, zda nedošlo k porušení citační etiky a zda jsou bibliografické citace úplné a v souladu s citačními zvyklostmi a normami. Zhodnoťte, zda převzatý software a jiná autorská díla, byly v ZP použity v souladu s licenčními podmínkami.

Komentář:

Textová část práce je perfektní. Postupuje systematicky od společných definic přes detailní vysvětlení jednotlivých algoritmů až po stručný popis implementace a vyhodnocení dosažených výsledků. Zahrnuje matematický aparát nutný pro pochopení témat i analýzu bezpečnostních aspektů jednotlivých algoritmů, včetně obrany proti možným útokům ze strany nepoctivého držitele části tajemství nebo i nepoctivého tvůrce dílů. Výjimečná je jazyková stránka práce - v textu jsem si nevšiml jediné chyby.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
3. Nepísemná část, přílohy	*95 (A)*

Popis kritéria:
Dle charakteru práce se případně vyjádřete k nepísemné části ZP. Například: SW dílo – kvalita vytvořeného programu a vhodnost a přiměřenost technologií, které byly využité od vývoje až po nasazení. HW – funkční vzorek – použité technologie a nástroje, Výzkumná a experimentální práce
– opakovatelnost experimentů

Komentář:

Program, který studentka vypracovala, řeší požadovanou problematiku - zašifruje vstupní soubor náhodně vygenerovaným klíčem a tento klíč pomocí zvoleného algoritmu rozdělí na části pro jednotlivé účastníky sdílecího schématu. Program je přehledně a čistě napsaný, vhodně komentovaný a řeší i praktické situace jako mazání citlivých dat poté, co už nejsou potřeba. K dokonalosti chybí volitelné ověření integrity jednotlivých dílů/detekce podvodníka (nebylo požadováno) a odstranění veřejného souboru (všechny údaje z něj mohly být umístěny v souboru se zašifrovanými daty).

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
4. Hodnocení výsledků, jejich využitelnost	*95 (A)*

Popis kritéria:
Dle charakteru práce zhodnoťte možnosti nasazení výsledků práce v praxi nebo uveďte, zda výsledky ZP rozšiřují již publikované známé výsledky nebo přinášející zcela nové poznatky.

Komentář:

Výstupem je program, který dovoluje uživateli zašifrovat tajný soubor náhodným klíčem, tento klíč rozdělit na zadaný počet dílů a předat účastníkům schématu tak, aby předem určený počet z nich mohl rekonstruovat klíč a dešifrovat soubor. Tento program je funkční, snadno použitelný, do značné míry platformově nezávislý (musí být zachován endián procesoru) a uvolněný pod GPL-like licencí.

Hodnotící kritérium:	*Způsob hodnocení – následující škálou 1 až 5:*
5. Aktivita a samostatnost studenta	5a: *1=výborná aktivita,* *2=velmi dobrá aktivita,* ***3=průměrná aktivita,*** *4=slabší, ale ještě dostatečná aktivita,* *5=nedostatečná aktivita* 5b: *1=výborná samostatnost,* *2=velmi dobrá samostatnost,* ***3=průměrná samostatnost,*** *4=slabší, ale ještě dostatečná samostatnost,* *5=nedostatečná samostatnost*

Popis kritéria:
V souvislosti s průběhem a výsledkem práce posuďte, zda byl student během řešení aktivní, zda dodržoval dohodnuté termíny, jestli své řešení průběžně konzultoval a zda byl na konzultace dostatečně připraven (5a). Posuďte schopnost studenta samostatné tvůrčí práce (5b).

Komentář:

Počátky spolupráce byly složitější, ale jakmile se studentka zabrala do tématu a začala zpracovávat jednotlivé algoritmy, získala potřebnou sebedůvěru a následně už pracovala samostatně a zodpovědně.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
6. Celkové hodnocení	*95 (A)*

Popis kritéria:
Shrňte stránky ZP, které nejvíce ovlivnily Vaše celkové hodnocení. Celkové hodnocení nemusí být aritmetickým průměrem či jinou hodnotou vypočtenou z hodnocení v předchozích jednotlivých kritériích. Obecně platí, že bezvadně splněné zadání je hodnoceno klasifikačním stupněm A.

Text hodnocení:

Práce srozumitelně provádí čtenáře problematikou algoritmů pro sdílení tajemství. Je velmi důkladně napsaná, počínaje teoretickými východisky a bezchybným jazykem konče. Součástí je i pěkně napsaný program, který zpřístupňuje vybrané algoritmy uživateli, a to ve snadno použitelné formě a pod přívětivou licencí. Práce tak plní všechno, co se od ní dalo očekávat, a demonstruje, že studentka zvládla teorii i praxi vysokoškolské práce. Práci doporučuji k obhajobě a hodnotím známkou A-výborně.

Podpis vedoucího práce: