FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Posudek oponenta závěrečné práce

Student:	Hana Svobodová
Oponent práce:	Ing. Tomáš Zahradnický, Ph.D.
Název práce:	Algoritmy pro sdílení tajemství
Obor:	Bezpečnost a informační technologie

Datum vytvoření: 9. 6. 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:
Studentka měla za úkol provést rešerši známých algoritmů pro sdílení tajemství, analyzovat jejich bezpečnost, a implementovat alespoň dva z nich v jazyce C s využitím knihovny OpenSSL. V práci mohly být uvedeny ještě algoritmy visuálního sdílení tajemství [1] anebo Rabinův algoritmus disperze informace [2]. Vzhledem k tomu, že jde o bakalářskou práci a v práci tři uváděné algoritmy patří k nejvíce používaným, považuji zadání za splněné.

[1] Rosulek M: The Joy of Cryptography. https://web.engr.oregonstate.edu/ rosulekm/crypto/crypto.pdf. 2019.
[2] Shiyuan Wang, Divyakant Agrawal, a Amr El Abbadi: A Comprehensive Framework for Secure QueryProcessing on Relational Data in The Cloud. https://www.cs.ucsb.edu/sites/default/files/docs/reports/2010-25.pdf. 2010.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
2. Písemná část práce	*95 (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:
Logická stránka práce je výborná. Práce je dobře členěna. Implementace je oddělena od popisu algoritmů. Algoritmy jsou popsány dobře, snad jen chybí ukázkový běh každého z nich.

Jazyková stránka věci je výborná. Nacházím jen chybu v psaní 256-bitový, k-tic, ... namísto 256bitový, ktic, ...

Typografická stránka práce je výborná.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
3. Nepísemná část, přílohy	*100 (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:
Přiložené médium DVD obsahuje zdrojové kódy práce a programů. Programy jsou funkční.

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

4. Hodnocení výsledků, jejich využitelnost	*90 (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:

Implementované algoritmy jsou funkční a je možné je použít.

Osobně bych ocenil, kdyby byla práce navržena a implementována jako součást knihovny OpenSSL, jako aplikace OpenSSL spustitelná přímo pomocí "openssl název_aplikace". Pokud bude studentka pokračovat v magisterském studiu, mohla by pokračovat a tuto věc zrealizovat. Práce by pak provedla zobecnění struktur pro libovolné, dosud neimplementované algoritmy sdílení tajemství, sjednocení názvů struktur a funkcí tak, aby dobře zapadly do ekosystému OpenSSL, ukládání dat ve formátu ASN.1 a kompatibilita s ostatními algoritmy v OpenSSL by mohly vytvořit skvělou diplomovou práci. Navíc by mohl být učiněn požadavek na začlenění do knihovny OpenSSL, čímž by význam práce násobně vzrostl, za předpokladu, že by byla psána v anglickém jazyce.

Hodnotící kritérium:	*Způsob hodnocení – nehodnotí se*

5. Otázky k obhajobě

Popis kritéria:
Uveďte případné dotazy, které by měl student zodpovědět při obhajobě ZP před komisí (body oddělte odrážkami).

Otázky:

1. Plánuje studentka pokračovat na své práci a pokusit se o začlenění své práce do OpenSSL?

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:

Bakalářskou práci Hany Svobodové doporučuji k obhajobě a hodnotím ji známkou A (výborně).

Podpis oponenta práce: