FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Hodnocení vedoucího závěrečné práce

Vedoucí práce:	doc. RNDr. Dušan Knop, Ph.D.
Student:	Jakub Tetera
Název práce:	Ověřitelnost implementace algoritmu RSA
Obor / specializace:	Bezpečnost a informační technologie
Vytvořeno dne:	14. května 2023

Hodnotící kritéria

1. Splnění zadání

- ▸ [1] **zadání splněno**
  [2] zadání splněno s menšími výhradami
  [3] zadání splněno s většími výhradami
  [4] zadání nesplněno

Z mého pohledu se jednalo o náročnější téma. Osobně se v tématu ověřitelnosti programů snažím držet jednodušších témat. RSA jako takové bylo pokusné a od začátku jsem čekal, že bude nutné dělat mnoho ústupků. K mému překvapení jich nakonec bylo potřeba daleko méně, než by se dalo čekat.

2. Písemná část práce 98 /100 (A)

Celá práce je psaná je psaná kvalitní a čtivou angličtinou. Pan kolega do práce investoval hodně času a na práci samotné je to vidět. Obsahu značné množství citované literatury, poskytuje dostatečný přehled tematiky ověřování programů a velmi dobře dokumentuje všechna rozhodnutí, která byla učiněna takříkajíc "jako cena za ověřitelnost". Celkově se jedná o velmi zdařilou práci, která si zaslouží výborné hodnocení. Za vyzdvihnutí stojí i to, že student sám a aktivně vyhledával ve výsedku použité zdroje a i fakt, že práce nad očekávání obsahuje i důkazy některých vlastností použitých algoritmů -- tímto se zaručuje, že v kódu předpokládané vlastnosti opravdu platí.

3. Nepísemná část, přílohy 100 /100 (A)

Čitelný, přehledný a velmi dobře komentovaný kód. Velmi dobře zvolené části méně intuitivních důkazů korektnosti jsou dobře popsány v doprovodné práci.

4. Hodnocení výsledků, jejich využitelnost 90 /100 (A)

Práce byla od počátku zamýšlena jako proof-of-concept a jako taková je velice zdařilá. Na opravdové nasazení by bylo třeba (jak student v práci komentuje) práci spojit i s ověřenou rozšířenou aritmetikou. Tím by zajisté bylo nutné i přepsat nějaké důkazy na mírně obecnější, ale toto všechno bylo očekáváno již v počátcích.

5. Aktivita studenta

- [1] **výborná aktivita**
- [2] velmi dobrá aktivita
- [3] průměrná aktivita
- [4] slabší, ale ještě dostatečná aktivita
- [5] nedostatečná aktivita

Student vždy docházel na sjednané schůzky připraven a vybaven dobrými dotazy. Odvedl opravdu velký a kvalitní kus práce!

6. Samostatnost studenta

- [1] **výborná samostatnost**
- [2] velmi dobrá samostatnost
- [3] průměrná samostatnost
- [4] slabší, ale ještě dostatečná samostatnost
- [5] nedostatečná samostatnost

Student sám pracoval a aktivně vyhledával nové a nové zdroje inspirace. Z mé strany nezbývá než vyjádřit naprostou spokojenost.

Celkové hodnocení 99 /100 (A)

Vysoce kvalitní práce provedená na tématu, které bylo od začátku vnímáno jako velká výzva. Práce kvalitní, poctivá a dobře čitelná. Kód přehledný, více než dostatečně komentovaný a navíc důkaz korektnosti celého kódu. Práci mohu s klidem doporučit k obhájení a nejen to -- dovolil bych si požádat komisi o zvážení navržení práce na cenu děkana.

Instrukce

Splnění zadání

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.

Písemná část práce

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. 52/2021, 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.

Nepísemná část, přílohy

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.

Hodnocení výsledků, jejich využitelnost

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.

Aktivita studenta

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.

Samostatnost studenta

V souvislosti s průběhem a výsledkem práce posuďte schopnost studenta samostatné tvůrčí práce.

Celkové hodnocení

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.