FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Posudek oponenta závěrečné práce

Oponent práce:	Ing. Jiří Smítka
Student:	Jakub Tetera
Název práce:	Ověřitelnost implementace algoritmu RSA
Obor / specializace:	Bezpečnost a informační technologie
Vytvořeno dne:	11. června 2023

Hodnotící kritéria

1. Splnění zadání

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

2. Písemná část práce 100 / 100 (A)

Předložená práce je informačně velmi bohatá a kvalitně zpracovaná. Po věcné stránce je v pořádku. K logické struktuře práce nemám výhrady. Text je čtivý a pro čtenáře dobře pochopitelný. U čtenáře se předpokládá alespoň povrchní znalost matematického pozadí RSA, což neznamená, že by měla být práce nějak rozšířena. Již nyní je rozsah práce nadstandardní. Domnívám se, že autor práce dobře zvážil, jaké části má v práci rozebrat více a jaké méně či vůbec.

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

Implementované kódy jsou přeložitelné, spustitelné a chováním odpovídají popisu v textu práce. Potěšilo mne, že autor umožnil spuštění testů pod Windows i pod Linuxem.

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

Práci shledávám jako přínosnou. Téma je velmi dobře zpracováno a dovoluje čtenáři na tuto práci navázat a pokračovat.

Celkové hodnocení

100 /100 (A)

Autor splnil zadání beze zbytku. Text je psán systematicky a je zřejmé, že autor ví, o čem píše. Autor prostudoval mnoho zdrojů a v textu se na tyto zdroje odkazuje. Při psaní textu přitom důsledně dbá na formální stránku. Práci vnímám jako kvalitativně nadstandardní.

Otázky k obhajobě

U implementace RSA jsou (dle požadavku v zadání práce) omezeny některé parametry (např. prvočísla mají max. 32 bitů). Jakým způsobem by se jaká část práce změnila, pokud bychom tato omezení změnili - např. definovali velikost prvočísla např. na 1024 bitů? Jak by se tato změna projevila?

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.

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.