FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Posudek oponenta závěrečné práce

Oponent práce:	RNDr. Jiřina Scholtzová, Ph.D.
Student:	Marek Holík
Název práce:	Těžké matematické problémy v kryptografii
Obor / specializace:	Bezpečnost a informační technologie
Vytvořeno dne:	3. června 2022

Hodnotící kritéria

1. Splnění zadání

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

Práce představuje až vyčerpávající přehled různých šifrovacích protokolů (celkem 39) založených na třech základních matematických problémech: prvočíselné faktorizace čísel, kvadratických reziduích a diskrétního logaritmu. Nepísemná část obsahuje přehled různých metod a jejich úspěšnost při prolomení daného principu, které student testoval na různých matematických programech.
Zadání bylo splněno.

2. Písemná část práce 92 / 100 (A)

Písemná část závěrečné práce je nestandardně dlouhého obsahu (přes 50 stran samotného textu), což způsobil dlouhý výčet různých protokolů. Z pohledu čtenáře bych raději viděla menší počet a více do detailu popsaných ve smyslu mechanismu fungování daného protokolu. Nyní plných 21 stránek práce z 53 zaujímá pouhý výčet algoritmů. Ty jsou ovšem velmi pěkně a jednotným stylem sepsané. Množství citací a jejich použití je v pořádku.
Práce je dobře strukturovaná, čte se příjemně, splňuje všechny náležitosti po logické, jazykové i typografické stránce. Jediné, co mne překvapilo je úvodní kapitola Notation, kde student shrnul použité matematické pojmy. Tuto kapitolu bývá zvykem více rozvést, včetně značení dalších pojmů, je-li kapitolou první, nebo naopak ji dát jako přílohu na závěr, je-li pojata tak, jak ji student sepsal. V této části mi pak chyběla zavedená matematická značení (Z_n, Z_n^*, neškodilo by také zavést N kvůli nejednoznačnosti z nulou, která v kryptografii může být problém a mám pocit, že se tato nejednoznačnost objevuje i v textu díky citacím z různých zdrojů) a snad ještě více některé kryptografické pojmy jako sémantická bezpečnost a kryptografická bezpečnost. Na tyto pojmy je v

pozdějších kapitolách často odkazováno, ale nejsou zavedeny. Podobně pojem kvadratická rezidua modulo n - je pouze zavedeno značení, nikoliv definice tohoto pojmu. Také bývá zvykem na konci každé kapitoly uvést pár vět jako krátký souhrn, protože ukončení kapitoly výčtem (algoritmů, metod, nastavení...) trochu kazí celkový dojem při čtení.
Co se kvality obsahu týče, po jazykové stránce je práce velmi dobrá, až na pár v angličtině nezvyklých obratů, které autor často používá (např. slovíčko "basing", které se snad v angličtině ani nevyskytuje a mělo by být nahrazeno spíše frází "based on"). Dále bývá zvykem v anglických textech psát v nadpisech všechna první písmena velká.

Všechny výše uvedené nedostatky považuji za drobné prohřešky, které snižují čitelnost a kvalitu odevzdané práce jen minimálně.

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

Student experimentoval s řešením tří výše zmíněných matematických problémů na matematických systémech Magma, SageMAth a Matlab, které mají implementované algoritmy pro řešení těchto problémů. Testoval a porovnával nastavení a úspěšnost těchto algoritmů. Výsledky jsou přehledně shrnuty v písemné části Measurements.
Kódy, nastavení a výsledky uloženy na médiu jsou přehledné.

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

Práce nebude mít dle mého názoru významné nasazení v praxi. Byla postavena jako přehledové seznámení se s různými metodami a otestování jejich síly na různých matematických systémech.

Celkové hodnocení 100 /100 (A)

Práce je velmi kvalitně zpracovaným dlouhým přehledem různých šifrovacích protokolů založených na třech základních matematických problémech: prvočíselné faktorizace čísel, kvadratických reziduích a diskrétního logaritmu.
Text práce je kvalitně a pečlivě sepsaný, obsahuje jen několik drobných nedostatků zmíněných výše, které nijak neovlivňují čitelnost ani srozumitelnost textu.
Zadání bylo splněno a doporučuji k obhajobě se známkou A (výborně).

Otázky k obhajobě

Mé otázky se týkají experimentální části týkající se kvadratických reziduí:
Nešlo by využít kombinaci faktorizace čísla n a poté řešit problém reziduí při znalosti této faktorizace?

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.