FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Hodnocení vedoucího závěrečné práce

Vedoucí práce:	Mgr. Martin Jureček, Ph.D.
Student:	Marek Holík
Název práce:	Těžké matematické problémy v kryptografii
Obor / specializace:	Bezpečnost a informační technologie
Vytvořeno dne:	12. května 2022

Hodnotící kritéria

1. Splnění zadání

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

Všetky body zo zadania práce považujem za splnené. Implementačná časť pre problém kvadratického rezidua je oproti implementačnej časti pre problémy faktorizácie čísel a diskrétneho logaritmu výrazne menšia. To je z toho dôvodu, že nie sú známe efektívne algoritmy na riešenie tohto problému, ktoré nepotrebujú faktorizáciu modulu.

2. Písemná část práce 95 /100 (A)

Práca je dobre členená a obsahuje množstvo protokolov a šifier, ktoré sú prehľadne spracované v podobe pseudokódu. Uvedené zdroje sú relevantné k práci študenta a myslím si, že na niektorých miestach práce ani nemuseli byť uvedené (typicky u známych definícií). K jednotlivým protokolom a šifrám by sa hodilo uviesť viac poznámok, avšak aj bez nich je rozsah práce na hornej hranici počtu doporučených strán.

3. Nepísemná část, přílohy 96 /100 (A)

V experimentálnej časti boli využité nástroje Matlab, Magma a SageMath a taktiež na generovanie náhodných prvočísel sa použila knižnica OpenSSL. U niektorých algoritmov sa použili dopredu nastavené hodnoty, avšak nájdenie optimálnych parametrov by bolo nad rámec práce. Všetky nástroje sú relevantné a experimenty je možné zopakovať a overiť výsledky.

4. Hodnocení výsledků, jejich využitelnost 95 /100 (A)

Predložená práca môže slúžiť ako zdroj informácií, ktorý pre tri vybrané matematické problémy obsahuje pomerne dlhý zoznam šifier a protokolov, ktorých bezpečnosť je založená na jednotlivých problémoch. Čitateľ navyše nájde porovnanie jednotlivých algoritmov a nástrojov vhodných k riešeniu daných problémov.

5. Aktivita studenta

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

Študent pravidelne konzultoval s vedúcim práce najnovšie výsledky a ďalšie kroky počas celého obdobia práce.

6. Samostatnost studenta

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

Študent si samostatne vyhľadal jednotlivé protokoly a šifry pre každý z uvedených troch problémov a taktiež si sám vybral nástroje, ktoré použil v experimentálnej časti. S textom práce bolo treba pomôcť, ale šlo hlavne o drobnosti.

Celkové hodnocení 96 /100 (A)

Predložená práca pre tri matematické problémy obsahuje široký zoznam šifier a protokolov a nástrojov k ich riešeniu. Niektoré články neuvádzajú popis šifier a protokolov v pseudokóde a tak študent musel daný algoritmus pochopiť a spracovať. Implementačná časť je pomerne široká a spracovaná až v do 36 tabuľkách. V texte práce je uvedená diskusia o výsledkoch. Vzhľadom k vyššie uvedeným bodom hodnotím prácu známkou A.

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.