FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Posudek oponenta závěrečné práce

Student:	Bc. Martin Holec
Oponent práce:	Mgr. Martin Jureček
Název práce:	Babystep-Giantstep Algorithm and Solution of Elliptic Curve Discrete Logarithm Problem
Obor:	Počítačová bezpečnost

Datum vytvoření: 28. 1. 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:
Zadanie práce považujem za splnené s výhradou ku kvalite textu, ktorý obsahuje množstvo chýb. Vo väčšine prípadov však ide o preklepy.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
2. Písemná část práce	*20 (F)*

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:
Druhá až štvrtá kapitola obsahujú pomerne veľa chýb a niektoré časti textu sú doslova prevzaté. Taktiež text neobsahuje žiadne príklady. Z týchto dôvodov nemôžem posúdiť, či študent rozumie svôjmu textu v plnom rozsahu.

Podrobnejšie:
- študent poskladal niektoré definície a tvrdenia z viacerých zdrojov a nezjednotil notáciu (napr. Kap. 2.5)
- práca obsahuje niekoľko pojmov a premenných, ktoré nie sú v texte definované (od strany 3)
- pseudokódy algoritmov sú vágne napísané, nie sú uvedené vstupy ani výstupy a obsahujú niekoľko chýb (napr. Alg. 3)
- text obsahuje množstvo preklepov a chýb (viac ako 40)

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
3. Nepísemná část, přílohy	*90 (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:
Implementácia algoritmov bola vykonaná v jazyku Julia a otestovaná v SageLab. Experimentálne výsledky je možné overiť. Použité technológie sú adekvátne.

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:

Výsledkom práce je súbor doporučení (reprezentácia eliptickej krivky, kofaktor, varianta baby-step giant-step algoritmu), vďaka ktorým je možné urýchliť výpočet diskrétneho logaritmu.

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) str. 28: prečo prvok "b" definovaný ako a^q mod p je štvorcom v grupe G?

2) str. 30: prečo platí vzťah (5.8)?

3) Aká je definícia PDL pre grupu bodov na EC?

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
6. Celkové hodnocení	*50 (E)*

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:

Študentovi viac vyhovuje implementovanie kódu ako písanie odborného textu. Škoda, že študent odovzdal prácu už v lete a neinvestoval viac energie do textu. Inak by to bola pekná diplomová práca.
Celkové hodnotenie študenta je na hranici obhájiteľnosti. Na obhajobe by mal študent preukázať, že rozumie danej problematike.

Podpis oponenta práce: