FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Hodnocení vedoucího závěrečné práce

Student:	Jiří Soukup
Vedoucí: práce:	Ing. Ivo Petr, Ph.D.
Název práce:	Kryptograficky slabé eliptické křivky a specializované útoky na ECDLP
Obor:	Bezpečnost a informační technologie

Datum vytvoření: 6. 6. 2020

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:

Cílem práce bylo objasnit konkrétní metodu řešení problému diskrétního logaritmu (DLP) na speciální třídě eliptických křivek. Hlavní část práce byla tedy rešeršní. Student nastudoval poměrně komplikované partie obecné algebry a kryptografie eliptických křivek a sepsal ucelený text, který objasňuje všechny části řešení problému. Dále student implementoval celou proceduru v prostředí SAGE a porovnal efektivitu algoritmu s efektivitou dvou běžně používaných algoritmů. Ačkoliv implementace algoritmu byla jednodušší, celé zadání považuji spíše za složitější vzhledem k náročnosti rešerše. Obě části zadání považuji za nadstandardně splněné.

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

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:

Hlavní přínos práce je text objasňující princip Smartova útoku. Ačkoliv je celý algoritmus znám, vzhledem k tomu že využívá pokročilé partie teorie čísel a kryptografie eliptických křivek, obvykle se v literatuře objevují jen jeho fragmenty. Studentovi se v předložené práci povedlo utříbit všechny klíčové poznatky, logicky je sestavit a demonstrovat na jednoduchých příkladech. Práce tak může sloužit jako velmi kvalitní studijní text. Text je po všech stránkách na velmi vysoké úrovni.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
3. Nepísemná část, přílohy	*100 (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:

Po stránce implementace byla práce spíše jednodušší, nicméně i zde student odvedl velmi kvalitní práci. Dokázal identifikovat chybu ve známé implementaci (zdvih křivky do p-adických čisel) a zobecněním algoritmu chybu odstranit. Výsledkem je funkční a srozumitelný kód.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
4. Hodnocení výsledků, jejich využitelnost	*100 (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:

Smartův útok, o kterém práce pojednává, je v kryptografické komunitě všeobecně znám a práce tedy podle očekávání spíše potvrzuje známé výsledky. Vzhledem ke kvalitě textové části práce zaslouží doporučení jako studijní text pro zájemce o kryptografii eliptických křivek.

Hodnotící kritérium:	*Způsob hodnocení – následující škálou 1 až 5:*
5. Aktivita a samostatnost studenta	5a: ***1=výborná aktivita,*** *2=velmi dobrá aktivita,* *3=průměrná aktivita,* *4=slabší, ale ještě dostatečná aktivita,* *5=nedostatečná aktivita* 5b: ***1=výborná samostatnost,*** *2=velmi dobrá samostatnost,* *3=průměrná samostatnost,* *4=slabší, ale ještě dostatečná samostatnost,* *5=nedostatečná samostatnost*

Popis kritéria:
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 (5a). Posuďte schopnost studenta samostatné tvůrčí práce (5b).

Komentář:

Student postupoval velmi samostatně a pravidelně podával zprávy o své činnosti. K problémům v řešení přistupoval proaktivně. Samostatná tvůrčí činnost studentovi nečiní potíže.

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

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:

Student dokázal nastudovat obtížné partie matematiky, vybrat klíčové koncepty a vztahy mezi nimi a sepsat ucelený text objasňující Smartův útok na anomálních eliptických křivkách. Práci lze doporučit jako studijní text, který je obohacen názornými příklady, ukázkovou implementací a porovnáním s dalšími algoritmy. Práce je velmi kvalitní, doporučuji ji k obhajobě a hodnotím stupněm A.

Podpis vedoucího práce: