FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Hodnocení vedoucího závěrečné práce

Student:	Martin Andrýsek
Vedoucí: práce:	Ing. Jiří Buček
Název práce:	Timing Attack on the RSA Cipher
Obor:	Informační technologie

Datum vytvoření: 13. 6. 2018

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:

Student splnil zadání tím, že naprogramoval časový útok na šifru RSA s Montgomeryho násobením publikovaný v odkazu [3]. Studentova implementace nefunguje tak, jak by měla a jak předpokládá použitá publikace, tedy útok neodhalí všechny bity klíče. To samo o sobě nemusí být na závadu, pokud je popsáno dostatečně podrobně, jakých výsledků je tedy dosaženo, a v tom práce poněkud selhává.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
2. Písemná část práce	*50 (E)*

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:

Písemná část práce je poměrně slabá. Vysvětlení principu útoku je velice stručné, stejně jako popis realizace a výsledky experimentů. Vzhledem k tomu, že se útok nepodařilo spolehlivě zprovoznit, citelně chybí podrobnější popis výsledků. Student měl zpracovat konkrétní data ze sérií experimentů, které provedl, a prezentovat naměřené časy např. ve formě histogramů, spočítat střední hodnotu a rozptyl apod.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
3. Nepísemná část, přílohy	*75 (C)*

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:

Student naprogramoval šifru RSA v jazyce Python, a následně pak provedl novou implementaci některých algoritmů (zejména Montgomeryho násobení) v jazyce C pomocí knihovny BIGNUM. Tím se pokusil zajistit nižší rozptyl časů pro tyto operace, než při jejich implementaci v Pythonu.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
4. Hodnocení výsledků, jejich využitelnost	*55 (E)*

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:

Studentovy výsledky jsou jen omezeně využitelné, jelikož ve svých experimentech nepořídil a systematicky neroztřídil výsledky měření časů operací, aby bylo možno vyvodit alespoň nějaké závěry. V současné podobě studentova implementace prolomí několik prvních bitů klíče, což je pozitivní zpráva, ale nedostatek dat omezuje využitelnost studentovy práce.

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 svoji práci konzultoval s vedoucím a věnoval úsilí řešení nastalých problémů. S ohledem na to, že student opakuje obhajobu, mohla být jeho aktivita větší.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
6. Celkové hodnocení	*55 (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:

Student naprogramoval implementaci časového útoku na RSA. Útok se mu nepodařilo zprovoznit tak, aby byl spolehlivě funkční, což samo o sobě není zásadní nedostatek. Větší problém je v nedostatečném popisu provedených experimentů a jejich vyhodnocení. I tak ale student prokázal schopnost samostatné práce a proto doporučuji jeho práci k obhajobě a hodnotím stupněm E.

Podpis vedoucího práce: