Hodnocení vedoucího závěrečné práce

České vysoké učení technické v Praze **Fakulta informačních technologií**

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

Datum vytvoření: 14. 6. 2017

Hodnotící kritérium:	*Způsob hodnocení - následující škálou 1 až 5:*
1. Náročnost a další komentář k zadání	*1=mimořádně náročné zadání,* ***2=náročnější zadání,*** *3=průměrně náročné zadání,* *4=lehčí, ale ještě dostatečně náročné zadání,* *5=nedostatečně náročné zadání*

Popis kritéria:
Podrobněji charakterizujte diplomovou (bakalářskou) práci a její případné návaznosti na předchozí nebo běžící projekty. Dále posuďte, čím je zadání této ZP náročné. (U obtížnější ZP lze dále tolerovat některé nedostatky, které by u ZP standardní obtížnosti tolerovány nebyly; a naopak u jednoduché ZP mohou být zjištěné nedostatky hodnoceny přísněji.)

Komentář:
Zadání vyžaduje samostatné studium odborných vědeckých publikací, a následnou implementaci útoku, což jej činí poměrně náročným.

Hodnotící kritérium:	*Způsob hodnocení - následující škálou 1 až 4:*
2. 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 splňuje zadání. V komentáři uveďte body zadání, které nebyly zcela splněny, případně rozšíření ZP oproti původnímu zadání. Nebylo-li zadání zcela splněno, pokuste se posoudit závažnost, dopady a případně i příčiny jednotlivých nedostatků.

Komentář:
Student v práci rozebírá principy šifrování i časových útoků RSA. Student implementoval vybrané varianty útoku v jazyce Python, které však v jeho implementaci nefungují tak, jak by teoreticky měly. To by vyžadovalo další čas a úsilí pro vyhodnocení chování studentovy implementace a zjištění příčin neúspěchu útoků. Student ale dodělával práci na poslední chvíli, a další analýzu a případné úpravy už nestihl provést.

Hodnotící kritérium:	*Způsob hodnocení - následující škálou 1 až 4:*
3. Rozsah písemné zprávy	*1=splňuje požadavky,* ***2=splňuje požadavky s menšími výhradami,*** *3=splňuje požadavky s většími výhradami,* *4=nesplňuje požadavky*

Popis kritéria:
Zhodnoťte přiměřenost rozsahu předložené ZP vzhledem k obsahu, tj. zda všechny části ZP jsou informačně bohaté a ZP neobsahuje zbytečné části.

Komentář:
Práce obsahuje hlavní části, které by mít měla, ty jsou ale mnohdy příliš stručné, což je způsobeno výše uvedeným nedostatkem času na straně studenta. Student by jistě byl schopen práci dotáhnout do lepšího stavu.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
4. Věcná a logická úroveň práce	*65 (D)*

Popis kritéria:
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.

Komentář:
Práce je po věcné stránce dobrá, avšak z důvodu stručnosti a chybějících částí trpí i její logická struktura, a tím pochopitelnost pro čtenáře. Např. v kapitole o útocích (kap. 3) chybí úvodní shrnutí. Čtenář, který není předem seznámen s probíranými útoky bude mít problém s pochopením jejich dalšího popisu.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
5. Formální úroveň práce	*65 (D)*

Popis kritéria:
Posuďte správnost používání formálních zápisů obsažených v práci. Posuďte typografickou a jazykovou stránku ZP, viz Směrnice děkana č. 14/2015, článek 3.

Komentář:
Student se snaží o korektní notaci operací a popis algoritmů. Vzhledem k uspěchanosti dokončování práce se mu však vloudily chyby, které neměl čas odstranit. Totéž se dá říci o jazykové stránce.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
6. Práce se zdroji	*65 (D)*

Popis kritéria:
Vyjádřete se k aktivitě studenta při získávání a využívání studijních materiálů k řešení ZP. Charakterizujte výběr studijních pramenů. Posuďte, zda student využil všechny relevantní zdroje nebo zda se pokoušel řešit již vyřešené problémy. Ověřte, zda jsou všechny převzaté prvky řádně odlišeny od vlastních výsledků a úvah, zda nedošlo k porušení citační etiky a zda jsou bibliografické citace úplné a v souladu s citačními zvyklostmi a normami.

Komentář:
Student aktivně vyhledával relevantní zdroje. Ne vždy je však odkazuje na místě, kde by to čtenář potřeboval. Počet studijních pramenů je poměrně malý, což je však dáno zejména úzkým zaměřením na jeden konkrétní druh útoku, a to vychází ze zadání práce.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
7. Hodnocení výsledků, publikační výstupy a ocenění	*55 (E)*

Popis kritéria:
Vyjádřete se k úrovni dosažených hlavních výsledků ZP, např. k úrovni teoretických výsledků, nebo k úrovni a funkčnosti technického nebo programového vytvořeného řešení, apod. Případně také zhodnoťte, zda software nebo zdrojové texty, které nevytvořil sám student, byly v ZP použity v souladu s licenčními podmínkami a autorským právem. Popište případnou publikační činnost a získaná ocenění související s řešením této ZP.

Komentář:
Student se pokusil implementovat útok časovým postranním kanálem na šifru RSA. Výsledný program však nefunguje tak dobře, jak se předpokládalo, a kompletní tajný klíč neodhalí. Výsledek je jen částečně použitelný, pro použití ve výuce kryptologických předmětů by bylo potřeba programy dopracovat do funkčního stavu.

Hodnotící kritérium:	*Způsob hodnocení - nehodnotí se*
8. Komentář o využitelnosti výsledků	

Popis kritéria:
Uveďte, zda hlavní výsledky ZP rozšiřují již publikované známé výsledky a/nebo přinášející zcela nové poznatky. Uveďte možnosti využití výsledků ZP v praxi.

Komentář:
V současné podobě je práce jen omezeně použitelná při výuce předmětů počítačové bezpečnosti.

Hodnotící kritérium:	*Způsob hodnocení - následující škálou 1 až 5:*
9. Aktivita a samostatnost studenta v průběhu řešení	9a: *1=výborná aktivita,* *2=velmi dobrá aktivita,* *3=průměrná aktivita,* *4=slabší, ale ještě dostatečná aktivita,* ***5=nedostatečná aktivita*** 9b: ***1=výborná samostatnost,*** *2=velmi dobrá samostatnost,* *3=průměrná samostatnost,* *4=slabší, ale ještě dostatečná samostatnost,* *5=nedostatečná samostatnost*

Popis kritéria:
Posuďte, zda byl student během řešení aktivní, zda dodržoval dohodnuté termíny, jestli své řešení průběžně konzultoval a zda byl na konzultace dostatečně připraven (9a). Posuďte schopnost studenta samostatné tvůrčí práce (9b).

Komentář:
Student je schopen samostatné práce a má schopnosti na to, aby nastudoval a implementoval netriviální útok na šifru. Z hlediska aktivity mi však nezbývá, než hodnotit ji jako nedostatečnou, jelikož značnou část řešení práce nechal na poslední chvíli, a z toho plyne její současný stav. Zde musím poznamenat, že kdyby šlo vše podle předpokladů, a algoritmus útoku by fungoval přesně podle publikovaných článků, mohl výsledek vypadat lépe, ale student si nenechal rezervu na řešení nastalých problémů.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
10. Celkové hodnocení	*51 (E)*

Popis kritéria:
Shrňte stránky ZP studenta, které nejvíce ovlivnily Vaše celkové hodnocení. Celkové hodnocení **nemusí** být aritmetickým průměrem či jinou hodnotou vypočtenou z hodnocení v předchozích jednotlivých kritériích 1 až 9.

Text hodnocení:
Student prokázal, že je schopen samostatného studia a implementace netriviálních útoků, které jsou relevantní z hlediska počítačové bezpečnosti a její výuky. Z důvodu špatné organizace práce však student nedotáhl řešení do zcela funkčního stavu, a na další analýzu a odstranění chyb už mu nezbyl čas. Z toho důvodu hodnotím práci pouze stupněm dostatečně.

Podpis vedoucího práce: