

Hodnocení vedoucího závěrečné práce

České vysoké učení technické v Praze

Fakulta informačních technologií

Student: Tomáš Hradský
Vedoucí práce: Mgr. Martin Jureček
Název práce: Útok na šifru A5/1 v reálném čase
Obor: Informační technologie (bakalářský)

Datum vytvoření: 4. 6. 2015

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: Cieľom bakalárskej práce bolo pochopiť štruktúru šifry A5/1 a niekoľko netriviálnych techník používaných pri kryptoanalýze tejto šifry. Práca sa hlavne zaoberala technikou time-memory tradeoff a to na teoretickej aj implementačnej rovine. Táto technika poskytuje vďaka využitiu predpočítaných dát získanie tajného kľúča šifry v reálnom čase a to na bežnom PC. Zadanie bakalárskej práce považujem za stredne náročné.	
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: Jednou z úloh zadania práce bola implementácia a otestovanie time-memory tradeoff útoku. Úlohu implementovať útok považujem za splnenú, avšak vzhľadom k tomu, že získanie dostatočného množstva predpočítaných dát sa ukázalo byť časovo príliš náročné, nebolo preto možné implementáciu dostatočne otestovať. Dopad tejto skutočnosti na kvalitu práce považujem za minimálny.	
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: Rozsah predloženej BP je v súlade s požadovaným rozsahom podľa príslušnej fakultnej smernice.	
Hodnotící kritérium:	Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):
4. Věcná a logická úroveň práce	93 (A)
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: Věcná a logická stránka práce je na dobrej úrovni. Nepresnosti sa v práci vyskytujú len minimálne. Hlavný útok práce by mohol byť uvedený prehľadne v pseudokóde na konci druhej kapitoly. Miesto toho je súhrnnejšie popísaný až v popise implementácie.	
Hodnotící kritérium:	Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):
5. Formální úroveň práce	95 (A)
Popis kritéria: Posuďte správnost používání formálních zápisů obsažených v práci. Posuďte typografickou a jazykovou stránku ZP, viz Směrnice děkana č. 12/2014, článek 3.	
Komentář: V práci sa nedostatky spôsobené nepresným vyjadrovaním a preklepmi vyskytujú taktiež len minimálne.	

<i>Hodnotící kritérium:</i>	<i>Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):</i>
6. Práce se zdroji	95 (A)
<i>Popis kritéria:</i> 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.	
<i>Komentář:</i> Zoznam literatúry obsahuje relevantné zdroje, na ktoré sa študent správne odkazuje vo svojej práci.	
<i>Hodnotící kritérium:</i>	<i>Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):</i>
7. Hodnocení výsledků, publikační výstupy a ocenění	95 (A)
<i>Popis kritéria:</i> 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.	
<i>Komentář:</i> Jadrom práce je celá druhá kapitola, ktorá uvádza čitateľa do problematiky bezpečnosti GSM komunikácie. Hlavným prínosom sú podkapitoly 2.3 a 2.4, v ktorých sú uvedené známe útoky na A5/1 a podrobne spracovaný time-memory tradeoff útok, ktorého realizácia je spracovaná v tretej kapitole.	
<i>Hodnotící kritérium:</i>	<i>Způsob hodnocení - nehodnotí se</i>
8. Komentář o využitelnosti výsledků	
<i>Popis kritéria:</i> Uvedte, zda hlavní výsledky ZP rozšiřují již publikované známé výsledky a/nebo přinášející zcela nové poznatky. Uvedte možnosti využití výsledků ZP v praxi.	
<i>Komentář:</i> Práca môže slúžiť ako užitočný zdroj literatúry, ktorý obsahuje niekoľko kryptoanalytických techník použiteľných nielen na konkrétnu šifru.	
<i>Hodnotící kritérium:</i>	<i>Způsob hodnocení - následující škálou 1 až 5:</i>
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
<i>Popis kritéria:</i> 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 samostatně tvůrčí práce (9b).	
<i>Komentář:</i> Študent absolvoval mnoho zmysluplných konzultácií, na ktorých preukázal pochopenie danej témy.	
<i>Hodnotící kritérium:</i>	<i>Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):</i>
10. Celkové hodnocení	95 (A)
<i>Popis kritéria:</i> 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.	
<i>Text hodnocení:</i> Práca vyžadovala pochopenie a implementovanie netriviálnych kryptoanalytických techník, ktoré študent zvládol výborne. Bakalársku prácu pána Hradského doporučujem k obhajobe a hodnotím ju stupňom A (výborne).	

Podpis vedoucího práce: