Hodnocení vedoucího závěrečné práce

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

Student: Martin Holec
Vedoucí práce: Mgr. Martin Jureček
Název práce: Correlation Attack on A5/1
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:
Bakalárska práca je venovaná štruktúre a kryptoanalýze šifry A5/1, ktorá sa používa na zabezpečenie komunikácie mobilných telefónov, ktoré sú v súlade so štandardom GSM. Práca obsahuje niekoľko netriviálnych kryptoanalytických postupov, pričom sa venuje hlavne korelačnému útoku, ktorý sa študent pokúsil teoreticky spracovať a implementovať. 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:
Študent podcenil časovú náročnosť vypracovania BP a veľkú časť práce písal na poslednú chvíľu, v dôsledku čoho práca obsahuje veľké množstvo chýb, viac ako 70. Implementácia vznikala taktiež na poslednú chvíľu a tak sa ju nepodarilo dokončiť.

Popis štruktúry šifry A5/1 nie je kvalitný, napr.:
- podkapitola o LFSR, ktorý je základným kameňom šifry, je takmer celá doslova skopírovaná z knihy
- nie je pravda, že taktovacie bity sú jediná nelineárna časť LFSR
- nedodržuje sa bežná terminológia, napr. miesto "last bits" má byť most significant bits
- posun registrov a taktiež pseudokód na str. 10 je nepresne a neodborne popísaný

3.kapitola o korelačnom útoku taktiež obsahuje množstvo chýb:
- tabuľka 3.1 na str. 20 je nesprávne
- množstvo preklepov a dvojitých značení(session key - secret key, running key - keystream, ...)
- interval "I" na str. 24. nie je príslušný pozícii "v", ale trojici (cl1, cl2, cl3)
- tabuľka 3.2 na str. 26 je taktiež nesprávne
- chýba zhrnutie celého útoku napr. do pseudokódu

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	*47 (F)*

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:
V práci sa vyskytuje pomerne veľké množstvo chýb a nepresností, viď bod 2. U štruktúry práce je taktiež priestor k zlepšeniu.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
5. Formální úroveň práce	*50 (E)*

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:
Po formálnej stránke práca taktiež obsahuje pomerne veľa nedostatkov, viď bod 2. Po jazykovej stránke by mohla byť použitá odbornejšia angličtina.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
6. Práce se zdroji	*40 (F)*

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:
Prácu som zdrojmi literatúry považujem za nedostatočnú. V zozname je množstvo nerelevantnej literatúry a častokrát sa stáva, že sa študent miesto odkazu na správny zdroj odkazuje na zdroj, ktorý má správny zdroj uvedený v jeho zozname literatúry.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
7. Hodnocení výsledků, publikační výstupy a ocenění	*48 (F)*

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:
Výstupy práce nie sú v súlade s očakávaním. Implementáciu útoku nepovažujem za príliš zložitú a verím, že by ju študent bez problémov zvládol, ak by si rozumnejšie rozvrhol čas. Za prínos považujem spracovanie niekoľkých kryptoanalytických techník z druhej kapitoly a ak odhliadnem od mnohých preklepov, tak aj popis jednoduchšej verzie korelačného útoku z kapitoly 3.2.

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:
Práca by mohla slúžiť ako užitočný zdroj literatúry, ktorý obsahuje niekoľko kryptoanalytických techník použiteľných nielen na konkrétnu šifru.

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=priemerná aktivita,*** *4=slabší, ale ještě dostatečná aktivita,* *5=nedostatečná aktivita* 9b: *1=výborná samostatnost,* *2=velmi dobrá samostatnost,* ***3=priemerná 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:
Na konzultáciach študent preukázal pochopenie veľkej časti danej problematiky a preto verím, že veľa chýb je spôsobených len nepozornosťou počas písania práce na poslednú chvíľu.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
10. Celkové hodnocení	*47 (F)*

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:
Veľká časť BP bola vypracovaná pod tlakom z nedostatku času, čo sa odrazilo na jej kvalite. Domnievam sa, že implementácia práce taktiež nie je z tohto dôvodu dokončená. Pán Holec odovzdal BP k obhajobe s vedomím, že som mu to nedoporučil. Práca sa pohybuje na hranici obhájiteľnosti, ale z uvedených dôvodov sa mierne prikláňam k tomu, aby bola práca prepracovaná.

Podpis vedoucího práce: