Posudek oponenta závěrečné práce

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

Student: Bc. Lenka Vábková
Oponent práce: Ing. Josef Kokeš
Název práce: Algebraická kryptoanalýza Baby Rijndael
Obor: Počítačová bezpečnost

Datum vytvoření: 15. 5. 2016

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 je mimořádně náročné tím, že vyžaduje využít značně komplikovaný matematický aparát pro provedení algebraického útoku na šifru, která je navržená tak, aby tomuto útoku odolávala. Studentka se musela seznámit s existujícími algoritmy, pochopit je, efektivně naimplementovat a také se pokusit vymyslet úpravy, které je pomohou reálně použít i navzdory konstrukci šifry.

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:
Zadání je z větší části splněno, není však zřejmé, zda a jak byl plněn požadavek na seznámení se "s navrhovanými, ale neprověřenými algebraickými útoky". V textu práce o tom není zmínka, v použité literatuře dokonce není příslušný zdroj ze zadání (!) vůbec zmíněn (!!).

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:
Příloha 5 směrnice děkana 14/2015 *doporučuje* pro DP rozsah 50 stran, starší směrnice 40. Předložená DP má 37 stran obsahového textu, z toho jsou 3 strany zcela prázdné. Text je sice extrémně hutný, ale právě proto by bylo dobré zvolit volnější tempo a proložit text detailnější rešerší, více příklady a podrobnějším vysvětlením probíraných témat. Jestli práce splňuje nebo nesplňuje požadavky není jasné -- po obsahové stránce splňuje, i když s výhradami, po formální stránce nikoliv (ale po ještě formálnější stránce jde jen o doporučení, ne požadavky).

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
4. Věcná a logická úroveň práce	*70 (C)*

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:
To, co je v práci uvedeno, je vesměs v pořádku (výhrady následují níže) a zaslouží si vysoké hodnocení. Bohužel kvůli její velmi krátké délce práce "visí ve vzduchu", chybí zasazení práce do kontextu, podrobná rešerše oblasti (zastupuje ji úvod dlouhý 1,5 strany), detailnější diskuse výsledků. Logická struktura a návaznosti jsou dobré, ale text je obecně velmi nepřátelský vůči čtenáři a tvrdě vyžaduje, aby si čtenář popsané matematické koncepty a techniky nastudoval samostatně a v této DP si jen přečetl o jejich aplikaci. Další dílčí problémy:
- V rovnici 1.3 by někde měla vystupovat proměnná i. Rovnice je zřejmě myšlená tak, že každé funkci f_i přísluší jiná sada koeficientů c_x, ale v textu to uvedeno není.
- Rovnice 1.6 používají úplně jiné značení než zbytek textu včetně uvozujícího odstavce k rovnicím 1.6. Ověřil jsem, že rovnice jsou správné, ale je nutné je přeznačit: místo u_x resp. v_x mělo být u_{4-x} resp. v_{4-x}, kde x je index použitý v rovnici 1.6.
- Vztah 1.7 je chybný, např. pro vstup u(x)=x^3+x^2+x+1 vychází v(x)=x^2+1, z definice S-boxu má ale vyjít v(x)=x^3+x^2+1. Navazující rovnice 1.10 už jsou ale v pořádku.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
5. Formální úroveň práce	*75 (C)*

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:
Formální zápisy jsou v pořádku, problémem je místy nekonzistentní značení v nich. Příkladem může být nejen rovnice 1.6 uvedená výše, ale také první odstavec strany 11, jehož symbolismus nesedí na dále používané rovnice. Množství překlepů je vyšší, než by mělo být, ale ještě snesitelné. Na straně 34 jsou zápisy typu "?15 řešení". Angličtina abstraktu by zasloužila větší kontrolu. Celkově práce budí dojem, že zatímco studiu problému a experimentování věnovala studentka mnoho úsilí, zpráva o odvedené práci byla psána ve spěchu a pečlivost musela ustoupit potřebě stihnout termín odevzdání.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
6. Práce se zdroji	*75 (C)*

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:
Zdrojů je v práci použito poměrně málo, a to většinou jen zmínkou v úvodu. Rozsáhleji citované jsou jen zdroje 4, 10 a 11. Zvolené zaměření práce s tím není v rozporu a se zdroji si vystačí, velmi je ale znát slabě zdokumentovaná (provedená zřejmě byla) rešerše problémové oblasti. Samotné užití cizích myšlenek je citováno v souladu s požadavky.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
7. Hodnocení výsledků, publikační výstupy a ocenění	*85 (B)*

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:
Dosažené výsledky mají velmi solidní úroveň. Studentce se podařilo zformulovat šifru v termínech algebraické kryptoanalýzy a provést útoky, přičemž přesvědčivě demonstrovala, že s rostoucím počtem rund velmi významně roste složitost útoku a už pro čtyři rundy je i redukovaný model AESu proti zvolené technice odolný. Techniky popsané v kapitole 2.3 vypadají slibně, bohužel podrobněji zkoumáno bylo jen využití pravděpodobnosti. Zcela stranou zůstala otázka, jestli mají všechny proměnné stejný význam nebo jestli některé proměnné mají zvláštní vliv na obtížnost luštění soustavy. Zde práce opět trpí přílišnou stručností a patrně tlakem termínů.

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:
Za nejpřínosnější část práce považuji provedené experimenty s útokem. To, že nedokázaly šifru prolomit, není špatně -- naopak to slouží jako indikátor, že i v tomto ohledu je šifra vytvořena natolik dobře, že se s rostoucím počtem rund velmi rychle stává výpočetně neprolomitelnou, a to i ve zmenšené variantě. Na provedenou práci by mohla dobře navázat další DP, která detailněji rozpracuje právě kapitolu 2.3.

Hodnotící kritérium:	*Způsob hodnocení - nehodnotí se*
9. Otázky k obhajobě	

Popis kritéria:
Uveďte případné dotazy, které by měl student zodpovědět při obhajobě ZP před komisí (body oddělte odrážkami).

Otázky:
Můžete odhadnout, zda jsou některé proměnné významnější pro schopnost šifru prolomit než jiné?

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
10. Celkové hodnocení	*80 (B)*

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:

Základní slabinou práce je přílišná stručnost zprávy, která se negativně odráží do všech aspektů hodnocení. Nepochybuji, že studentka problematice porozuměla, ale nedokázala tuto svoji znalost "prodat" čtenáři, který se tak o ní může jen dohadovat. Na druhou stranu, nelze upřít, že požadovaná práce odvedena byla, což u takto obtížného zadání zdaleka nelze brát jako samozřejmost. S ohledem na to i přes vznesené výhrady doporučuji práci k obhajobě a hodnotím ji stupněm B (na hranici s C).

Podpis oponenta práce: