Hodnocení vedoucího závěrečné práce

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

Student: Bc. Jakub Tomanek
Vedoucí práce: Ing. Josef Kokeš
Název práce: Diferenciální kryptoanalýza šifry Baby Rijndael
Obor: Počítačová bezpečnost

Datum vytvoření: 15. 5. 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 samo o sobě je nadprůměrně náročné svým zaměřením na oblast kryptoanalýzy. Jen díky tomu, že navazuje na několik už existujících prací, ve kterých bylo možné hledat inspiraci, ho nehodnotím jako mimořádně náročné. Student každopádně musel porozumět složitým teoretickým konceptům a následně je vhodně aplikovat. Při tom se musel vypořádat s výraznou výpočetní náročností jednotlivých dílčích úkolů.

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 bylo splněno. Student k němu přistoupil značně ambiciozně a provedl mnohem hlubší analýzu, než bylo očekáváno.

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 zprávy je přiměřený. Délku navyšuje množství grafů a obrázků, které však jsou nezbytné pro plné znázornění provedené analýzy a jejích výsledků.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
4. Věcná a logická úroveň práce	*95 (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:
Práce je po věcné i logické stránce mimořádně kvalitní. Postup analýzy je popsán srozumitelným způsobem, jednotlivé kroky na sebe logicky navazují. V řadě případů šla analýza do podstatně větší hloubky, než bylo požadováno.

V práci se vyskytuje několik zbytečných chyb, které však mají spíše charakter překlepů. Nejvážnější je na str. 36, kde student pracuje s jednou diferenciální charakteristikou, aby pod tabulkou bez zjevného důvodu přešel k charakteristice jiné. Z kontextu je však zřejmé, že jde jen o zapomenutý starý popisek, obsah samotný je v pořádku. Podobně na straně 38 dole nacházíme kladný exponent, evidentně ale byl myšlen exponent záporný. Tyto chyby jsou nešťastné, nesnižují však výrazně kvalitu práce.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
5. Formální úroveň práce	*90 (A)*

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:
Po formální a jazykové stránce je práce velmi dobrá, ačkoliv se nevyhnula několika drobným chybám. Jde zejména o překlepy, kterých ale není mnoho, zapomenutý anglický popisek u obrázku 5.3 a podobně. Naopak jen chválit lze formální zápisy včetně důkazů.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
6. Práce se zdroji	*85 (B)*

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:
Ke studentově práci s prameny a množství, obsahu či relevanci zdrojů nemám vážnější výhrady, uvítal bych ale, kdyby zahraniční zdroje byly novějšího data. Aktuální zdroje jsou vesměs jen české. U zdroje č. 2 chybí název časopisu (ve zdrojovém kódu se vyskytuje). Nepříjemné, ne však chybné, je řazení zdrojů podle výskytu v textu.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
7. Hodnocení výsledků, publikační výstupy a ocenění	*95 (A)*

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 jsou velmi kvalitní. Student přistoupil k analýze velmi důkladně a shromáždil obrovské množství informací, které přehledně a srozumitelně zpracoval. Důraz na přesnost je v práci mimořádný.

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:
Výsledky navazují na dříve provedené analýzy šifry Baby Rijndael, ale z pohledu zcela jiné kryptoanalytické techniky. V tomto smyslu jde tedy o zcela nové poznatky. Nepodařilo se nalézt způsob, jak útok provést v praxi na plný AES, to se však dalo očekávat a z pohledu uživatele není špatné, když je takto dále potvrzena síla nejrozšířenější blokové šifry.

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:
Perfektní.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
10. Celkové hodnocení	*95 (A)*

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 odvedl mimořádně důkladnou a kvalitní práci v náročném oboru kryptoanalýzy. Demonstroval, že použitým technikám rozumí a dokáže je uplatnit, přišel i s řadou podnětných originálních nápadů. Oceňuji velmi pečlivou analýzu jednotlivých možností, která byla časově velmi náročná a její následné zpracování do podoby poměrně stručné zprávy značně komplikované. Výsledkem je práce, která komplexně pokrývá diferenciální kryptoanalýzu šifry Baby Rijndael.

Podpis vedoucího práce: