FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

# Hodnocení vedoucího závěrečné práce

| | |
|---|---|
| **Student:** | Bc. Marek Bielik |
| **Vedoucí: práce:** | Mgr. Martin Jureček |
| **Název práce:** | Algebraic Cryptanalysis of Small Scale Variants of the AES |
| **Obor:** | Systémové programování |

**Datum vytvoření:** 8. 1. 2021

| *Hodnotící kritérium:* | *Způsob hodnocení – následující škálou 1 až 4:* |
|---|---|
| **1. Splnění zadání** | ***1=zadání splněno,***<br>*2=zadání splněno s menšími výhradami,*<br>*3=zadání splněno s většími výhradami,*<br>*4=zadání nesplněno* |

*Popis kritéria:*
Posuďte, zda předložená ZP dostatečně a v souladu se zadáním obsahově vymezuje cíle, správně je formuluje a v dostatečné kvalitě naplňuje. V komentáři uveďte body zadání, které nebyly splněny, posuďte závažnost, dopady a případně i příčiny jednotlivých nedostatků. Pokud zadání svou náročností vybočuje ze standardů pro daný typ práce nebo student případně vypracoval ZP nad rámec zadání, popište, jak se to projevilo na požadované kvalitě splnění zadání a jakým způsobem toto ovlivnilo výsledné hodnocení.

*Komentář:*
Všetky body popísané v pokynoch pre vypracovanie práce považujem za splnené.

| *Hodnotící kritérium:* | *Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):* |
|---|---|
| **2. Písemná část práce** | *99 (A)* |

*Popis kritéria:*
Zhodnoťte přiměřenost rozsahu předložené ZP vzhledem k obsahu, tj. zda všechny části ZP jsou informačně bohaté a ZP neobsahuje zbytečné části. Dále 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. Posuďte správnost používání formálních zápisů obsažených v práci. Posuďte typografickou a jazykovou stránku ZP, viz Směrnice děkana č. 26/2017, článek 3. Posuďte, zda student využil a správně citoval relevantní zdroje. Ověřte, zda jsou všechny převzaté prvky řádně odlišeny od vlastních výsledků, zda nedošlo k porušení citační etiky a zda jsou bibliografické citace úplné a v souladu s citačními zvyklostmi a normami. Zhodnoťte, zda převzatý software a jiná autorská díla, byly v ZP použity v souladu s licenčními podmínkami.

*Komentář:*
Predložená práca študenta je dobre čitateľná s minimálnym počtov drobných chýb. Rozsah práce je v súlade s požadovaným rozsahom podľa príslušnej fakultnej smernice. Typografická aj jazyková stránka je taktiež na veľmi dobrej úrovni. Uvedené zdroje sú relevantné k práci študenta. Celkovo je z textu práce je cítiť, že študent sa snažil vysvetliť pomerne rozsiahlu problematiku algebraickej kryptoanalýzy a nevyhýba sa ani jej náročnejším partiám.

| *Hodnotící kritérium:* | *Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):* |
|---|---|
| **3. Nepísemná část, přílohy** | *100 (A)* |

*Popis kritéria:*
Dle charakteru práce se případně vyjádřete k nepísemné části ZP. Například: SW dílo – kvalita vytvořeného programu a vhodnost a přiměřenost technologií, které byly využité od vývoje až po nasazení. HW – funkční vzorek – použité technologie a nástroje, Výzkumná a experimentální práce
– opakovatelnost experimentů

*Komentář:*
Generovanie rovníc bolo vykonané v jazyku Python s použitím knižníc z prostredia SageMath. Magma a CryptoMiniSat boli použité k riešeniu polynomiálnych rovníc. Všetky dosiahnuté experimentálne výsledky je možné overiť.

| *Hodnotící kritérium:* | *Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):* |
|---|---|
| **4. Hodnocení výsledků, jejich využitelnost** | *100 (A)* |

*Popis kritéria:*
Dle charakteru práce zhodnoťte možnosti nasazení výsledků práce v praxi nebo uveďte, zda výsledky ZP rozšiřují již publikované známé výsledky nebo přinášející zcela nové poznatky.

*Komentář:*

Študentove výsledky preukázali, že kombináciou rôzných techník ako napr. guess-and-determine alebo zjednodušenie polynómov vďaka pridaným párom otvorený a šifrový text, je možné prelomiť niektoré zjednodušené varianty AES, ktoré sa priamou metódou algebraickej kryptoanalýzy prelomiť nedali. Takéto výsledky sú vhodné k publikovaniu a navyše existuje nemalý priestor k ich vylepšeniu, čo čiastočne študent naznačuje vo svojej práci.

| *Hodnotící kritérium:* | *Způsob hodnocení – následující škálou 1 až 5:* |
|---|---|
| **5. Aktivita a samostatnost studenta** | 5a:<br>***1=výborná aktivita,***<br>*2=velmi dobrá aktivita,*<br>*3=průměrná aktivita,*<br>*4=slabší, ale ještě dostatečná aktivita,*<br>*5=nedostatečná aktivita*<br>5b:<br>***1=výborná samostatnost,***<br>*2=velmi dobrá samostatnost,*<br>*3=průměrná samostatnost,*<br>*4=slabší, ale ještě dostatečná samostatnost,*<br>*5=nedostatečná samostatnost* |

*Popis kritéria:*
V souvislosti s průběhem a výsledkem práce posuďte, zda byl student během řešení aktivní, zda dodržoval dohodnuté termíny, jestli své řešení průběžně konzultoval a zda byl na konzultace dostatečně připraven (5a). Posuďte schopnost studenta samostatné tvůrčí práce (5b).

*Komentář:*

So študentom sme absolvovali viac ako sto konzultácií, na ktorých ma študent presvedčil, že rozumie detailne danej problematike. Taktiež hodnotím pozitívne, že študent mohol svoju prácu odovzdať už v lete, avšak rozhodol sa dokončiť niektoré ďalšie experimenty a taktiež rozšíriť a vylepšiť text, čo sa mu podarilo.

| *Hodnotící kritérium:* | *Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):* |
|---|---|
| **6. Celkové hodnocení** | *100 (A)* |

*Popis kritéria:*
Shrňte stránky ZP, které nejvíce ovlivnily Vaše celkové hodnocení. Celkové hodnocení nemusí být aritmetickým průměrem či jinou hodnotou vypočtenou z hodnocení v předchozích jednotlivých kritériích. Obecně platí, že bezvadně splněné zadání je hodnoceno klasifikačním stupněm A.

*Text hodnocení:*

V práci je prehľadne spracované použitie algebraickej kryptoanalýzy na zmenšené verzie šifry AES a výsledky práce sú vhodné k publikácii. Preto študentovu prácu hodnotím známkou A.

Podpis vedoucího práce: