# Hodnocení vedoucího závěrečné práce

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

**Student:** Bc. Lukáš Solil
**Vedoucí práce:** Ing. Josef Kokeš
**Název práce:** Redukované modely šifry Rijndael
**Obor:** Počítačová bezpečnost

**Datum vytvoření:** 8. 5. 2016

| *Hodnotící kritérium:* | *Způsob hodnocení - následující škálou 1 až 5:* |
|---|---|
| **1. Náročnost a další komentář k zadání** | *1=mimořádně náročné zadání,*<br>***2=náročnější zadání,***<br>*3=průměrně náročné zadání,*<br>*4=lehčí, ale ještě dostatečně náročné zadání,*<br>*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 hodnotím jako náročnější, protože vedle programování vyžaduje schopnost vypořádat se s matematickou definicí šifry a její transformací na menší modely, včetně podrobného doložení, proč je tato transformace v souladu s původní specifikací.

| *Hodnotící kritérium:* | *Způsob hodnocení - následující škálou 1 až 4:* |
|---|---|
| **2. 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 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 ve všech bodech splněno. Student navíc ke všem dílčím požadavkům přistoupil velmi ambiciozně a zvlášť u bodu praktické demonstrace použití redukovaných modelů musím zdůraznit, že dokonce navrhl vlastní kryptoanalytickou techniku. Že jí šifra odolala není jeho chybou.

| *Hodnotící kritérium:* | *Způsob hodnocení - následující škálou 1 až 4:* |
|---|---|
| **3. Rozsah písemné zprávy** | ***1=splňuje požadavky,***<br>*2=splňuje požadavky s menšími výhradami,*<br>*3=splňuje požadavky s většími výhradami,*<br>*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:*
Práce odpovídá požadavkům na rozsah DP. Jednotlivé části jsou informačně bohaté, nenacházím zbytečná místa. Na CD je také k dispozici poměrně rozsáhlý manuál k instalaci a použití vytvořených programů.

| *Hodnotící kritérium:* | *Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):* |
|---|---|
| **4. Věcná a logická úroveň práce** | *90 (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:*
Po věcné stránce je práce výborná. Studentovi se podařilo přesně matematicky formulovat svoje myšlenky a přitom udržet srozumitelnost pro čtenáře. Jedinou skutečnou chybu jsem našel v algoritmu 5.1, který tak, jak je napsán, nemůže fungovat (je nutné uložit hodnotu ŠT_{i-1}) -- tato chyba je však jen důsledek nepozornosti při přepisu algoritmu na papír, protože v programu je každému programátorovi evidentní.

| *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. 12/2014, článek 3.

*Komentář:*

Po formální stránce je práce též výborná. Jazykové chyby téměř neobsahuje. Formální zápisy jsou z větší části v pořádku, i když chyby se vyskytnou: nekonzistentní zápis Galoisových polích, kde zkratka GF je někdy psána normálním písmem a jindy kurzívou (např. na konci kapitoly 1.4.1); výraz pro šifrový text v kapitole 5 má "Š" psané normálně a "T" kurzívou; ve značení množiny prvků dosažitelných opakovaným šifrováním chybí složené závorky apod. Nejde však o velké chyby a jsou více než bohatě vyrovnány na DP mimořádně precizní formulací matematických myšlenek (použití standardních formátů definice-věta-důkaz). Větší chyby nacházím v angličtině ve výsledné aplikaci, zejména mě dráždí použití výrazu "bites" tam, kde autor píše o bitech, ale text v aplikaci je i tak srozumitelný.

| *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:*

Práce se zdroji je velmi dobrá, zdrojů sice není extrémně mnoho a zahrnují i citace z méně vhodných zdrojů (Wikipedie, EDUX), ale jsou relevantní a pokrývají dobře zpracovanou látku. Chybí mi zahrnutí článku "Raphael Chung-Wei Phan: Mini Advanced Encryption Standard (Mini-AES): A Testbed for Cryptanalysis Students. In: Cryptologia, Volume 26, Issue 4, 2002, DOI 10.1080/0161-110291890948", který by se k tématu práce velmi hodil, ale je k dispozici pouze v placené podobě. U zdroje [9] jsem si skoro jistý, že to není ročník 2442.

| *Hodnotící kritérium:* | *Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):* |
|---|---|
| **7. Hodnocení výsledků, publikační výstupy a ocenění** | *98 (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:*

Práce velmi precizně formuluje podmínky a pravidla pro vytváření redukovaných modelů šifry Rijndael. Vytvořené programy jsou přehledné a funkční, a to i mimo cílovou platformu Linux (ověřeno na Windows). Demonstrační kryptoanalýza je zajímavá, i když zřejmě pro modely AESu nefunkční, a jednoznačně nad rámec toho, co bylo po studentovi možné spravedlivě požadovat.

| *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:*

Textová podoba práce poslouží jako dobrý odrazový můstek pro využití modelů šifry Rijndael pro kryptoanalýzu. Vytvořené aplikace pak dovolí tuto kryptoanalýzu snadno provést, protože vytvoření použitelného modelu je s nimi jednoduchou záležitostí -- zbývá provést pouze výkonnostní optimalizaci, která však musí být "šitá na míru" jak konkrétní modelu, tak hlavně konkrétní kryptoanalýze.

| *Hodnotící kritérium:* | *Způsob hodnocení - následující škálou 1 až 5:* |
|---|---|
| **9. Aktivita a samostatnost studenta v průběhu řešení** | 9a:<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>9b:<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:*
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:*

Student byl při zpracovávání práce velmi aktivní i samostatný. Chodil na konzultace, dodržoval termíny i stanovené úkoly, téměř pokaždé přišel s vlastními nápady na pokračování v práci.

| *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 se s větší náročností zadání vypořádal velmi pěkně a stvořil práci, která je všestranně užitečná pro kryptoanalýzu šifer postavených na bázi šifry Rijndael. Zvlášť bych chtěl upozornit na mimořádně precizní formulaci matematických myšlenek, kterou v práci nalezneme. Nad rámec požadavků přišel s návrhem vlastní nové kryptoanalytické techniky, kterou svými modely ověřil (bohužel neúspěšně). Bez nejmenších pochyb splnil požadavky, které jsou na diplomovou práci kladené a vytvořil vysoce nadprůměrně kvalitní dílo. Práci doporučuji k obhajobě a hodnotím stupněm A.

Podpis vedoucího práce: