Hodnocení vedoucího závěrečné práce

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

Student: Bc. Šárka Hatašová
Vedoucí práce: Ing. Josef Kokeš
Název práce: Lineární kryptoanalýza šifry Anubis
Obor: Počítačová bezpečnost

Datum vytvoření: 11. 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:
Pro zpracování zadání musela studentka vynaložit značné úsilí, nastudovat množství náročných publikací, vymyslet a zdokumentovat vhodnou redukci šifry a také implementovat výpočetně značně náročný algoritmus.

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.

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:
Práce splňuje stanovené požadavky na rozsah.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
4. Věcná a logická úroveň práce	*98 (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:
Text práce je logicky dobře uspořádán a logicky vede čtenáře, i když kapitola 3 je množstvím matematických formalismů (které jsou v ní ale nezbytné) k čtenáři poměrně tvrdá. Věcné chyby jsem nenašel.

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:
Formální úroveň práce je velmi dobrá. Narazil jsem na tři chyby, které mají charakter překlepů, u obrázku 5.2 chybí oranžové body (bias -32/256). Formální zápisy jsou v pořádku, typografická stránka odpovídá standardní předloze. Menší výhradu mám k jisté rozkolísanosti jazyka v rámci kapitol, kdy kapitola 1 se zdá být psána méně formálním stylem než zbytek textu.

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

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 perfektní. Zdrojů sice není mnoho, ale jsou výborně voleny a studentce muselo dát jejich nalezení i zpracování velkou práci.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
7. Hodnocení výsledků, publikační výstupy a ocenění	*90 (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 zajímavé. Už při použití tří rund modelu šifry Anubis se úspěšnost lineární kryptoanalýzy výrazně snížila, což indikuje, že šifra je v tomto směru dobře navržená. Přínosem práce je její bibliografie, která dobře reprezentuje stav lineární kryptoanalýzy řady moderních šifer, a také to, že seznamuje čtenáře se symetrickou blokovou šifrou s velmi zajímavými vlastnostmi.

Jedinou pochybnost mám u vytvořených programů: Studentka v práci použila knihovnu Matrix, u níž se mi nepodařilo dohledat licenci. Autor implementace je odkazován a z kontextu je zřejmé, že s použitím knihovny souhlasí, explicitní licence ale chybí. Protože však je knihovna použita zcela okrajově a jen v částech, které by každý student prvního ročníku FITu snadno naprogramoval sám, nespatřuji v tom vážný problém.

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:
Šifra Anubis se nestala vítězem soutěže, do které byla přihlášena, takže v praxi je odsouzena na okraj zájmu, což poněkud postihuje i využitelnost této práce. Přesto si myslím, že předložená DP využitelná je, minimálně v tom, že ukazuje, že použitá konstrukce šifry je silná a může dobře sloužit pro návrh. Také myšlenky týkající se vytváření modelů šifry a konstrukce lineárních aproximací větších celků jsou přínosné.

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:
Není co dodat, studentka byla mimořádně aktivní a přitom naprosto samostatná.

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:
Studentka si zvolila velice náročné téma závěrečné práce a velmi dobře ho zpracovala. Všechny části práce jsou vysoce nadprůměrné a bez pochyb dokazují, že studentka je schopna inženýrské práce. Práci doporučuji k obhajobě a hodnotím známkou A.

Podpis vedoucího práce: