Hodnocení vedoucího závěrečné práce

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

Student: Bc. Jakub Labant
Vedoucí práce: Ing. Josef Kokeš
Název práce: Lineární kryptoanalýza šifry GOST
Obor: Počítačová bezpečnost (magisterský)

Datum vytvoření: 11. 5. 2015

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:
Vypracování ZP vyžadovalo po studentovi značný objem tvůrčí práce. Pro úspěšné splnění zadání navíc musel nastudovat množství jazykově i odborně náročných materiálů.

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:
Bez výhrad.

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:
Porovnejte rozsah předložené písemné zprávy s požadovaným rozsahem, viz Směrnice děkana č. 9/2011, článek 3. Pro hodnocení ZP je také důležité, zda všechny části písemné zprávy jsou informačně bohaté a pro práci nezbytné. Text ZP by neměl obsahovat zbytečné části.

Komentář:
Bez výhrad.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
4. Věcná a logická úroveň práce	*80 (B)*

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:
Věcně je práce na vysoké úrovni, místy však autor sklouzává k tvrzením, která jsou minimálně odvážná:
- DES není "ekvivalent" GOSTu (str. 1).
- Použití náhodných S-boxů u GOSTu není spolehlivě doloženo (str. 7).
- Řešení problému modulárního sčítání vzhledem k lineární kryptoanalýze není dostatečně podloženo, carry funkce jsou závislé nejen na klíči ale i na datech včetně neaktivních bitů, proto je zřejmě nelze považovat za konstantní (str. 36).

Práce je přehledně a logicky členěna. Text je dobře srozumitelný, jen v kapitole 2 klade na čtenáře možná až příliš vysoké požadavky.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
5. Formální úroveň práce	*60 (D)*

Popis kritéria:
Posuďte správnost používání formálních zápisů obsažených v práci. Posuďte typografickou a jazykovou stránku ZP, viz Směrnice děkana č. 9/2011, článek 3.

Komentář:
Zápisy vesměs odpovídají zvyklostem v odborné literatuře.
Abstrakt v angličtině je těžkopádným doslovným přepisem české verze. Nejde o správnou angličtinu.
Některé odstavce jsou poněkud těžkopádné i v češtině (Úvod na str. 1, kapitola 1.4.2).
V práci i po korektuře zůstává mnoho překlepů, chybějící či přebývající diakritiky, chybějící či přebývající interpunkce (str. 3 - "následovně", "265-bitový klíč", "hdonota" atd.).
Na konci řádků zůstávají jednopísmenné předložky a spojky.

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:
Autor používá zdroje v souladu s požadavky na citační etiku. Zdrojů je přiměřené množství a jsou kvalitní. Jistou slabinu spatřuji v nekonzistentním zápisu jednotlivých zdrojů (např. formát jména autora u zdroje [1] a [5], formát časopisu u [2] a [3] nebo [1] a [9]).

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 kvalitní. Přesvědčivě ukazují, že GOST je vůči lineární kryptoanalýze značně odolný i při nízkém počtu rund. Ukazují také, jak i jednoduché algebraické operace (modulární sčítání, bitový posun) mohou znesnadnit kryptoanalýzu a prolomení šifry. Důležité jsou naměřené výsledky v pětirundové verzi šifry, kde už dochází k důkladnému promíchání informace a klíče a v důsledku přestávají fungovat i techniky, které autor úspěšně použil na třírundovou verzi šifry (kterou je nutné považovat za nejmenší smysluplnou).

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:
Práci lze zařadit mezi teoretické výzkumné práce. Do problematiky se snaží přinést něco nového a myslím si, že se jí to daří. Omezení jen na 3 a 5 rund je však příliš svazující pro časopiseckou publikaci.

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:
Student byl ve vypracování práce velmi aktivní, na dohodnuté konzultace chodil včas a připraven, s relevantními otázkami nebo s dobrým řešením dříve diskutovaných problémů.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
10. Celkové hodnocení	*90 (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:
Autor samostatně přistoupil k problému kryptoanalýzy šifry, která zatím nepodstoupila rozsáhlý výzkum (nebo aspoň jeho výsledky nebyly publikovány). Dokázal nalézt techniky, které v jednoduchém případě šifru úspěšně napadají, nemají ale sílu prolomit ji v případech složitějších. Místy slabší formální stránka práce a příliš odvážná práce s teorií (modulární sčítání) by patrně vedly spíš na hodnocení B, vzhledem k složitosti tématu a množství vynaloženého tvořivého úsilí však doporučuji práci hodnotit stupněm A.

Podpis vedoucího práce: