Posudek oponenta závěrečné práce

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

Student: Bc. Vojtěch Myslivec
Oponent práce: Ing. Josef Kokeš
Název práce: Asymetrický šifrovací algoritmus McEliece
Obor: Počítačová bezpečnost

Datum vytvoření: 19. 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:
Zadání samo o sobě je průměrně náročné, protože by mu vyhověla i pouhá reimplementace známých přístupů, student však zvolil přístup podstatně ambicioznější, čímž se práce stala náročnější až velmi náročnou.

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. Přesnější by bylo říci, že bylo významně překonáno.

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:
Vlastní text práce má 70 stran, dalších 20 zabírá literatura a přílohy, nic z toho není nadbytečné.

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:
Práce je skoro perfektní. Velmi logickým a srozumitelným způsobem seznamuje čtenáře s předmětnou oblastí, až do značné úrovně detailu. Několik věcných chyb, na které jsem narazil, má spíš charakter překlepu (algoritmus na str. 39 nemá správně zakončenou rekurzi, na str. 47 je parametr k určen jako n-r, ne n-k).

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
5. Formální úroveň práce	*75 (C)*

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 zápisy, typografie, algoritmy, tabulky, grafy, to vše je bez připomínek. Poněkud slabší je bohužel jazyková stránka - narazil jsem na několik hrubek v i/y, nepříjemně často se vyskytují chyby v čárkách (zejm. za vloženými přívlastkovými větami). Pozornosti utekly některé formální zápisy (2^11 vs. 2^{11} na str. 23 dole) a bohužel není vždy shoda mezi uváděným a skutečně používaným značením (str. 5 vs. str. 83). Galoisovo těleso píseme s jedním L. Velmi rušivě působí při čtení zvýrazňování některých termínů, které se často opakuje a není zřejmý důvod, proč vůbec je použito (např. tvary slova "kryptosystém").

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
6. Práce se zdroji	*98 (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:
Volba literatury a práce se zdroji jsou perfektní. Drobné výhrady mám opět k formální stránce - zápisy nejsou vždy konzistentní (např. [1] má mezi autorem a názvem práce čárku, ostatní zdroje tečku, některé zdroje používají plná jména autorů zatímco jiné jen iniciály, apod.). Chybí datum citace online zdrojů.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
7. Hodnocení výsledků, publikační výstupy a ocenění	*100 (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 vynikající. Práce je výborným zdrojem pro popis kryptosystému McEliece, srozumitelně popisuje jak samotný algoritmus, tak jeho bezpečnostní aspekty a možné směry vývoje. Také vytvořený software (v nástroji Mathematica) je výborný. Škoda, že autor nenaimplementoval i obecný generátor vhodných Goppa kódů, to však lze pochopit, protože už by to bylo daleko nad rámec stanovených požadavků a konec konců pro tuto implementaci poskytuje práce naprosto vyhovující podklady.

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:
Práce výborně shrnuje známé poznatky o kryptosystému McEliece v jednom dokumentu a spolu s provedenou implementací může sloužit jako výborný referenční zdroj, např. pro výuku nebo experimenty. Pro praktické použití by bylo třeba doplnit implementaci o generátor Goppa kódů, což je ale výrazně nad rámec požadavků zadání. Vytvořené knihovny pro Mathematicu, zejména části implementujjící podporu pro rozšířená algebraická tělesa, mohou být dobře použity i v jiných oblastech, a to okamžitě, bez dalších úprav.

Hodnotící kritérium:	*Způsob hodnocení - nehodnotí se*
9. Otázky k obhajobě	

Popis kritéria:
Uveďte případné dotazy, které by měl student zodpovědět při obhajobě ZP před komisí (body oddělte odrážkami).

Otázky:
- Má vůbec smysl hledat úsporu prostoru u soukromého klíče, i s ohledem na vaše tvrzení, že kapacity disků jsou téměř neomezené a limit je primárně v přenosu veřejného klíče?
- Zkoušel jste změřit dobu generování klíčů, šifrování a dešifrování pro bezpečné parametry, tedy např. m=12, t=41?

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
10. Celkové hodnocení	*98 (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:
Vynikající práce, která detailně seznamuje čtenáře s velmi slibným a aktuálním*) asymetrickým algoritmem McEliece. Úroveň zpracování tématu je výjimečná a je doprovázena velmi kvalitní softwarovou podporou, kterou lze navíc použít i v jiných oblastech. Jediným slabším místem jsou jazykové chyby, které ale nesnižují výrazně hodnotu práce. Doporučuji proto práci k obhajobě, hodnotím ji stupněm A (výborně) a jsem přesvědčen, že by komise měla zvážit navržení práce na cenu děkana.

*) http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf

Podpis oponenta práce: