# Hodnocení vedoucího závěrečné práce

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

**Student:** Bc. Jan Žák
**Vedoucí práce:** prof. Ing. Róbert Lórencz, CSc.
**Název práce:** Current Development of Authenticated Encryption and its Usage in the TLS Protocol
**Obor:** Počítačová bezpečnost (magisterský)

**Datum vytvoření:** 3. 6. 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:*
Zadání vyžaduje teoretickou a praktickou znalost šifrovacích algoritmů. Rovněž je zadání náročné z hlediska realizace aplikace a jejího testování.

| *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 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:*
Zhodnoťte přiměřenost rozsahu předložené ZP vzhledem k obsahu, tj. zda všechny části ZP jsou informačně bohaté a ZP neobsahuje zbytečné části.

*Komentář:*
Rozsah splňuje požadavky.

| *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 věcně velmi dobře napsaná. Výskyt nepřesností a logických chyb je nepatrný.

| *Hodnotící kritérium:* | *Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):* |
|---|---|
| **5. Formální úroveň práce** | *95 (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 na velmi dobré úrovní. Možná by přispěl k úplné "dokonalosti" pečlivější výběr zkratek v seznamu zkratek, preciznější kontrola grafického vzhledu atd.

| *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 s literaturou je na vynikající úrovni. Autor důsledně dodržuje uvádění zdrojů, ze kterých čerpal. Počet použitých zdrojů je nadprůměrný.

| *Hodnotící kritérium:* | *Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):* |
|---|---|
| **7. Hodnocení výsledků, publikační výstupy a ocenění** | *95 (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:*
Výstupy práce mají vysokou implementační a experimentální úroveň. Dosažené výsledky v předkládané práci mohou být základem pro vytvoření informativní publikace, která může být zaslána do technicko-populárního časopisu zabývajícího se bezpečnostní problematikou.

| *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:*
Na výsledky práce mohou tématický navázat další ZP.

| *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 přistupoval k řešení problematiky diplomové práce velmi aktivně a samostatně.

| *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:*
Práce je velmi vydařená. Autor prezentuje hlubokou znalost řešené problematiky a v textu práce precizně a systematicky používá zvolené zdroje. Práce prezentuje tématicky komplexní a implementačně náročný projekt. Oceňuji zejména snahu autora o implementaci a ověření funkčnosti šifry NORX, která byla přihlášena do soutěže CAESAR (Competition for Authenticated Encryption: Security, Applicability and Robustness). Taktéž oceňuji jeho snahu o sledování a dokumentování zmiňované soutěže.

Podpis vedoucího práce: