



# Hodnocení vedoucího závěrečné práce

**Student:** Bc. Jan Rahm  
**Vedoucí práce:** Ing. Jiří Buček, Ph.D.  
**Název práce:** Multivariate cryptography  
**Obor:** Počítačová bezpečnost

**Datum vytvoření:** 9. 6. 2020

<b>Hodnotící kritérium:</b>	<b>Způsob hodnocení – následující škálou 1 až 4:</b>
<b>1. Splnění zadání</b>	<b>1=zadání splněno, 2=zadání splněno s menšími výhradami, 3=zadání splněno s většími výhradami, 4=zadání nesplněno</b>
<b>Popis kritéria:</b> Posuďte, zda předložená ZP dostatečně a v souladu se zadáním obsahově vymezuje cíle, správně je formuluje a v dostatečné kvalitě naplňuje. V komentáři uveďte body zadání, které nebyly splněny, posuďte závažnost, dopady a případně i příčiny jednotlivých nedostatků. Pokud zadání svou náročností vybočuje ze standardů pro daný typ práce nebo student případně vypracoval ZP nad rámec zadání, popište, jak se to projevilo na požadované kvalitě splnění zadání a jakým způsobem toto ovlivnilo výsledné hodnocení.	
<b>Komentář:</b> Student splnil zadání v plném rozsahu.	
<b>Hodnotící kritérium:</b>	<b>Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):</b>
<b>2. Písemná část práce</b>	<b>85 (B)</b>
<b>Popis kritéria:</b> Zhodnoťte přiměřenost rozsahu předložené ZP vzhledem k obsahu, tj. zda všechny části ZP jsou informačně bohaté a ZP neobsahuje zbytečné části. Dále 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. Posuďte správnost používání formálních zápisů obsažených v práci. Posuďte typografickou a jazykovou stránku ZP, viz Směrnice děkana č. 26/2017, článek 3. Posuďte, zda student využil a správně citoval relevantní zdroje. Ověřte, zda jsou všechny převzaté prvky řádně odlišeny od vlastních výsledků, zda nedošlo k porušení citační etiky a zda jsou bibliografické citace úplné a v souladu s citačními zvyklostmi a normami. Zhodnoťte, zda převzatý software a jiná autorská díla, byly v ZP použity v souladu s licenčními podmínkami.	
<b>Komentář:</b> Písemná část práce je stručná, ale obsahuje všechny nezbytné části. Práci by prospělo obohatit kapitolu věnující se principům multivariační kryptografie o více příkladů a podrobnější vysvětlení.	
<b>Hodnotící kritérium:</b>	<b>Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):</b>
<b>3. Nepísemná část, přílohy</b>	<b>90 (A)</b>
<b>Popis kritéria:</b> Dle charakteru práce se případně vyjádřete k nepísemné části ZP. Například: SW dílo – kvalita vytvořeného programu a vhodnost a přiměřenost technologií, které byly využité od vývoje až po nasazení. HW – funkční vzorek – použité technologie a nástroje, Výzkumná a experimentální práce – opakovatelnost experimentů	
<b>Komentář:</b> Přílohou jsou jednak zdrojové kódy pro PC a pro mikrokontrolér ESP32, a také pracovní soubory pro Wolfram Mathematica s ukázkami principů podepisování, ověřování podpisu a generování klíčů pro vybraná schémata z multivariační kryptografie. Studentovi bych doporučil propříštit důsledně označovat autorství jím vytvořených souborů, není dobré se v tomto spoléhat jen na textovou část práce.	
<b>Hodnotící kritérium:</b>	<b>Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):</b>
<b>4. Hodnocení výsledků, jejich využitelnost</b>	<b>92 (A)</b>
<b>Popis kritéria:</b> Dle charakteru práce zhodnoťte možnosti nasazení výsledků práce v praxi nebo uveďte, zda výsledky ZP rozšiřují již publikované známé výsledky nebo přinášející zcela nové poznatky.	

*Komentář:*

Výsledkem je užitečný popis základních principů multivariační kryptografie, a dále srovnání implementačních aspektů vybraných schémat (LUOV a RB) jednak na PC, a také na vestavěné platformě ESP32. Srovnání s klasickými schématy RSA a ECDSA dává vodítko pro možnost nahrazení těchto schémat testovanými algoritmy postkvantové kryptografie i na platformách s omezenými prostředky jako je ESP32.

*Hodnotící kritérium:*

*Způsob hodnocení – následující škálou 1 až 5:*

**5. Aktivita a samostatnost studenta**

5a:

**1=výborná aktivita,**

2=velmi dobrá aktivita,

3=průměrná aktivita,

4=slabší, ale ještě dostatečná aktivita,

5=nedostatečná aktivita

5b:

1=výborná samostatnost,

**2=velmi dobrá samostatnost,**

3=průměrná samostatnost,

4=slabší, ale ještě dostatečná samostatnost,

5=nedostatečná samostatnost

*Popis kritéria:*

V souvislosti s průběhem a výsledkem práce posudte, zda byl student během řešení aktivní, zda dodržoval dohodnuté termíny, jestli své řešení průběžně konzultoval a zda byl na konzultace dostatečně připraven (5a). Posudte schopnost studenta samostatně tvůrčí práce (5b).

*Komentář:*

Student pravidelně konzultoval a byl vždy dostatečně připraven. S většinou překážek se vypořádal zcela samostatně a případně podněty od vedoucího práce adekvátně zapracoval.

*Hodnotící kritérium:*

*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*

**6. Celkové hodnocení**

91 (A)

*Popis kritéria:*

Shrňte stránky ZP, které nejvíce ovlivnily Vaše celkové hodnocení. Celkové hodnocení nemusí být aritmetickým průměrem či jinou hodnotou vypočtenou z hodnocení v předchozích jednotlivých kritériích. Obecně platí, že bezvadně splněné zadání je hodnoceno klasifikačním stupněm A.

*Text hodnocení:*

Student prokázal schopnost samostatné tvůrčí práce. Práci doporučuji k obhajobě a navrhuji klasifikovat výborně.

Podpis vedoucího práce: