



# Hodnocení vedoucího závěrečné práce

**Vedoucí práce:** prof. Ing. Róbert Lórencz, CSc.  
**Student:** Bc. Ivana Trummová  
**Název práce:** Analýza složitosti binárních algoritmů pro modulární inverzi  
**Obor / specializace:** Počítačová bezpečnost  
**Vytvořeno dne:** 29. května 2021

## Hodnotící kritéria

### 1. Splnění zadání

- ▶ [1] zadání splněno
- [2] zadání splněno s menšími výhradami
- [3] zadání splněno s většími výhradami
- [4] zadání nesplněno

Zadání bylo splněno bez výhrad. Všechny body v pokynech pro vypracování práce považuji za splněné.

### 2. Písemná část práce 97 /100 (A)

Předložená práce studentky je přehledná a dobře čitelná, prakticky bez chyb. Rozsah práce je v souladu s požadovaným rozsahem. Typografická a jazyková stránka je na velmi dobré úrovni. Uvedené zdroje jsou odpovídající obsahu práce. Práce obsahuje teoretický základ, požadovanou rešeršní část a dále provedenou analýzu příslušných algoritmů.

### 3. Nepísemná část, přílohy 100 /100 (A)

Příslušné experimenty byly realizované v jazyce C. Všechny experimentální výsledky je možné ověřit.

### 4. Hodnocení výsledků, jejich využitelnost 100 /100 (A)

Výsledky práce odpovídají plně zadání. Všechny vytvořené programy je možné použít pro další experimenty. Uvedené výsledky a závěry analýz jsou hodnotné pro další výzkum. Rovněž diplomantka provedla v práci korekci některých algoritmů, které byly publikovány a odkazují se na práce [1,2] ze zadání.

## 5. Aktivita studenta

- ▶ [1] **výborná aktivita**
- [2] velmi dobrá aktivita
- [3] průměrná aktivita
- [4] slabší, ale ještě dostatečná aktivita
- [5] nedostatečná aktivita

Aktivita diplomantky byla vysoká a odpovídala situaci a řešené problematice.

## 6. Samostatnost studenta

- ▶ [1] **výborná samostatnost**
- [2] velmi dobrá samostatnost
- [3] průměrná samostatnost
- [4] slabší, ale ještě dostatečná samostatnost
- [5] nedostatečná samostatnost

Se studentkou jsem absolvoval řadu konzultací, na kterých projevovala zájem o řešenou problematiku a odpovídající nasazení. Rovněž musím ocenit její samostatnost při řešení netriviálních problémů.

## Celkové hodnocení

100 /100 (A)

Diplomantka provedla kus dobré práce. V souladu se zadáním porovnála binární algoritmy řešící výpočet multiplikativní modulární inverze, které se odkazují na práce [1,2] v zadání. Výsledky analýz příslušných algoritmů jsou použitelné pro další výzkum v dané oblasti. Práci hodnotím plným počtem bodů i z důvodu diplomantkou prokázaných schopností provádět výzkum a to jak v oblasti rešeršní tak analytické.

## **Instrukce**

### **Splnění zadání**

Posudte, 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, posudte 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.

### **Písemná část práce**

Zhodnoťte přiměřenost rozsahu předložené ZP vzhledem k obsahu, tj. zda všechny části ZP jsou informačně bohaté a ZP neobsahuje zbytečné části. Dále posudte, 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. Posudte správnost používání formálních zápisů obsažených v práci. Posudte typografickou a jazykovou stránku ZP, viz Směrnice děkana č. 26/2017, článek 3.

Posudte, 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.

### **Nepísemná část, přílohy**

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.

### **Hodnocení výsledků, jejich využitelnost**

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.

### **Aktivita studenta**

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.

### **Samostatnost studenta**

V souvislosti s průběhem a výsledkem práce posudte schopnost studenta samostatně tvůrčí práce.

### **Celkové hodnocení**

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.