FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

# Hodnocení vedoucího závěrečné práce

| | |
|---|---|
| **Vedoucí práce:** | Mgr. Martin Jureček, Ph.D. |
| **Student:** | Bc. Jiří Soukup |
| **Název práce:** | Algebraická kryptoanalýza proudových šifer založených na LFSR |
| **Obor / specializace:** | Počítačová bezpečnost |
| **Vytvořeno dne:** | 9. května 2022 |

## Hodnotící kritéria

### 1. Splnění zadání

▸ [1] **zadání splněno**
[2] zadání splněno s menšími výhradami
[3] zadání splněno s většími výhradami
[4] zadání nesplněno

Všetky body zo zadania práce považujem za splnené.

### 2. Písemná část práce 98 / 100 (A)

Práca je dobre členená a má odpovedajúci rozsah. Uvedené zdroje sú relevantné k práci študenta. Teoretická aj praktická časť sú pekne spracované. Obzvlášť pomerne zložitý algoritmus F4 pre výpočet Groebnerových báz je vysvetlený veľmi podrobne.

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

Generovanie rovníc bolo naimplementované v jazyku Python a na výpočet Groebnerových báz sa využil software Magma. Súčasťou práce je užívateľská dokumentácia, na základe ktorej nebude zložité použiť študentov kód v nadväzujúcich prácach.

### 4. Hodnocení výsledků, jejich využitelnost 95 / 100 (A)

Študent sa zaoberal kryptoanalýzou pedagogických šifier, ktoré sa nevyužívajú v praxi. V priebehu práce sme uvažovali nad kryptoanalýzou šifry E0, ktorá sa používa v Bluetooth technológii, avšak práca by bola výrazne časovo náročnejšia. Študentovi sa podarilo prelomiť 72 bitový filter generátor používajúci vyváženú booleovskú šifru.

## 5. Aktivita studenta

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

Študent pravidelne konzultoval s vedúcim práce najnovšie výsledky a ďalšie kroky počas celého obdobia práce bez väčších časových okien.

## 6. Samostatnost studenta

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

Študent si samostatne naštudoval potrebnú teóriu o Groebnerových bázach. Ďalej sa zoznámil s algebraickým nástrojom Magma a dokázal ho spojiť so svojimi skriptami v Pythone a tak dokázal prevádzať šifry na sústavy polynomiálnych rovníc, ktoré potom následne riešil pomocou F4 algoritmu.

# Celkové hodnocení 98 /100 (A)

Práca je po teoretickej aj praktickej stránke dobre spracovaná. Študent bol schopný pochopiť relatívne zložitú teóriu a využiť ju v algebraickej kryptoanalýze až 72 bitovej prúdovej šifry. V prípade, že by študent mal k dispozícii viac času na diplomovú prácu, tak si myslím, že by sa dosiahli ešte výrazne lepšie výsledky. Vzhľadom k vyššie uvedeným bodom hodnotím prácu známkou A.

# Instrukce

## Splnění zadání

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.

## 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 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. 52/2021, 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.

## 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 posuďte, 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 posuďte schopnost studenta samostatné 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.