FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Hodnocení vedoucího závěrečné práce

Vedoucí práce:	Mgr. Olha Jurečková
Student:	Bc. Jiří Hájek
Název práce:	Testování náhodnosti proudové šifry Elephant
Obor / specializace:	Počítačová bezpečnost
Vytvořeno dne:	5. června 2023

Hodnotící kritéria

1. Splnění zadání

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

Všechny body ze zadání považuji za splněné.

2. Písemná část práce 90 /100 (A)

Práce je dobře členěna a má odpovídající rozsah. Seznam literatury obsahuje práce relevantní k tématu. Práce je dobře čitelná a obsahuje několik překlepů/chyb, např. v příkladu 1 v kap. 1, nebo vynechání absolutní hodnoty v příkladu 4.1.2.5. Jde však jenom o drobné nedostatky, které lze snadno odstranit a nijak výrazně neovlivňují srozumitelnost textu.

3. Nepísemná část, přílohy 90 /100 (A)

Implementace byla provedena v jazyce Python. Přiložené zdrojové kódy by mohly obsahovat více komentářů. Naměřené výsledky lze ověřit.

4. Hodnocení výsledků, jejich využitelnost 90 /100 (A)

Přínos studenta spočívá v otestování šifry Elephant pomocí monomiálních a kubických testů, což doteď nebylo nikde publikováno. Výsledky z kubických testů by mohly být použity u kryptoanalýzy šifry, což ale by bylo nad rámec zadání.

5. Aktivita studenta

[1] výborná aktivita

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

Student pracoval pravidelně bez větších přestávek a na emaily odpovídal poměrně rychle.

6. Samostatnost studenta

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

Student sám zvládl nastudovat potřebnou teorii a vyřešil technické problémy spojené s testováním šifry.

Celkové hodnocení 91 /100 (A)

Předložená diplomová práce je pomerně kvalitně zpracována. Student prokázal, že je schopen porozumět a naimplementovat monomiální a kubické testy, ve kterých dosáhl zajímavých výsledků. Oceňuji, že si student ke všem testům vymyslel vlastní příklady, které usnadňují pochopení teorie. Z těchto důvodů hodnotím práci 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.