Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

POSUDEK OPONENTA DIPLOMOVÉ PRÁCE

Student: **Bc. Martin Mikala** **Oponent:** **Ing. Jan Plucar, Ph.D.**

Studijní program: **Inženýrská informatika**
Studijní obor/Specializace: **Kybernetická bezpečnost**
Akademický rok: **2021/2022**

Téma diplomové práce: **Zero-knowledge protokol v kryptografii**

Hodnocení práce:

Předložená diplomová práce se zabývá studiem Zero-knowledge protokolů v kryptografii, což je aktuální a často diskutované téma. Zadání práce hodnotím jako technicky středně náročné. Student však musel věnovat poměrně velké množství času již vydané literatuře.

Body zadání rozdělují práci mezi část rešeršní a část praktickou. Rešeršní část je vypracována velmi detailně. Z textu lze poznat, že student diskutované problematice rozumí. Drobnou výtku mám k místy zbytečně dlouhému popisu dobře známých metod a technologií (například popis teorie Turingova stroje, kapitoly věnující se složitosti, atd.). Redukce textu vybraných teoretických částí by zvýšila čitelnost práce.

V praktické části student implementuje několik skriptů, které mají za úkol demonstrovat různé mechanismy fungování protokolů. Vzorové implementace jsou zvoleny správně a úroveň implementace odpovídá magisterskému stupni studia.

Po formální stránce je práce na dobré úrovni. Vytknout lze místy nižší kvalitu obrázků (např. obr 10.1. str 43). Studijní prameny odpovídají řešenému tématu. Student řádně odlišil převzaté myšlenky od svých.

Celkově hodnotím práci jako velmi zdařilou. Otázky k obhajobě nemám.

Celkové hodnocení práce:
Známku uvede oponent dle svého uvážení dle klasifikační stupnice ECTS:
A – výborně, B – velmi dobře, C – dobře, D – uspokojivě, E – dostatečně , F – nedostatečně.
Stupeň F znamená též „nedoporučuji práci k obhajobě“.

Předloženou diplomovou práci doporučuji k obhajobě a navrhuji hodnocení

A - výborně.

V případě hodnocení stupněm „F – nedostatečně“ uveďte do připomínek a slovního vyjádření hlavní nedostatky práce a důvody tohoto hodnocení.

Datum 1. 6. 2022 Podpis oponenta diplomové práce