VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Semestrální práce

magisterský navazující studijní program **Informační bezpečnost**

Ústav telekomunikací

Student: Bc. Samuel Kopecký ***ID:*** 211799

Ročník: 2 ***Akademický rok:*** 2022/23

NÁZEV TÉMATU:

Modulární komunikace postavená na postkvantové kryptografii

POKYNY PRO VYPRACOVÁNÍ:

Téma je zaměřeno na implementaci knihovny obsahující postkvantové algoritmy pro výměnu klíče, šifrovaní pomocí veřejného klíče a digitální podpis. Konkrétní výběr algoritmů pro implementaci a volba implementačního jazyka je na volbě studenta po předchozí konzultaci. Řešitel musí v rámci semestrální práce implementovat aspoň jeden algoritmus z vybrané kategorie. Výstupem SP bude funkční implementace algoritmu obsahující výkonové testování a porovnání s dostupným řešením.

Student v navazující diplomové práci implementuje vždy další jeden algoritmus z každé kategorie a pomocí vytvořené knihovny implementuje komunikaci klient-server, která bude využívat výhradně postkvantovou kryptografii. Klientská část aplikace bude obsahovat konsolové rozhraní, které bude umožňovat stáhnutí a nahrání souborů a výměnu zpráv s ostatními uživateli aplikace.
Dále student navrhne kompatibilní rozhraní, pomocí kterého je možné do aplikace klienta a serveru snadno přidat další postkvantové algoritmy. Práce bude taktéž obsahovat porovnání rychlosti a výkonnosti s ostatními implementacemi postkvantových algoritmů ve vybraném jazyce.

DOPORUČENÁ LITERATURA:

podle pokynů vedoucího práce

Termín zadání: 1.10.2022 ***Termín odevzdání:*** 12.12.2022

Vedoucí práce: Ing. David Smékal

doc. Ing. Jan Hajný, Ph.D.
předseda rady studijního programu

UPOZORNĚNÍ:

Autor semestrální práce nesmí při vytváření semestrální práce porušit autorská práva třetích osob, zejména nesmí zasahovat nedovoleným způsobem do cizích autorských práv osobnostních a musí si být plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č.40/2009 Sb.