

# Master's Thesis

Master's study program **Information Security**

Department of Telecommunications

**Student:** Bc. Samuel Kopecký

**ID:** 211799

**Year of  
study:** 2

**Academic year:** 2022/23

## TITLE OF THESIS:

**Modular network communication using post-quantum cryptography**

## INSTRUCTION:

The topic of the thesis is focused on the implementation of the library of post-quantum algorithms for key exchange, public key encryption and digital signature. The student implements at least one algorithm from the selected category.

In the diploma thesis, the student implements algorithm from each category and implements post-quantum client-server communication. The client part of the application will contain an API for downloading and uploading files and exchanging messages with other users.

The thesis will compare the speeds and performances with other implementations of post-quantum algorithms.

## RECOMMENDED LITERATURE:

Podle pokynů vedoucího práce

**Date of project  
specification:** 6.2.2023

**Deadline for  
submission:** 19.5.2023

**Supervisor:** Ing. David Smékal

**doc. Ing. Jan Hajný, Ph.D.**  
Chair of study program board

## WARNING:

The author of the Master's Thesis claims that by creating this thesis he/she did not infringe the rights of third persons and the personal and/or property rights of third persons were not subjected to derogatory treatment. The author is fully aware of the legal consequences of an infringement of provisions as per Section 11 and following of Act No 121/2000 Coll. on copyright and rights related to copyright and on amendments to some other laws (the Copyright Act) in the wording of subsequent directives including the possible criminal consequences as resulting from provisions of Part 2, Chapter VI, Article 4 of Criminal Code 40/2009 Coll.