BRNO UNIVERSITY OF TECHNOLOGY
FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

Semestral 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. The output of the semester project will be a functional implementation of the algorithm including performance testing and comparison with an existing solution.
In the diploma thesis, the student implements another 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: 1.10.2022 ***Deadline for submission:*** 12.12.2022

Supervisor: Ing. David Smékal

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