# POST-QUANTUM CRYPTOGRAPHY PROJECT

In the final project for the Cryptography course, you and your team will evaluate different aspects of the recently approved standard for Post-Quantum Cryptography [1].

As before, instead of coding these algorithms from scratch, you will leverage pre-existing implementations within the programming language of your choice, selecting suitable libraries that offer these implementations.

In this process, you need to research how these algorithm work, then how libraries are implemented, to later discuss how easy is to find them and use them. Then, you will create a program where you use them and evaluate how easy is to use them, how well documented are and, finally, how efficient they are.

The approved algorithms are:

- ML-KEM Scheme [2].
- ML-DSA Signature Scheme [3].
- SLH-DSA Signature Scheme [4].

Also, there are some libraries you can easily find like [5], [6] and [7], but if you research, you can find more.

The sections required for this report are presented along with a short description of what it is expected to be presented. Also, you and your team should check the rubric on the canvas assignment where you will upload this report. Remember to upload a PDF file along with the code of your project.

**References**

[1]. Comments Requested on Three Draft FIPS for Post-Quantum Cryptography, https://csrc.nist.gov/Projects/post-quantum-cryptography

[2]. Draft FIPS 203, Module-Lattice-Based Key-Encapsulation Mechanism Standard, https://doi.org/10.6028/NIST.FIPS.203.ipd

[3]. Draft FIPS 204, Module-Lattice-Based Digital Signature Standard, https://doi.org/10.6028/NIST.FIPS.204.ipd

[4]. Draft FIPS 205, Stateless Hash-Based Digital Signature Standard, https://doi.org/10.6028/NIST.FIPS.205.ipd

[5]. PQCRYPTO, https://libpqcrypto.org/python.html

[6]. Open Quantum Safe (OQS) project, https://github.com/open-quantum-safe/liboqs/

[7]. Python 3 bindings for liboqs, https://github.com/open-quantum-safe/liboqs-python

## PRELIMINARIES

- Title page
- Contents

## MAIN PART

- Introduction
  - Problem description: Post-Quantum Cryptography Standards are ready to be used?
  - Motivation: Why we want to solve that problem (what will be better if we solve it)
- Background
  - Post-Quantum Cryptography Standards
    - ML-KEM Scheme
    - ML-DSA Signature Scheme
    - SLH-DSA Signature Scheme
  - Post-Quantum Cryptography libraries (explain the libraries you use)
- Methodology
  - Explain how you will evaluate:
    - How easy is to use the libraries.
    - How well documented libraries are.
    - That you will create a program to evaluate how efficient the libraries are.
  - Technical description of your program.
- Findings/results
  - Discuss the results of your evaluation focusing on how mature these algorithms are to use them in a system development.
- Conclusions and recommendations
  - Conclude with what you did, how you did it, results, and benefits. If there any disadvantages of what you present, discuss them, and give recommendations.

## SUPPLEMENTARY

- References/bibliography