Module Lattice Based Key Encapsulation Mechanism

Module-Lattice-Based Key-Encapsulation Mechanism Standard NIST requests comments on three draft Federal Information Processing Standards (FIPS):

   FIPS 203, Module-Lattice-Based Key-Encapsulation Mechanism Standard

   FIPS 204, Module-Lattice-Based Digital Signature Standard

   FIPS 205, Stateless Hash-Based Digital Signature Standard

These proposed standards specify key establishment and digital signature schemes that are designed to resist future attacks by quantum computers, which threaten the security of current standards. The three algorithms specified in these standards are each derived from different submissions to the NIST Post-Quantum Cryptography Standardization Project.

a) Write a short code to accomplish these standards

b) What steps needs by CA to accommodate these standards

**N.B. If you need to submit your developed code or other materials, please upload the materials in google drive/github and provide the link in your PDF file.**