UAB COLLEGE OF ARTS AND SCIENCES
The University of Alabama at Birmingham

Department of Computer Science

CS 645/745: Modern Cryptography
Instructor: Dr. Yuliang Zheng

OpenSSL and Post Quantum OpenSSL

OpenSSL is the most widely used library for TLS (https://www.openssl.org/). OQS-OpenSSL from Open Quantum Safe is a new library that extends OpenSSL to include post quantum (PQ) capabilities (https://openquantumsafe.org/applications/tls.html#oqs-openssl).

The goal of this assignment is to develop knowledge and skills to use OpenSSL as well as OQS-OpenSSL. Although the libraries work on a variety of platforms including Windows, Mac OS and Linux, students are required to complete this assignment in either a Mac or Linux environment. If you use a Windows PC, you can install a Linux distribution inside VMware or simply turn on Windows Subsystem for Linux.

Note that VMware Workstation Player is available to UAB students for free:
https://www.uab.edu/it/home/
> Software > VMware Academic Software

Part I. OpenSSL

Students are to follow the guide below to complete this part of the assignment

- "OpenSSL Cookbook" by Ivan Ristic (https://www.feistyduck.com/library/openssl-cookbook/),

You will

1. Build and install the latest version of OpenSSL from source code (not binaries), if it's not already installed
2. Generate public-private key pairs and certificates; select your desired cipher suites
3. Create a private certification authority (see Chapter 1.5 of "OpenSSL Cookbook")
4. Test with OpenSSL (Chapter 2 of "OpenSSL Cookbook")
    a. Use www.cnn.com as a known SSL server

Part II. OQS-OpenSSL

Repeat the above exercise with OQS-OpenSSL. Specifically,

1. Build and install the latest version of OQS-OpenSSL from source code (not binaries)
2. Generate PQ public-private key pairs and certificates; select your desired cipher suites
3. Create a PQ private certification authority (similar to Chapter 1.5 of "OpenSSL Cookbook")
4. Test with OpenSSL (similar to Chapter 2 of "OpenSSL Cookbook")
    a. Use test.openquantumsafe.org with an appropriate port number as a known PQ SSL server. See the following page for more info: https://test.openquantumsafe.org/

Submit

A written report showing that you have mastered techniques for

1. Building and installing the latest versions of OpenSSL (if not already installed) and OQS-OpenSSL from source code (not binaries)
2. Creating a private certification authority and a PQ private certification authority
3. Testing with OpenSSL and OQS-OpenSSL

Screenshots of live runs are to be included, although they should not be overused in completing your report.