# CSCE4013/5013 Homework 6 (Programming)

**Due date: November 19, 2018**

**Full Grade: 100 pts**

## I. Task Description

In this assignment, you need to implement a Merkle hash tree, and use it to authenticate messages between sender Alice and receiver Bob. For this assignment, the digital signature scheme should use RSA; hash function should use SHA-256.

**Part 1:** Implement the Merkle hash tree and generate extended signature at the sender Alice. The sender's program should take 8 manually input messages from the command line. Each message will have 4 English letters or less. Then build a Merkle tree from these 8 messages, and generate a digital signature for the root of the tree. Print the tree root to the screen.

Now the sender's program should let the user to manually choose one of the 8 messages via the command line. Then it generates the *extended signature* for the chosen message, which includes the correct hash values and the digital signature for the tree root. It writes the message as well as the extended signature into a file named sig.txt.

Before the receiver verifies the message and signature, your program should give the user a chance to read the file sig.txt and change its content if the user wants to. This is to simulate a modification attack to the message.

**Part 2:** Verify the extended signature at the receiver Bob. The receiver's program reads the message and the extended signature from sig.txt. Then it verifies whether the extended signature is valid or not. Print the reconstructed tree root to the screen. And print the verification result, success or failure, to the screen.

## II. Tests

You need to demo your program to the instructor. A demo sign-up sheet will be distributed in class later. During the demo, your program will be tested as described above.

## III. Other Instructions

Any programming language is fine.

Submit your source code, your **executable**, and necessary support files to Blackboard as a .zip file named in this format: HW6.YourLastName.YourFirstName.zip.