Homework 3

- Honor Code: You must work completely independently on this assignment. Do not discuss the questions or answers with each other before the assignment is due. Any breach of the honor code will be handled per the University's policy on academic honesty.
- Follow the instructions very careful. Answers that do not conform to the instructions will not be given credit.
- Submit your solutions through Blackboard. Include all code you write for this lab in a zip or tar.gz file.
- Understand all the code given to you in this lab. Search for documentation online if there is a primitive or API you have not encountered before. You are not responsible for understanding the underlying mathematics behind the cryptographic primitives. However, you are responsible for using these primitives in an application in a secure manner.
- Use Java 8.
- Only use the external Java libraries provided to you in the lab.

In this lab, you will implement the ScroogeCoin cryptocurrency. You will act as Scrooge and verify transactions sent to you by users and add them to your ledger.

Your submission will only be the DefaultScroogeCoinServer.java class. Do not modify any of the other existing classes, as the auto-grading script will use the original implementations of all the other classes.

Your grade will be based entirely on the percent of test cases passed.

A few JUnit test cases have been given to you as sanity checks on your code, but the grading will be based different test cases. You should invest time in developing your own test cases.

In this lab, you will implement a ScroogeCoin application server.

Assume the following about the server:

1. Has the URL is https://scroogecoin.com.

2. Only accepts connections over HTTPS.

3. Has a valid SSL certificate.

4. Does not authenticate any users, include Scrooge.

5. Scrooge is the only person in control of the server.

These assumptions enable users to trust that any response they receive from the server is authorized by Scrooge. However, because the server does not authenticate users, your implementation will need to rely on digital signatures to process transactions securely. Scrooge runs the server and then submits transactions to the server through a web browser, like any other user.

Implement the following methods per the comments in the DefaultScroogeServer.java class file.

```
DefaultScroogeServer.init(KeyPair)

DefaultScroogeServer.epochHandler(List<Transaction>)

DefaultScroogeServer.isValid(Transaction)

DefaultScroogeServer.getUTXOs()
```