German University in Cairo

Faculty of MET (CSEN 1001 Computer and Network Security Course)

Dr. Amr El Mougy
Reham Ayman
Abdelrahman Osama

Project Description

Deadline: 11:59pm Saturday 30 of May

Guidelines

This project should be done **individually or in team of two**. You can share ideas, consult the TA, and search online. **However, all work done in this project must be done individually or by all team members**.

The main aim of this project is to test your knowledge of the security concepts taught in this course.

Teams have to implement the Extra Required Deliverables for Teams in addition to the General Deliverables.

All external assets used from the internet must be credited and commented in your project.

Any plagiarism detected will be penalized with a zero.

You are free to use any programming language.

Submission

- Final submission due to Saturday**, May 30th, 2020** via MET Website.
- Submit a .Zip file containing your project. The Zip file naming format should be the following **[ID] [TutoiralNumber] (e.g. [37 - 1111] [T01]**
- In case there was a problem in the submission through the MET website, then send an email to your TA with the title same as the name of the Zip file.
- **If you are working in a team, include a Readme file containing the team members' names, IDs and Tutorial number.**

German University in Cairo

Faculty of MET (CSEN 1001 Computer and Network Security Course)

Dr. Amr El Mougy
Reham Ayman
Abdelrahman Osama

Description

What is the main Idea?

In this project, we will design a cryptocurrency similar to ScroogeCoin. A network of **100** users will simulate the transaction processes. Initially each user will have **10** ScroogCoins. As long as the system is running, a random transaction with random amount (within the range of amount the user has) will be created from User **A** to User **B**. The transaction is signed by the private-key of the sender. Scrooge get notified by every transaction. Scrooge verifies the signature before accumulating the transaction. Once Scrooge accumulates **10** transaction, he can form a block and attach it to the blockchain. **You are allowed to use predefined hash and digital signature libraries. Mention which libraries you used.**

General Deliverables

- A designated entity “Scrooge” publishes an append-only ledger that contains all the history of transactions.
- The ledger is a blockchain, where each block contains transactions, its ID, the hash of the block, and a hash pointer to the previous block. The final hash pointer is signed by Scrooge.
- A simulation of the network, with multiple users and the randomized process of making a transaction, making each transaction reach an arbitrary user.
- The design and implementation of the ledger based on the concept of the blockchain (hash linked list).
- Upon detecting any transaction, scrooge verifies it by making sure the coin really belongs to the owner **and it has not been spent before**.
- If verified, Scrooge adds the transaction to the blockchain. Double spending can only happen before the transaction is published.
- For digital signature, use any of the technique described throughout the course.

German University in Cairo

Faculty of MET (CSEN 1001 Computer and Network Security Course)

Dr. Amr El Mougy
Reham Ayman
Abdelrahman Osama

Extra Required Deliverables (for Teams)

- ❖ Implement Merkel Tree for the blockchain you create. The Merkel Tree should reflect the change in the blockchain when adding a new block to the blockchain.
- ❖ Transaction verification **using Merkel Tree** to make sure that the coins are not spent before by the same user.

Output Format

- ❖ Print initially the public key and the amount of coins for each user.
- ❖ Scoorge should print the block under construction for each new transaction added (include the transaction details).
- ❖ Print the blockchain after a new block is appended.
- ❖ Terminate the code using the key ‘Space’.
- ❖ Save all the printed data to a text file upon termination.