Reichman University: Blockchains and Cryptocurrencies

Exercise 1

Assigned: November 23, 2022 Due: December 7, 2022

General Instructions

How to Submit The homework exercise has two parts:

1. Question 1 requires you to write a formal proof, and its answer should be submitted via the course Moodle by uploading a PDF file. **The submitted homework must be typed** (not hand-written and scanned).

   You will receive a 2 point bonus for the exercise if your submission was prepared in LaTeX, and contains the LaTeX macro in a footnote. You can download a latex homework template to get you started. If you don't want to install latex locally, there are online latex editors such as Overleaf that you can use.

2. Questions 2 to 4 are coding questions and should be submitted via the Inginious Server.

Pair Submission You are encouraged to solve the **theory part** of this exercise in pairs. To register your pair, write your partner's name and inginious username at the top of the page you submit. When you solve in a pair, each member of the pair should submit the solution independently, but you and your partner may submit identical solutions.

Note that the *Inginious* part of the assignment should not be submitted in pairs (you are welcome to discuss solutions with your classmates, but don't copy code).

Homework Questions

1. (40 points) **(Dolev-Strong: Validity)** In class we proved the *consistency* of Dolev-Strong. Prove the *validity* of the protocol. I.e., if the sender is honest, then all honest parties will output the sender's input bit. (This is exercise 2 in Elaine's book.)

2. (5 points) **(Signatures)** Solve the Digital Signatures task on Inginious (this was a task we did in class).

3. (5 points) **(Byzantine Generals)** Solve the Byzantine Generals task on Inginious (this was a task we did in class).

4. (50 points) **(Dolev-Strong)** Solve the Dolev-Strong task on Inginious (this is a new task).