EE374 Blockchain Infrastructure **Stanford, Spring 2025**

Homework #2

Due: Fri, April-18-2025, 11:59pm – Gradescope entry code: `R57ZN7`

Please upload your answers timely to Gradescope. Start a new page for every problem. We strongly suggest LaTeX to type your answers. For the programming/simulation questions you can use any reasonable programming language (please no assembly, brainfuck, etc. ☺). Comment your source code and include the code and a brief overall explanation with your answers. A tentative point distribution (in % of the total) is provided in brackets. For most problems there is more than one valid way of solving them!

1. (20%) Hash functions.
   a) State the random oracle model for hash functions.
   b) Look at the following hash of a recent Bitcoin block:
   00000000000000000000009942393c797d6d0bff9e88bc1ae84a3d7e7546f46f61
   How many attempts did the network approximately require to mine this block under the random oracle model?
   c) State the collision resistance property of hash functions.
   d) Argue that a hash function under the random oracle model is collision resistant.
2. (10%) Explain the key differences between the accounts model and Bitcoin's UTXO model.
3. (20%) Answer the following questions.
   a) **What's the output of the following script if the input is 7? What function does it implement?**

```
<7>
OP_DUP
OP_DUP
OP_ADD
OP_DUP
OP_ADD
OP_ADD
```

   b) **What's the output of the following script? What function does it implement?**

```
<11>
<3>
OP_2DUP
OP_MAX
OP_TOALTSTACK
OP_MIN
OP_FROMALTSTACK
```

Hint: You can use https://ide.scriptwiz.app to verify your answers.

4. (15%) Parse the following Bitcoin transaction and write it in the format stated here: https://gist.github.com/RobinLinus/7971daeb88ecd939825bc456721d9378

```
01000000018e70ee5afa829e776d006cdb340c79029e95d9bdd059751590196
97172e944ea000000008a4730440220694ff325724a4f4b0f3f0c36bf8e94ca
c58ad7c9b4d5bd8c7286c0da623f0b2c02206ae94680a8f31f30cd846da258e
919c94afe2dd629b4f4ce11bbe8165ff99a5f014104fc60372d27b067ca306b
a812ced9c8cd69296b83a40b9b57c593258c1b9e0ee1c0c621ca558b878395f
9645a4b67a96e51843e9c060d43a3833fdd29a91f4f31ffffffff0200e1f505
000000001976a914f369e8330a1e9a349721c3d790ae4d38b68e525288ac00e
9a435000000001976a914f10eb3bfce5ab24537e571ceb3862d2949f7c5e288
ac00000000
```

Hint: You can find the data model of Bitcoin transactions here https://gist.github.com/RobinLinus/7971daeb88ecd939825bc456721d9378

5. (35%) According to Figure 7 of lecture note #2, the mining pool *F2Pool* has about 20% of the total hash rate of the current Bitcoin network.

   a) What is the distribution of the time we need to wait until a block is mined by *F2Pool*? Justify your answer.

   b) What is the probability that the next block mined is from *F2Pool*? Justify your answer.

   c) At the end of Lecture 2, we consider an attack on the confirmation rule where a transaction enters the ledger as soon as its block enters the longest chain. Alice's transaction is in a block B and she is trying to mine two blocks in private before the honest miners are able to mine a new block on B, so as to remove the transaction from the ledger. Suppose *F2Pool* is trying to perform this attack. What is the probability it will succeed? You can assume the attacker starts mining the private blocks as soon as the transaction enters the mempool, and that the transaction will be in the next block mined by the network. Make explicit any other assumptions you are making in deriving the answer.