CS 435 : Intro to Cryptography **Fall 2020**

Homework 7

Professor Somesh Jha **Due:** Dec 3

Q 2-4 are each worth 30 points.

1. You will get 10 points for attending the talk.
2. Describe your thoughts about the talk. What topics were covered? What was your favorite topic covered in the talk? General impressions?
3. Describe the PBFT protocol by Castro-Liskov described in the talk. How are digital signatures used in the protocol? How many faults can the protocol withstand?
4. Describe the use of hash functions in proof-of-work (POW) in crypto-currencies. Analyze this construction using the random-oracle model of hash functions.