Blockchain (UE20CS335)

Open book assignment 2

1. The RSA Algorithm: Given p=13, q= 31, d = 7, What should be the value of e?
2. The Diffie Hellman algorithm: Alice and Bob have chosen prime value q = 17 and primitive root = 5. If Alice's secret key is 4 and Bob's secret key is 6, what is the secret key they exchanged? Explain.
3. What is distributed consensus? How that can be guaranteed in blockchain?
4. What are the advantages and disadvantages of using PoS over PoW.
5. If you have to choose, which society do you support: The PoW or The PoS? Please give a clear reason to justify your thoughts.
6. What is the role of SGX technology in proof of elapsed time?
7. Can Proof of authority be used in public blockchain setup? Justify.
8. Why is it difficult to become a validator in Proof of authority? What are the requirements for becoming a validator node?
9. In hashing, what is the difference between strong and weak collision?
10. What has happened in "The DAO story"? Which type of forking took place to make the system correct?
11. Proof of Space is used by SpaceMint. True /false? If true, how are they using Proof of space in their setup?
12. Paxos and RAFT gives assurance of liveness or safety. Comment.
13. It is given in literature that in blockchain setup, it is better to use PBFT than BFT. Why?
14. What is the difference between Pre-prepare, Prepare and Commit stage of PBFT?
15. Can two consensuses be merged? Give an example to justify.