NOC22-CS44: Blockchain and Its Applications
Assignment 2

Correct choices are highlighted in Yellow. Give partial marks for partially correct answers.

1. Let Bob wants to send a long message to Alice. Alice should be able to confirm that it was indeed sent by Bob, and Bob later cannot deny that he had sent the message. They also want that nobody else should be able to see its content. Alice and Bob plan to use public key cryptography and cryptographic hashing techniques. Let the key pairs of Alice and Bob be (Pub A, Pri A) and (Pub B, Pri B), respectively. Let E, D and H be the encryption, decryption and hash functions, respectively. Let M denote the Message and H(M) its digest. Which of the following describes the correct order of steps to be used by Alice to send the digitally signed message.
   i. At Bob: M' = E(M, K_{pubA})
   ii. At Alice: M = E(M', K_{priA})
   iii. Bob sends the message M' to Alice
   iv. The signature along with the message is sent to Alice (M, M')
   v. Bob: M' = E(M, K_{priB})
   vi. Signing the message with his private key: S = E(H(M), K_{priB})
   vii. M = E(M', K_{pubB})

   a. i, iii, ii, v, iv, vii, vi
   b. i, ii, iii, iv, v, vi, vii
   c. v, vii, ii, i, iii, iv, vi
   d. vii, vi, v, iv, iii, ii, i

2. Digitally signing transactions by sender in Blockchain does not ensure to solve repudiation/ verifiability problems. Is the above statement True or False?
   a. True
   b. False

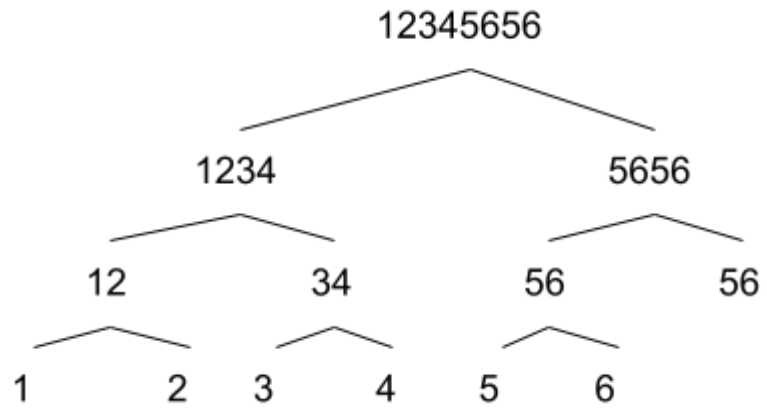
3. Which of the following is used to point a block in blockchain:
   a. Hash Pointer
   b. User ID
   c. Transaction ID
   d. Timestamp

Hint: Refer to the Week 1 Slide for Hash Pointer

4. Suppose you have 6 data points -- 1 to 6. The post-order traversal of the Merkle Tree is given by (here 8 means hash of 8, 43 means the combined hash of 4 and 3, and so on):
   a. {12345656, 1234, 5656, 12, 34, 56, 56, 1, 2, 3, 4, 5, 6}
   b. {1, 12, 2, 3, 4, 34, 1234, 5, 6, 56, 123456}
   c. {1, 2, 12, 3, 4, 34, 1234, 5, 6, 56, 78, 5678, 12345678}

d. {1, 2, 12, 3, 4, 34, 1234, 5, 6, 56, 56, 5656, 12345656}

Hint:



Post order Traversal : {1, 2, 12, 3, 4, 34, 1234, 5, 6, 56, 56, 5656, 12345656}

5. Which of the following is true for using a digital signature in blockchain?
   a. To check the validity of the source of a transactions
   b. None of the above.
   c. It will ensures that no one can deny of their own transaction
   d. It supports user authentication

Hint: Refer to Week 2 Slide for Digital Signature.

6. Which are the main Consensus Algorithms?
   a. Proof of Work
   b. Proof of Wager
   c. Proof of Stake
   d. Proof of Mining

Hint: PoW and Pos are the main consensus algorithms

7. Why is consensus hard in asynchronous system?

   I. No notion of global time

   II. faults in network

   III. nodes may crash/ faulty nodes

   a. II, III

   b. I, II

   c. I, III

   d. I, II, II

Hint: Due to lack of global timing reference,various kinds of faults it is very difficult to come to agreement between nodes unanimously.

8. Liveliness property ensures the output should be produced within a finite time limit?

a. False
b. True

Hint: Refer to Week 2 Slide, liveliness property talks about eventual termination.

9. Paxos consensus support(s) which of the below properties
    a. Liveliness
    b. Safety
    c. Both
    d. None of the above

Hint: Refer to Week 2 Slide, Paxos supports safety but not liveliness.

10. Which is/are true for Raft consensus?
    a. Crash Fault Tolerant
    b. Byzantine Fault Tolerant
    c. Both
    d. None of the above

Hint: Raft does not support byzantine fault tolerance in basic form.