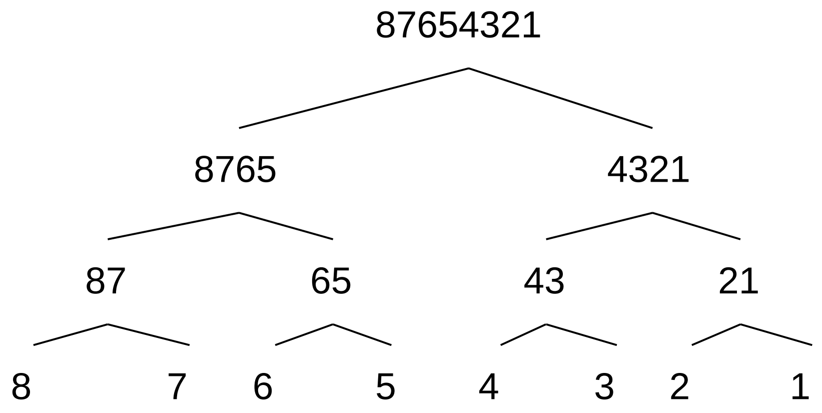
NOC22-CS44: Blockchain and Its Applications
Assignment 2

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

1. Suppose you have eight data points -- 8 to 1. 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. {8, 7, 87, 6, 5, 65, 8764, 4, 3, 43, 2, 1, 21, 4321, 87654321}
   b. {8, 87, 7, 8764, 6, 65, 5, 87654321, 4, 43, 3, 4321, 2, 21, 1}
   c. {1, 2, 12, 3, 4, 34, 1234, 5, 6, 56, 7, 8, 78, 5678, 12345678}
   d. {87654321, 8765, 87, 8, 7, 65, 6, 5, 4321, 43, 4, 3, 21, 2, 1}

Hint:



Post order Traversal : {8, 7, 87, 6, 5, 65, 8764, 4, 3, 43, 2, 1, 21, 4321, 87654321}

2. 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

3. Digital signing of a transaction or document involves hashing the content of the document and then _____.
   a. encrypting it with private key
   b. encrypting it with public key
   c. encrypting it with nonce
   d. rehashing it

Hint: In Digital Signature the message is signed using the Private key and it is verified using the Public key

4. What is the objective of using a digital signature?
    a. It supports the integrity of messages
    b. None of the above.
    c. It supports both user authentication and integrity of messages
    d. It supports user authentication

Hint: Refer to Week 2 Slide for Digital Signature.

5. 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

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

Hint: Refer to Week 2 Slide for Consensus Algorithm

7. Which statement(s) is correct for Fischer-Lynch-Paterson impossibility result:
    I. Consensus is impossible with even a single faulty node?
    II. Ensures safety and liveness together
        a. Both are correct
        b. Only I
        c. Only II
        d. Both are incorrect

Hint: Refer to Week 2 Slide for Distributed Consensus. FLP Impossibility Theorem cannot ensure " Safety " and Liveness " together

8. Why is consensus hard?
    I. No notion of global time
    II. faults in network
    III. nodes may crash/ faulty nodes
        a. I, II, II
        b. I, II
        c. I, III
        d. II, III

Hint: Refer to Week 2 Slide

9. In a RSA cryptosystem Alice uses two prime numbers p = 7 and q =17 to generate her public and private keys. If the public key of Alice is 11. Then the private key of Alice is ____________.

    Ans: Numerical Answer Type - 35

Hint: In an RSA cryptosystem, for public key: GCD(ϕ(n) , e) = 1
And, for private key: (e * d) mod ϕ(n) = 1
Where,
ϕ(n) = (p -1)*(q – 1) = (7 – 1)(17 – 1) =6*16 = 96
Such that 1 < e, d < ϕ(n)

Therefore, the private key is:
$(11 * d) \bmod \phi(n) = 1$

$\Rightarrow d = 35$

10. A popular public-private key implementation known as Rivest-Shamir-Adelman (RSA) algorithm is used for the Bitcoin and Ethereum Blockchain. True or False?
    a. True
    b. False

Hint: Bitcoin uses Elliptic Curve Digital Signature Algorithm