Course Name: Blockchain and its Applications (NOC25_CS08)

Assignment 2 - Week 2 (Jan 2025)

TYPE OF QUESTION: MCQ/MSQ

Number of questions: 10 **Total mark: 10 X 1 = 10**

QUESTION 1

Alice employs the RSA cryptosystem with the prime numbers p=11 and q=19 to derive her public and private keys. Given that her public key is e=11, what is her corresponding private key d?

a) 35
b) 131
c) 101
d) 149

Answer: (b)

Detailed solution:
Compute $\phi(n)=(p-1)(q-1)=180$.
Find d as the modular inverse of $e=11$ modulo $\phi(n)=180$ using $d = e^{-1} \pmod{180}$, giving $d=131$

QUESTION 2

Alice wants to send a message to Bob with **confidentiality** and **integrity**. The steps are as follows:

1. Alice encrypts the message using Bob's _____ key.
2. Alice then signs the _____ of the message with her _____ key.
3. Bob decrypts the message using his _____ key.
4. Bob verifies Alice's signature using her _____ key.

a) public, hash, private, public, private
b) private, message, public, private, public
c) public, hash, private, private, public
d) public, hash, private, public, public

Answer: (c)

Detailed solution:
Alice first encrypts the message using Bob's public key for confidentiality and signs the hash of the message with her private key to ensure integrity and authenticity. Bob then decrypts the message with his private key and verifies Alice's signature using her public key to confirm the message's authenticity and integrity.

QUESTION 3

Digitally signing transactions by the sender in Blockchain ensures the resolution of repudiation/verifiability problems. Based on this, which one of the following is correct:

a) It allows the sender to deny the transaction at any point.
b) It ensures that the sender cannot deny the transaction and the recipient can verify its authenticity.
c) It provides encryption but does not verify the sender's identity.
d) It guarantees the transaction will remain confidential but does not resolve repudiation issues.

Answer: (b)

Detailed solution:
Digital signatures in blockchain ensure that the sender cannot deny sending the transaction (non-repudiation) and that the recipient can verify the authenticity and integrity of the transaction (verifiability).

QUESTION 4

What is the primary purpose of Alice signing a message with her **private key** in a blockchain transaction?

a) To encrypt the message
b) To prevent others from reading the message
c) To prove the message came from Alice
d) To hide the contents of the message

Answer: (c)

Detailed solution:
When Alice signs a message with her **private key**, it serves as proof that the message came from her (authentication) and ensures the integrity of the message (it hasn't been tampered with).

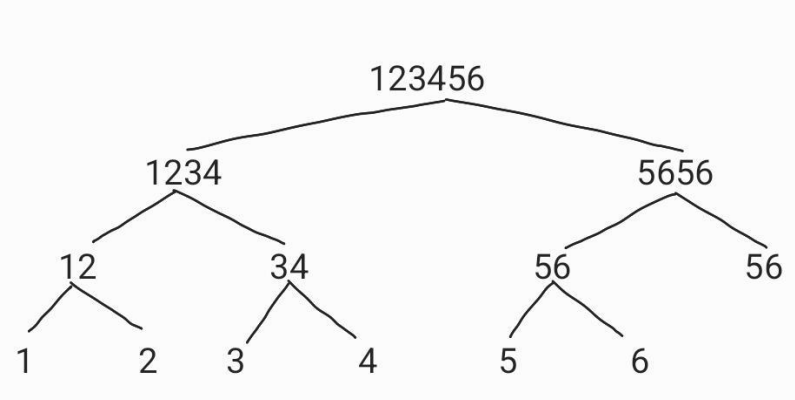
QUESTION 5

Consider 6 data points labeled 1 to 6. The post-order traversal of the Merkle Tree is provided as follows (where 1 represents the hash of data point 1, 43 denotes the combined hash of 4 and 3, and so on):

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

Answer: (c)

Detailed solution:



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

QUESTION 6

Which of the following is used to refer to a block in a blockchain?

a) Future nonce
b) Block size
c) Previous Block Hash
d) Transaction Timestamp

Answer: (c)

Detailed solution:
In a blockchain, each block contains a **previous block hash**. This hash pointer links the current block to the previous one, ensuring the integrity and immutability of the blockchain.

QUESTION 7

Which of the following **does not align** with the primary design goals of cryptocurrency development?

a) Decentralization of control and decision-making
b) Immutability of transaction records
c) Centralized control over transactions
d) Transparency and accessibility of transaction data

Answer: (c)

Detailed solution:
Centralized control over transactions: This contradicts the essence of cryptocurrencies, which are designed to operate without central authority or intermediaries.

QUESTION 8

Which of the following statements is/are **true** regarding **Bitcoin** and its **consensus algorithm**?

1. Bitcoin uses Proof of Work (PoW) for transaction validation and block addition.
2. Bitcoin operates on a peer-to-peer (P2P) network.
3. Bitcoin uses Proof of Stake (PoS) for centralization.
4. Miners are rewarded with transaction fees and block rewards in Bitcoin.

a) 1, 2, 3
b) 2, 3, 4
c) 1, 2, 4
d) 1, 3, 4

Answer: (c)

Detailed solution:
Bitcoin uses Proof of Work (PoW) for consensus, where miners solve cryptographic puzzles to validate transactions and add blocks to the blockchain. The network operates on a decentralized peer-to-peer (P2P) model, with no central server, allowing nodes to communicate directly. Miners are incentivized with transaction fees and block rewards for securing the network by validating and adding blocks.

QUESTION 9

What is the primary focus of 'safety' in Bitcoin's protocol?

a) Preventing invalid transactions
b) Ensuring blocks are mined quickly
c) Guaranteeing that only some of the transactions are private
d) Maximizing the number of transactions per block

Answer: (a)

Detailed solution:
In Bitcoin, **safety** ensures the integrity of the blockchain by preventing invalid transactions, such as double-spending.

QUESTION 10

Which of the following is the primary goal of a consensus algorithm in a distributed system?

a) To ensure that all nodes process transactions at the same speed
b) To guarantee that all nodes in the system agree on a single value or state
c) To minimize the number of nodes required for network communication
d) To prevent malicious attacks by encrypting all data transmitted between nodes

Answer: (b)

Detailed solution:
The primary goal of a **consensus algorithm** is to ensure that all nodes in a distributed system agree on a single value or state, even if some nodes may fail or act maliciously. This is crucial for maintaining consistency and reliability across the system.