National Forensic Sciences University
School of Cyber Security and Digital Forensics

Course Name: M.Sc. Cyber Security (Batch: 2022-24)

Semester – III

Subject Code: CTMSCS SIII P1Time: 03.30pm to 5.00 pm

Subject Name: Blockchain and Cryptocurrencies **Date:** 30-10-2023

Exam: Mid Semester Examination (October - 2023)

Q1. What is the primary purpose of a Merkle Tree in a blockchain?

a) To secure private keys and digital assets.
b) To encrypt all transactions in the blockchain.
c) To efficiently verify the integrity of transactions in a block.
d) To mine new cryptocurrency coins.

1 marks

Q2. In the context of blockchain, what is the main role of ECDSA?

a) To store and distribute digital assets.
b) To achieve distributed consensus among nodes.
c) To create and verify digital signatures for transactions.
d) To encrypt communication between nodes.

1 marks

Q3. What is the primary function of a private key in the context of digital signatures?

a) To verify the authenticity of a message.
b) To encrypt the message content.
c) To create a digital signature for a message.
d) To ensure the message's confidentiality.

1 marks

Q4. What is Nakamoto Consensus in the context of blockchain?

1 marks

a) A mathematical puzzle miners solve to add blocks to the blockchain.
b) A consensus mechanism used to agree on the blockchain's state.
c) A form of asymmetric cryptography used for security.
d) A decentralized exchange for cryptocurrencies.

Q5. Write short notes on the following

6 mark

(a) Zero-knowledge Proof
(b) Byzantine General Problem

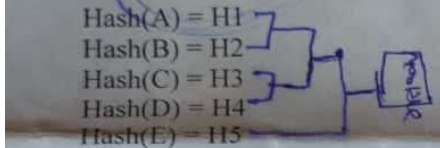
Q6. Consider a hypothetical blockchain where the target time for mining a block is set at 3 seconds. The previous block had a target value of 2000000. The actual time it took to m the previous block was 250 seconds. Calculate the new target value for the next block.

marks

Five

Q7. You are constructing a Merkle Tree for a set of four transactions blocks: Block A, Block B, Block C, Block D and Block E. Each block is hashed individually to create the leaf nodes of the Merkle Tree. The hash values for the leaf nodes are as follows:

Hash(A) = H1
Hash(B) = H2
Hash(C) = H3
Hash(D) = H4
Hash(E) = H5



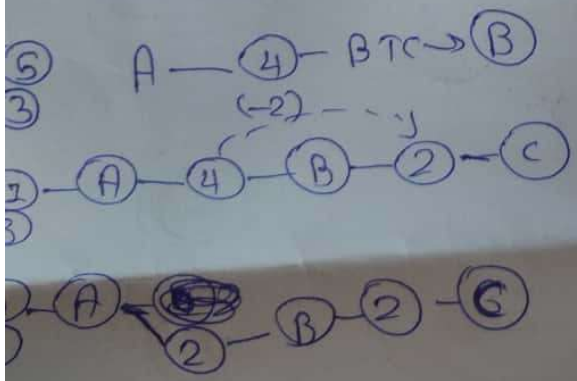
Construct the Merkle Tree by calculating the hash values for the intermediate nodes and finally the root node. For concatenation operation use || symbol. Show your work step by step. **5marks**

Q8. Compare hard-fork and soft-fork in detail with examples. **5 marks**

Q9. Define Blockchain. Differentiate between public and private blockchain. **5 marks**

Q10.Explain the concept of Proof of Work (PoW) and Proof of Stake (PoS) as a consensus mechanism in blockchain. Discuss the differences between PoW and PoS. **10 marks**

Q11. Consider a blockchain with three users: User A, User B, and User C. User A currently holds two Unspent Transaction Outputs (UTXOs) in their wallet:
UTXO1 with a value of 5 BTC.
UTXO2 with a value of 3 BTC.
User A initiates a transaction to send 4 BTC to User B. Afterward, User B decides to send 2 BTC to User C and keeps the remaining balance. Calculate the new UTXOs for User A, User B, and User C after both transactions are processed. Assume there are no transaction fees involved. Explain how the UTXOs change for each user after these transactions and describe the process step by step. **10 marks**



visibility
Computing
Encryption
Validation (PoW, PoS, PoB)
Security