National Forensic Sciences University

School of Cyber Security and Digital Forensics

Course Name: M.Tech Artificial Intelligence and Data Science (Batch: 2024-26) Semester - II

Subject Code: CTMTAIDS SII P5 EL1 Time: 03.30 pm to 05.00 pm
Subject Name: Blockchain Security and Investigations
Exam: Mid Semester Examination (March - 2025) Date: 21-03-2025

Answer all questions.

Q1. Why is quantum computing considered a threat to current cryptographic systems?

a) It can generate keys faster than classical computers

b) It can break traditional encryption algorithms using Shor's algorithm

c) It allows faster computation of hash functions

d) It replaces the need for digital signatures **2 marks**

Q2. What is the primary function of a Merkle Root in blockchain technology?

a) To encrypt transaction data

b) To provide a single hash representing all transactions in a block

c) To replace consensus algorithms **2 marks**

d) To ensure transactions are always reversible

Q3. What is the primary advantage of using hash pointers in data structures like blockchains?

a) They allow data retrieval without encryption

b) They enable efficient data storage

c) They provide tamper-evidence by linking blocks

d) They reduce computation time for hashing **2 marks**

Q4. Which of the following is NOT a fundamental property of a secure cryptographic system?

a) Confidentiality

b) Integrity

c) Redundancy

d) Authentication **2 marks**

Q5. 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.

10 marks

Q6. Given the elliptic curve equation:

$$E : y^2 \equiv x^3 + ax + b \mod p$$

where $a = 2$, $b = 3$, and $p = 17$, determine whether the points $P(5, 1)$ and $Q(6, 3)$ lie on the curve. Verify by substituting the coordinates into the elliptic curve equation and checking if both sides are congruent modulo p. **10 marks**

Q7. Consider the elliptic curve:

$$y^2 \equiv x^3 + 1 \mod 2$$

with the generator point:

$$G = (0, 1)$$

You are tasked with signing a message using the Elliptic Curve Digital Signature Algorithm (ECDSA) with the following parameters:

- **Private key** $K_{prv} = 1$
- **Message text** $m = 1$
- **Random integer (nonce)** $i = 1$

Follow the steps of the ECDSA algorithm to:

a) Compute the digital signature (r, s).

b) Verify the signature using the public key.

10 marks

Q8. Consider a decentralized cryptocurrency network that processes transactions using Byzantine Fault Tolerance (BFT) and ensures user privacy through Zero-Knowledge Proofs (ZKP). The network has 30 nodes, and a transaction must be validated by a consensus of nodes to be confirmed on the blockchain. However, some of these nodes may act maliciously. (a) What is the maximum number of faulty nodes the system can tolerate and still maintain consensus? (b) How many nodes are required to agree on a transaction for the system to reach consensus and commit the transaction? **6 marks**

Q9. Explain hash pointers and its role in securing the blockchain. **6 marks**