National Forensic Sciences University
School of Cyber Security & Digital Forensics
M.Tech. AIDS (2024-25)

Subject Code: (CTMTAIDS SII P5 EL1) **Date: 10/02/2025**
Subject Name: Blockchain Security & Investigation
Exam: TA- I Examination (Feb 2025) **Time: 11:00 AM to 11:45 AM**

Q1. Answer the following question in short brief. (Any 3) **[15 Marks]**

1) Explain the differences between symmetric and asymmetric encryption with examples.

2) Explain blockchain in detail, along with an example.

3) Discuss the mining and consensus mechanism, and explain them with an example.

4) Discuss the challenges faced by classical cryptography with the advent of quantum computing.

5) Compare and contrast blockchain technology with conventional distributed databases.

Q2. Answer the following question in word(s). (Attempt all) **[10 Marks]**

1) _____cryptography uses the same key for both encryption and decryption.

2) The main purpose of a hash function is _____.

3) _____ ensures data integrity and authenticity.

4) _____ is memory hard algorithm.

5) What is the purpose of Zero Knowledge Proof?

- a) To verify the integrity of a hash function
- b) To prove the knowledge of a fact without revealing the fact itself
- c) To encrypt data with zero errors
- d) To detect faults in a distributed system

6) The Byzantine Generals Problem is related to _____.

7. Quantum shor's algorithm pose a challenge to _____ classical cryptographic method.

8) _____ is the primary function of a Merkle Patricia Tree in blockchain.

9) In blockchain, _____ is used to describe a change in the protocol that is not backward-compatible.

10) The agreement among network nodes on transaction validity is _____.