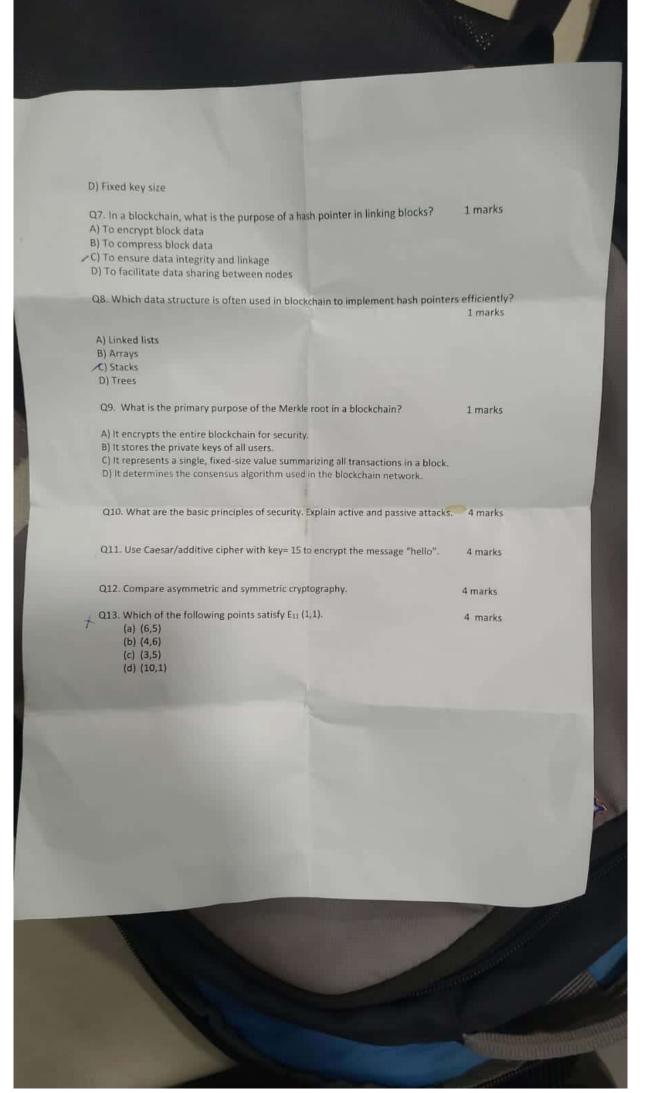# National Forensic Sciences University
School of Cyber Security and Digital Forensics
Course Name: M.Sc. Digital Forensics and Information Security (Batch: 2022-24)
Semester - III   Exam: TA - I (September- 2023)

Subject Code: CTMSDFIS SIII P3
Subject Name: Blockchain and Cryptocurrencies.

Time: 12.45 pm to 1.30 pm
Date: 18-09-2023

1 marks

Q1. What is the primary purpose of a blockchain?
A) Storing large amounts of data
B) Ensuring the privacy of user information
C) Enabling decentralized and tamper-resistant record-keeping
D) Facilitating high-speed financial transactions

1 marks

Q2. In a blockchain, what is a "block"?
A) A single user account
B) A unit of cryptocurrency
C) A group of transactions bundled together
D) A secure login method

Q3. Which cryptographic key is used for both encryption and decryption in symmetric cryptography?
1 marks
A) Public key
B) Private key
C) Shared secret key
D) Digital signature

Q4. In symmetric encryption, what is the primary concern?
1 marks
A) Key distribution
B) Public key storage
C) Hash collisions
D) Data authenticity

Q5. What is the key feature of asymmetric cryptography?
1 marks
A) Both parties use the same private key
B) Encryption and decryption use different keys
C) Encryption and decryption use the same key
D) Keys are generated by a central authority

Q6. Which property should a good cryptographic hash function have?
1 marks
A) Reversibility
B) Collision resistance
C) Low computational complexity

D) Fixed key size

Q7. In a blockchain, what is the purpose of a hash pointer in linking blocks?   1 marks
A) To encrypt block data
B) To compress block data
C) To ensure data integrity and linkage ✓
D) To facilitate data sharing between nodes

Q8. Which data structure is often used in blockchain to implement hash pointers efficiently?
        1 marks

A) Linked lists
B) Arrays
C) Stacks ✓
D) Trees

Q9. What is the primary purpose of the Merkle root in a blockchain?   1 marks

A) It encrypts the entire blockchain for security.
B) It stores the private keys of all users.
C) It represents a single, fixed-size value summarizing all transactions in a block.
D) It determines the consensus algorithm used in the blockchain network.

Q10. What are the basic principles of security. Explain active and passive attacks.   4 marks

Q11. Use Caesar/additive cipher with key= 15 to encrypt the message "hello".   4 marks

Q12. Compare asymmetric and symmetric cryptography.   4 marks

Q13. Which of the following points satisfy E_{11} (1,1).   4 marks
    (a) (6,5)
    (b) (4,6)
    (c) (3,5)
    (d) (10,1)