NOC22-CS44: Blockchain and Its Applications
Assignment 1

Correct choices are highlighted in Yellow. Give partial marks for partially correct answers.

1. What is expected by a decentralized solution for a successful Supply Chain management?
    a. No one should trust each other, however they should cooperate
    b. Everyone should trust and cooperate with each other
    c. No one should trust and cooperate with each other.
    d. Trust and cooperation does not matter here

Hint: In a real-time scenario a supply chain management system has multiple stakeholders and the information submitted by them is not guaranteed to be correct.

2. What does trust mean, in a decentralized blockchain?
    a. To secure the chain using specific protocols.
    b. To validate the transactions and blocks for tamper proofing.
    c. To execute and confirm the transactions.
    d. None of the above

Hint: Trust in a decentralized blockchain means someone can not deny the information later on. Which implies the answer is (a), (b) and (c).

3. Where are the transactions recorded in a blockchain?
    a. On a SQL Database
    b. On a distributed immutable ledger
    c. On a distributed opaque immutable ledger
    d. On a centralized immutable ledger

Hint: Refer to the slide. Definition of Blockchain - An immutable append only ever growing chain of data. Data once added cannot be deleted or modified later

4. What is one of the requirements of a secure hashing function?
    a. It is an ECC function
    b. It is a one way function
    c. It is log function
    d. It is a secret function

Hint: Refer to the Week 1 slide. Definition of Blockchain - An immutable append only ever growing chain of data. Data once added cannot be deleted or modified later

5. For a 512 bit hash function, the attacker needs to compute how many hash operations in order to find two matching outputs?

a. 1.158×10^{77}
b. 1.340×10^{154}
c. 3.403×10^{38}
d. 2.895×10^{76}

Hint: If a hash function produces □ bits of output, an attacker needs to compute only $2^{□/2}$ hash operations on a random input to find two matching outputs. $2^{512/2} = 2^{256} \approx 1.158 \times 10^{77}$

6. Which of the following is a correct statement about a cryptographic hash function?
   a. given the same message the hash function would not return the same hash
   b. it is not very difficult to generate the original message from the hash
   c. a small change in the message, impacts the hash value
   d. one can easily find two different messages with same hash

Hint: Refer to the Week 1 slide for the properties of cryptographic hash functions.

7. What are the security features of a hash function?
   a. Deterministic
   b. Puzzle-friendly
   c. Collision-resistance
   d. Preimage resistance

Hint: Refer to the Week 1 slide for the properties of cryptographic hash functions.

8. SHA-512 hashing algorithm used by Bitcoin blockchain to determine the hash of a block. This above statement is True or False.
   a. True
   b. False

Hint: SHA-256 is used in Bitcoin mining to construct the Bitcoin blockchain

9. If a participant node tampers with a block, it results in which action(s).
   a. Modification of hash
   b. Mismatching of hash values
   c. The local chain of node rendered in an invalid state
   d. Only the previous block will be in an invalid state

Hint: In the blockchain network, each block has a hash of the previous block. When someone changes any data in the present block the hash of the block will be changed, this will affect the previous block because it has the address of the previous block.

10. What is the hash value of “swayam” if SHA-256 is used? (case sensitive)
    a. 3bb8668bb7a3f9e127d4429d24ca0de0c3247843ccc528d9612d46d6ad699a63
    b. 4bb8668bb7a3f9e127d4429d24ca0de0c3247843ccc528d9612d46d6ad699a63
    c. 4bb8668bb7a3f9e127d4429d24ca0de0c3247843ccc528d9612d46d6ad699a56
    d. 3bb8668bb7a3f9e127d4429d24ca0de0c3247843ccc528d9612d46d6ad699a92

Hint: Verify the result https://emn178.github.io/online-tools/sha256.html