NOC22-CS44: Blockchain and Its Applications
Assignment 1

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

1. Which one is true for an ideal decentralized solution for business management?
   a. A centralized authority should decide the overall trust
   b. Everyone should trust and cooperate with each other
   c. No one should trust and cooperate with each other
   d. No one should trust each other, however they should cooperate

Hint: In a real-time scenario a decentralized system has multiple stakeholders and the information submitted by them is not guaranteed to be correct. A collective agreement has to be established.

2. Which of the statements below is/are true for successful run of decentralized distributed systems?
   a. Network of different players
   b. Players must trust each other
   c. If they cooperate, the society gets benefitted
   d. None of the above

Hint: In a decentralized distributed system, a group of parties who may or may not know or trust each other. But they should cooperate to reach a collective decision to benefit the system as whole. So in a decentralized system trusting everyone is not always necessary to reach a decision..

3. Where are the transactions logs recorded in a blockchain?
   a. Centralized editable database
   b. Editable log file
   c. On centralized immutable database
   d. On append only distributed immutable ledger

Hint: Refer to the slide of week1. An immutable append only ever growing chain of data is used for blockchain. Data once added cannot be deleted or modified later.

4. What are the properties of cryptographic hash function?
   a. It should be deterministic
   b. It should be collision free
   c. Ability to hide the input message
   d. Puzzle friendly

Hint: Refer to the Week 1 slide. All the above properties are desirable for secure hashing.

5. For a 512 bit hash function, the attacker needs to compute how many hash operations in order to find two matching outputs in the initial round?
   a. 2^{512}
   b. 2^{128}
   c. 2^{256}
   d. 2^{60}

Hint: If a hash function produces N bits of output, an attacker needs to compute only $2^{N/2}$ hash operations on a random input to find two matching outputs initially. The attacker can use the output combination again to use in subsequent rounds.

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. Non-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. For hash computation in SHA-512, what is the size of the block that the message is divided into?

    a. 1024
    b. 512
    c. 256
    d. 1248

Hint: The message is divided into blocks of size 1024 bits, and the output produced is a 512-bit message digest.

10. What is the message for hash value of “8abe09bf65aefdb8e84bd8564efb765179cc01ee3f45809e47c8c9a02f72ff83” if SHA-256 is used? (case sensitive)

    a. Consensus
    b. Swayam
    c. SWAYAM
    d. Consensus

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