Blockchain and Its Applications
Assignment 2

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

1. Alice employs the RSA cryptosystem with the prime numbers p = 7 and q = 17 to derive her public and private keys. Given that Alice's public key is 11, her corresponding private key is _____.

   Ans: Numerical Answer Type - 35

2. Bob wishes to send a lengthy message to Alice with the requirement that Alice can verify its origin and Bob cannot later disown the message. They also want to ensure the confidentiality of the message. Alice and Bob decide to employ public key cryptography and cryptographic hashing techniques. Let the key pairs for Alice and Bob be (Pub A, Pri A) and (Pub B, Pri B) respectively, and let E, D, and H denote the encryption, decryption, and hash functions respectively. M represents the message, and H(M) is its digest. Which of the following outlines the correct sequence of steps for Alice to send the digitally signed message?

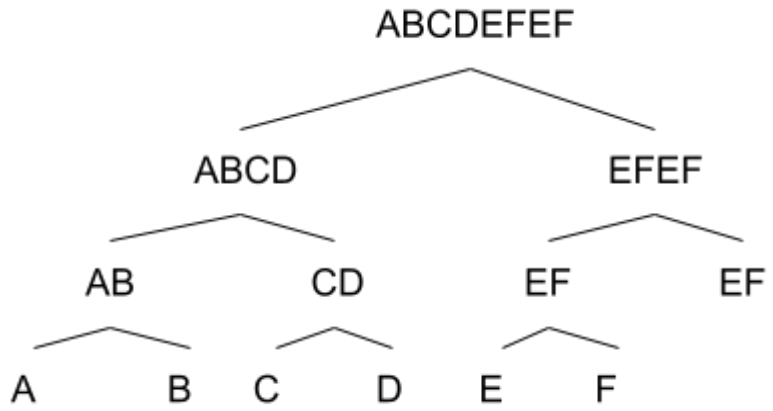
   i. At Bob: M' = E(M, K_{pubA})
   ii. At Alice: M = E(M', K_{priA})
   iii. Bob sends the message M' to Alice
   iv. The signature along with the message is sent to Alice (M, M')
   v. Bob: M' = E(M, K_{priB})
   vi. Signing the message with his private key: S = E(H(M), K_{priB})
   vii. M = E(M', K_{pubB})

   a. v, vii, ii, i, iii, iv, vi
   b. i, iii, ii, v, iv, vii, vi
   c. i, ii, iii, iv, v, vi, vii
   d. vii, vi, v, iv, iii, ii, i

3. The act of digitally signing transactions by the sender in Blockchain ensures the resolution of repudiation/verifiability problems.
   a. True
   b. False
4. Which of the following is used to point to a block in the blockchain:
   a. Hash Pointer
   b. User ID
   c. Transaction ID
   d. Timestamp
5. Suppose you have 6 data points -- A to F. The post-order traversal of the Merkle Tree is given by (here A means hash of A, DC means the combined hash of D and C, and so on):
   a. {ABCDEFEF, ABCD, EFEF, AB, CD, EF, EF, A, B, C, D, E, F}
   b. {A, AB, B, C, D, CD, ABCD, E, F, EF, ABCDEF}

c. {A, B, AB, C, D, CD, ABCD, E, F, EF, GH, EFGH, ABCDEFGH}
d. {A, B, AB, C, D, CD, ABCD, E, F, EF, EF, EFEF, ABCDEFEF}

Hint:



Post order Traversal : {A, B, AB, C, D, CD, ABCD, E, F, EF, EF, EFEF, ABCDEFEF}

6. Which of the following is true for using a digital signature in blockchain?
   a. To check the validity of the source of a transactions
   b. None of the above.
   c. It will ensures that no one can deny of their own transaction
   d. It supports user authentication

Hint: Refer to Week 2 Slide for Digital Signature.

7. Which are the main Consensus Algorithms?
   a. Proof of Work
   b. Proof of Wager
   c. Proof of Stake
   d. Proof of Mining

Hint: PoW and Pos are the main consensus algorithms

8. Why is consensus hard in an asynchronous system?
   I. No notion of global time
   II. faults in network
   III. nodes may crash/ faulty nodes
   a. II, III
   b. I, II
   c. I, III
   d. I, II, II

Hint: Due to a lack of global timing reference, and various kinds of faults it is very difficult to agree with nodes unanimously.

9. The Liveliness property ensures the output should be produced within a finite time limit?
   a. False
   b. True

Hint: Refer to Week 2 Slide, liveliness property talks about eventual termination.

10. Paxos consensus support(s) which of the below properties
    e. Liveliness
    f. Safety
    g. Both
    h. None of the above

Hint: Refer to Week 2 Slide, Paxos supports safety but not liveliness.