X

(https://swayam.gov.in) (https://swayam.gov.in/nc_details/NPTEL)

nm [redacted]

NPTEL (https://swayam.gov.in/explorer?ncCode=NPTEL) » Blockchain and its Applications (course)

Click to register for Certification exam (https://examform.nptel.ac.in/2025_01/exam_form/dashboard)

If already registered, click to check your payment status

Course outline

About NPTEL ()

How does an NPTEL online course work? ()

Week 0 ()

Week 1 ()

Week 2 ()

Lecture 6 : Basic Cryptographic

Week 2 : Assignment 2

Your last recorded submission was on 2025-02-05, 23:02 IST Due date: 2025-02-05, 23:59 IST.

1) ***1 point***

Alice employs the RSA cryptosystem with the prime numbers p=11 and q=19 to derive her public and private keys. Given that her public key is e=11, what is her corresponding private key d?

a) 35
b) 131
c) 101
d) 149

- ○ a.
- ◉ b.
- ○ c.
- ○ d.

2) ***1 point***

Alice wants to send a message to Bob with **confidentiality** and **integrity**. The steps are as follows:

1. Alice encrypts the message using Bob's _____ key.
2. Alice then signs the _____ of the message with her _____ key.
3. Bob decrypts the message using his _____ key.
4. Bob verifies Alice's signature using her _____ key.

a) public, hash, private, public, private
b) private, message, public, private, public
c) public, hash, private, private, public
d) public, hash, private, public, public

○ a.
○ b.
◉ c.
○ d.

3) ***1 point***

Digitally signing transactions by the sender in Blockchain ensures the resolution of repudiation/verifiability problems. Based on this, which one of the following is correct:

a) It allows the sender to deny the transaction at any point.
b) It ensures that the sender cannot deny the transaction and the recipient can verify its authenticity.
c) It provides encryption but does not verify the sender's identity.
d) It guarantees the transaction will remain confidential but does not resolve repudiation issues.

○ a.
◉ b.
○ c.
○ d.

4) ***1 point***

What is the primary purpose of Alice signing a message with her **private key** in a blockchain transaction?

a) To encrypt the message
b) To prevent others from reading the message
c) To prove the message came from Alice
d) To hide the contents of the message

○ a.
○ b.
◉ c.
○ d.

5) ***1 point***

Consider 6 data points labeled 1 to 6. The post-order traversal of the Merkle Tree is provided as follows (where 1 represents the hash of data point 1, 43 denotes the combined hash of 4 and 3, and so on):

a) {12345656, 1234, 12, 1, 2, 34, 3, 4, 5656, 56, 5, 6}
b) {1, 12, 2, 3, 4, 34, 1234, 5, 6, 56, 123456}
c) {1, 2, 12, 3, 4, 34, 1234, 5, 6, 56, 56, 5656, 12345656}
d) {1, 2, 12, 3, 4, 34, 1234, 5, 6, 56, 5656, 12345656}

○ a.
○ b.
◉ c.
○ d.

Download Videoes ()

6) ***1 point***

Which of the following is used to refer to a block in a blockchain?

a) Future nonce
b) Block size
c) Previous Block Hash
d) Transaction Timestamp

- ○ a.
- ○ b.
- ◉ c.
- ○ d.

7) ***1 point***

Which of the following **does not align** with the primary design goals of cryptocurrency development?

a) Decentralization of control and decision-making
b) Immutability of transaction records
c) Centralized control over transactions
d) Transparency and accessibility of transaction data

- ○ a.
- ○ b.
- ◉ c.
- ○ d.

8) ***1 point***

Which of the following statements is/are **true** regarding **Bitcoin** and its **consensus algorithm**?

1. Bitcoin uses Proof of Work (PoW) for transaction validation and block addition.
2. Bitcoin operates on a peer-to-peer (P2P) network.
3. Bitcoin uses Proof of Stake (PoS) for centralization.
4. Miners are rewarded with transaction fees and block rewards in Bitcoin.

a) 1, 2, 3
b) 2, 3, 4
c) 1, 2, 4
d) 1, 3, 4

- ○ a.
- ○ b.
- ◉ c.
- ○ d.

9) **1 point**

What is the primary focus of 'safety' in Bitcoin's protocol?

a) Preventing invalid transactions
b) Ensuring blocks are mined quickly
c) Guaranteeing that only some of the transactions are private
d) Maximizing the number of transactions per block

- (●) a.
- ( ) b.
- ( ) c.
- ( ) d.

10) **1 point**

Which of the following is the primary goal of a consensus algorithm in a distributed system?

a) To ensure that all nodes process transactions at the same speed
b) To guarantee that all nodes in the system agree on a single value or state
c) To minimize the number of nodes required for network communication
d) To prevent malicious attacks by encrypting all data transmitted between nodes

- ( ) a.
- (●) b.
- ( ) c.
- ( ) d.

You may submit any number of times before the due date. The final submission will be considered for grading.

Submit Answers