X

NPTEL

reviewer4@nptel.iitm.ac.in ▾

Courses » Blockchain Architecture Design and Use Cases

Announcements **Course** Ask a Question Progress FAQ

Unit 5 - Week 2 : Unit 2

Register for Certification exam

Course outline

- How to access the portal
- Prerequisite
- Week 1 : Unit 1
- Week 2 : Unit 2
  - Lecture 06 : Basic Crypto Primitives – II
  - Lecture 07 : Bitcoin Basics – I
  - Lecture 08 : Bitcoin Basics – II
  - Lecture 09 : Bitcoin Basics – III
  - Lecture 10 : Distributed Consensus
  - Lecture Materials
  - Feedback for Week 2
  - Quiz : Assignment 2

Assignment 2

The due date for submitting this assignment has passed.
As per our records you have not submitted this assignment. **Due on 2019-02-13, 23:59 IST.**

1) Suppose, you are using RSA algorithm based cryptosystem to securely share the number of marbles that you have currently with you, among your friends. The private key that you are using is (3,15). Your friends know the corresponding public key is (11,15). One of your friends wants to share the exact amount of marble content only to you. What are the maximal possible marbles that your friend can have so that he/she can secretly share that to you? ***1 point***

- 14
- 15
- 16
- No such limit exists

No, the answer is incorrect.
Score: 0

Accepted Answers:
14

2) In the previous problem, suppose an attacker somehow manages to know your public key (11,15). Additionally, he observes that your friend is sending an encrypted message with ciphertext 6. Is it possible for the attacker to guess the original message that your friend sends to you? ***1 point***

- Yes, without any hurdle he can guess
- Possible, only if the attacker can guess proper encryption key
- Possible, only if the attacker can guess proper decryption key
- Not possible as guessing the keys are difficult

No, the answer is incorrect.
Score: 0

Accepted Answers:
Yes, without any hurdle he can guess

receiver's public key

No, the answer is incorrect.
Score: 0

Accepted Answers:
sender's private key

4) Consider the following three scenarios and select the double spending attack example(s): ***1 point***

- Jena brought a piece of jewellery using 20 bitcoins. On delivery, the bitcoins are transferred from Jena's wallet to the jewellery shop's wallet. She somehow manages to reverse the bitcoin transfer and tries to use the same for another purchase.
- Alice and Bob have 30 unspent bitcoins each. Alice and Bob transfer 10 bitcoins to each other,Jena.
- Hari has 40 unspent bitcoins. Hari sends the entire amount each to Dick and Tom.

No, the answer is incorrect.
Score: 0

Accepted Answers:
Jena brought a piece of jewellery using 20 bitcoins. On delivery, the bitcoins are transferred from Jena's wallet to the jewellery shop's wallet. She somehow manages to reverse the bitcoin transfer and tries to u the same for another purchase.
Hari has 40 unspent bitcoins. Hari sends the entire amount each to Dick and Tom.

5) How does the pseudo-anonymity of a user is maintained in bitcoin? ***1 point***

- using the generated unique identifier based on the user's email address
- using the generated unique identifier based on the user's private key
- using the generated unique identifier based on the user's public key
- using the generated unique identifier based on the user's private and public key

No, the answer is incorrect.
Score: 0

Accepted Answers:
using the generated unique identifier based on the user's public key

6) What is the output of the following script? ***1 point***

<data1> <data2> OP_SHA256 OP_RIPEMD160 OP_SWAP OP_HASH160 OP_EQUALVERIFY
Assume data1 and data2 are identical.

- True
- False
- Empty
- Failure

No, the answer is incorrect.
Score: 0

Accepted Answers:
Empty

7) What is the output of the following script? ***1 point***

scriptSig: <sig><pubKey>
scriptPubKey: OP_DUP OP_HASH256 <pubKeyHash> OP_EQUAL OP_CHECKSIG

- True
- Empty
- Failure

No, the answer is incorrect.
Score: 0

Accepted Answers:
Failure

8) What is/are the content(s) of the block header in bitcoin? ***1 point***

- [ ] Merkle root
- [ ] Previous block header hash
- [ ] Next block's Merkle root
- [ ] Target threshold nBits

No, the answer is incorrect.
Score: 0

Accepted Answers:
Merkle root
Previous block header hash
Target threshold nBits

9) Suppose, five trustworthy nodes are performing some task distributedly. As per the process, ***1 point*** at a certain interval, every nodes of the team shares the results for making the consensus. After starting the task, two trustworthy nodes drop the plan and they are replaced by two other nodes whose trustworthy information is unknown. After joining the new nodes, some discrepancy occurs in the system. What is the type of the fault it is in the context of distributed consensus?

- ( ) Crash Fault
- ( ) Network Fault
- ( ) Byzantine Fault

No, the answer is incorrect.
Score: 0

Accepted Answers:
Byzantine Fault

10) In distributed consensus, all the non-faulty individuals' decision must be identical. This property is ***1 point***

- ( ) Termination
- ( ) Validity
- ( ) Integrity
- ( ) Agreement

No, the answer is incorrect.
Score: 0

Accepted Answers:
Agreement

Previous Page End