Unit 3 - Week 2

Course outline

How to access the portal?

Week 1

Week 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
- Quiz : Assignment 2
- Week 2 Feedback Form : Blockchain Architecture Design and Use Cases
- Assignment 2 Solution

Week 3

Week 4

Week 5

Week 6

Week 7

Week 8

Week 9

Week 10

Week 11

Week 12

VIDEO DOWNLOAD

FAQ

Live Session

Text Transcripts

Assignment 2

The due date for submitting this assignment has passed.
As per our records you have not submitted this assignment.

Due on 2019-08-21, 23:59 IST.

1) Suppose, we have designed a new RSA algorithm with $\phi(91) = 91 * \prod_{p|91}(1 - 1/p)$, keeping all other parameters as actual RSA algorithm. **1 point**

If the decryption key is 29, the encryption key is:

- 29
- 5
- 7
- 72

No, the answer is incorrect.
Score: 0
Accepted Answers:
5

2) Suppose, you and your friends have a few numbers of locks and you all want to share that numbers among yourselves securely using RSA based cryptosystem. You are using the private key as (5,27) and your friends are using the public key as (13,27). One of your friends wants to share the exact amount of locks only to you. What are the maximal possible locks that your friend can have so that he/she can secretly share that to you? **1 point**

- 26
- 27
- 28
- No such limit exists

No, the answer is incorrect.
Score: 0
Accepted Answers:
26

3) Suppose, an attacker gets access to the ciphertext which is 8 and public key (13,27). Keeping the other parameters same as the previous question, can the attacker guess the original message? **1 point**

- Yes
- Possible, only if the attacker can rightly guess proper decryption key
- Possible, only if the attacker can rightly guess proper encryption key
- Guessing the original message is impossible as guessing the keys are difficult

No, the answer is incorrect.
Score: 0
Accepted Answers:
Yes

4) Which is used for signing the message digest in the public-key cryptosystem? **1 point**

- using the public key of the receiver
- using the private key of the receiver
- using the public key of the sender
- using the private key of the sender

No, the answer is incorrect.
Score: 0
Accepted Answers:
using the private key of the sender

5) Which is/are the example/s of the double-spending attack? **1 point**

- Alice has a total of 40 unspent bitcoins from two different transactions with an equal amount of bitcoins each. She sends the entire amount each to Dick and Tom from one of the transaction
- Bob brought a car using x bitcoins. On delivery, the bitcoins are transferred from his wallet to the shopper's wallet. Simultaneously, he uses that bitcoins for another purchase
- Alice and Bob each have 20 unspent bitcoins. Both of them transfer 10 bitcoins to each other
- Bob has 20 unspent bitcoins. He sends the entire amount each to Dick and Tom

No, the answer is incorrect.
Score: 0
Accepted Answers:
Alice has a total of 40 unspent bitcoins from two different transactions with an equal amount of bitcoins each. She sends the entire amount each to Dick and Tom from one of the transaction
Bob brought a car using x bitcoins. On delivery, the bitcoins are transferred from his wallet to the shopper's wallet. Simultaneously, he uses that bitcoins for another purchase
Bob has 20 unspent bitcoins. He sends the entire amount each to Dick and Tom

6) Which of the following bitcoin scripts will generate a TRUE outcome? **1 point**

i) scriptSig: <sig>
scriptPubKey: <pubKey> OP_DUP OP_HASH256 <pubKeyHash> OP_EQUAL OP_VERIFY OP_CHECKSIG
ii) scriptSig: <pubKey>
scriptPubKey: OP_HASH160 <pubKeyHash> OP_EQUAL
iii) scriptSig: <pubKey>
scriptPubKey: <pubKey> OP_EQUALVERIFY
iv) scriptSig: <sig>
scriptPubKey: <pubKey> OP_CHECKSIG

- i, ii, iii
- iii, iv
- i, ii, iv
- All of the above

No, the answer is incorrect.
Score: 0
Accepted Answers:
i, ii, iv

7) Which of the Select the script which checks the equality of the hash values: **1 point**

- <data1> <data2> OP_SHA256 OP_SHA256 OP_SWAP OP_HASH256 OP_EQUAL
- <data1> <data2> OP_HASH160 OP_SWAP OP_RIPEMD160 OP_SHA256 OP_EQUAL
- <data1> <data2> OP_HASH160 OP_HASH160 OP_EQUAL
- <data1> <data2> OP_SHA256 OP_SWAP OP_RIPEMD160 OP_HASH160 OP_EQUAL

No, the answer is incorrect.
Score: 0
Accepted Answers:
<data1> <data2> OP_SHA256 OP_SHA256 OP_SWAP OP_HASH256 OP_EQUAL

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

- Merkle root
- Timestamp with explicit timezone
- Next block's Merkle root
- Target threshold nBits

No, the answer is incorrect.
Score: 0
Accepted Answers:
Merkle root
Target threshold nBits

9) Suppose, 15 trustworthy nodes are performing some task distributedly. As per the process, at a certain interval, every node of the team shares the results for making the consensus. After starting the task, 7 trustworthy nodes drop the plan and they are replaced by 7 other nodes whose trustworthy information is unknown. After joining the new nodes, some discrepancy occurs in the system, although all the nodes are running correctly without any software or hardware error. What is the type of fault it is in the context of distributed consensus? **1 point**

- Crash Fault
- Network Fault
- Byzantine Fault

No, the answer is incorrect.
Score: 0
Accepted Answers:
Byzantine Fault

10)In distributed consensus, all the correct individuals either reach a value or null. What is the name of the property? **1 point**

- Termination
- Validity
- Integrity
- Agreement

No, the answer is incorrect.
Score: 0
Accepted Answers:
Integrity