

X

NPTEL

reviewer3@nptel.iitm.ac.in ▼

Courses » Blockchain Architecture Design and Use Cases

Announcements

**Course**

Ask a Question

Progress

Mentor

FAQ

## Unit 4 - Week 2 : Unit 2

### Course outline

How to access the portal

FAQ

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
- ☐ Quiz : Assignment 2
- ☐ Week 2 - Feedback
- ☐ Assignment-2 Solution

### Assignment 2

The due date for submitting this assignment has passed.

As per our records you have not submitted this assignment.

**Due on 2018-08-22, 23:59 IST.**

1) Suppose, we have designed a new RSA algorithm with

**1 point**

$$\phi(55) = 55 * \prod_{p|55} (1 - 1/p),$$

keeping all other parameters as actual RSA algorithm. If the encryption key is 27, the decryption key is:

- ☐ 27
- ☐ 3
- ☐ 5
- ☐ 40

**No, the answer is incorrect.**

**Score: 0**

**Accepted Answers:**

3

2) In public key cryptosystem, the message digest is signed by:

**1 point**

- ☐ sender's public key
- ☐ sender's private key
- ☐ receiver's public key
- ☐ receiver's private key

**No, the answer is incorrect.**

**Score: 0**

**Accepted Answers:**

sender's private key

© 2014 NPTEL - Privacy & Terms - Honor Code - FAQs -



A project of



In association with



Funded by

Week 7	ce De	<input type="radio"/> X->Y:30,X->Z:30	
Week 8		<input type="radio"/> All of the above	
Week 9		No, the answer is incorrect. Score: 0	
Week 10		Accepted Answers: X->Y:30,X->Z:30	
Week 11		4) The users access the bitcoin wallet using:	1 point
Week 12		<input type="radio"/> his/her email address <input type="radio"/> his/her public key based address <input type="radio"/> his/her private key based address <input type="radio"/> his/her public and private key based address	
VIDEO DOWNLOAD			

No, the answer is incorrect.  
Score: 0

Accepted Answers:  
his/her public key based address

5) The digital signature algorithm used in bitcoin: 1 point

☐ Elliptic Curve Digital Signature Algorithm  
☐ Digital Signature Algorithm  
☐ RSA Algorithm  
☐ All of the above

No, the answer is incorrect.  
Score: 0

Accepted Answers:  
Elliptic Curve Digital Signature Algorithm

6) Suppose, a user X wants to transfer 20 bitcoins to his friend Y through bitcoin wallet. The necessary details X must send to Y so that his friend can validate the transfer: 1 point

☐ transaction, X's signature, X's private key  
☐ transaction, X's signature, Y's public key  
☐ transaction, X's signature, X's public key  
☐ transaction, Y's public key, X's public key

No, the answer is incorrect.  
Score: 0

Accepted Answers:  
transaction, X's signature, X's public key

7) Consider the following bitcoin script and select the one(s) with 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

8) 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

9) The outcome of the script: **0 points**

scriptSig: <sig> <pubKey>  
scriptPubKey: OP\_RETURN OP\_DUP OP\_HASH256 <pubKeyHash>  
OP\_EQUALVERIFY OP\_CHECKSIG

- ☐ Fail
- ☐ True
- ☐ False
- ☐ Nothing

No, the answer is incorrect.

Score: 0

Accepted Answers:

Fail

10) The computing resources are highly essential for: **1 point**

- ☐ Mining
- ☐ Block creation
- ☐ Scripting
- ☐ Coding

No, the answer is incorrect.

Score: 0

Accepted Answers:

Mining

11) In distributed consensus, all the correct individuals either reach a value or null. The property is **1 point**

- ☐ Termination
- ☐ Validity
- ☐ Integrity
- ☐ Agreement

No, the answer is incorrect.

Score: 0

Accepted Answers:

*Integrity*

12) The distributed consensus mechanism works in an open Internet grade computing system is: **1 point**

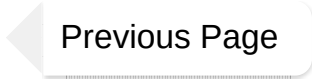
- ☐ Shared memory
- ☐ Message passing
- ☐ PBFT
- ☐ None of the above

No, the answer is incorrect.

Score: 0

Accepted Answers:

*PBFT*

 Previous Page

End 