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

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

Week 7
Week 8
Week 9
Week 10
Week 11
Week 12
VIDEO DOWNLOAD

- X->Y:30,X->Z:30
- All of the above

No, the answer is incorrect.
Score: 0

Accepted Answers:
X->Y:30,X->Z:30

4) The users access the bitcoin wallet using: ***1 point***

- his/her email address
- his/her public key based address
- his/her private key based address
- his/her public and private key based address

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