Blockchain Basics
Week 3

PRACTICE QUIZ -1

1. A popular public-private key implementation known as Rivest-Shamir-Adelman (RSA) algorithm is used for the Bitcoin and Ethereum Blockchain. True or False?

False

True

Correct

Correct!

1 / 1 point

2.Question 2

For the simple symmetric key example discussed in the lecture, it is easy to derive the “secret” key from the encrypted data. True or False?

True

False

Correct

Correct! Please note that symmetric keys have other issues such (i) key distribution -- how do you send the key to the parties involved (ii) you need to create different secret key for different receivers, you cannot share the same key with different participants.

On the contrary, in a public-key encryption, you can publish the public key for any participant to use and not reveal the private key.

1 / 1 point

3.Question 3

256 bit ECC key-pair is equivalent in strength to approximately 3072-bit RSA key-pair. Thus ECC is much stronger encryption than RSA method. True or False?

True

False

Correct

Correct!

PRACTICE QUIZ -2

1. What is one of the requirements of secure hashing function?
It is an ECC function

It is a secret function

It is a one way function

It is log function

Correct

Correct!

1 / 1 point

2.Question 2

What type of hash is used when there is a fixed number of items to be hashed, such as the items in a block header, and we are verifying the composite block integrity?

Tree-structured Hash

Either

Complex hash

Simple Hash

Correct

Correct!

1 / 1 point

3.Question 3

What type of hash function is used, when there is variable number of items to be hashed, such as the many state changes in a block?

Simple Hash

Either

Complex hash

Tree-structured Hash

Correct

Correct!

1 / 1 point

4.Question 4

Keccak 256 is a commonly used algorithm for hash generation in Ethereum blockchain. True or False?

True

False

Correct

Correct!

PRACTICE QUIZ -3

1. Digital signing of a transaction/document involves, hashing the content of the document and then ____.

encrypting it with public key

encrypting it with private key

encrypting it with nonce

rehashing it

Correct

Correct!

PRACTICE QUIZ -4

1. n Ethereum, the block hash is the hash of all the elements in the ________ .
State tree

Block header

Transaction hash tree

Receipt tree

Correct

Correct!

1 / 1 point

2.Question 2

Merkle tree hash is used for computing _________ hash.

state root

transaction root

receipt root

all of the above

Correct

Correct!

1 / 1 point

3.Question 3

Block hash allows for the formation of the chain link by embedding previous block hash in the current block header. True or False?

True

False

Correct

Correct!

1 / 1 point

4.Question 4

If a participant node tampers with a block, it results in ____.

hash changing

mismatch of hash values

the local chain of node rendered in an invalid state

All of the above

Correct

Correct!

GRADED QUIZ

1. The transaction Merkle Tree root value in a Bitcoin block is calculated using ___.

hash of transactions

none

previous block’s hash

number of transactions

Correct

Correct.

1 / 1 point

2.Question 2

Follow the steps given in the tool at this link to manually calculate the hash of the block #490624. You can obtain the details required in the tool from this link except for the timestamp. Please use the timestamp from this link.

What is the hash of the block #490624? Copy and paste the answer.

000000000000000000d4c8b9d5388e42bf084e29546357c63cba8324ed4ec8bf
Correct

Correct

1 / 1 point

3.Question 3

Follow the guidelines in the encryption tool at this link to better understand the concept of Public-Private key encryption and answer the question below.

When encrypting a message with the public key, which key is required to decrypt the message?

Private Key

Both Public key and Private key

Inverted Public Key

Public Key

Correct

Correct

1 / 1 point

4.Question 4

What type of hashing algorithm does Bitcoin blockchain use to determine the hash of a block?

SHA-512

SHA-256

MD5

SHA-1

Correct

That’s correct. Bitcoin uses: SHA256(SHA256(Block_Header))

1 / 1 point

5.Question 5

In Ethereum, which algorithm is applied to the private key in order to get a unique public key.

RSA

SHA 256

ECC

Keccak

Correct

That’s correct. Addresses of account are generated using the public key-private key pair. First, a 256-bit random number is generated and designated as a private key, kept secure and locked using a passphrase. Then an ECC algorithm is applied to the private key to get a unique public key.

1 / 1 point

6.Question 6

Which of the following methods can be used to obtain the original message from its generated hash message using SHA-256?

Hashing the generated hash again, twice

Hashing the reverse of generated hash

Original message cannot be retrieved

Hashing the generated hash again

Correct

That’s correct. SHA-256 is a one-way hash function, that is a function which is infeasible to invert.

1 / 1 point

7.Question 7

In Ethereum, hashing functions are used for which of the following?

1. Generating state hash.

2. Generating account addresses.

3. Decrypting senders message.

4. Generating block header hash.

1,3,4

1,2,4

1,2,3

2,3,4

Correct

That’s correct. In Ethereum, hashing functions are used for generating account addresses, digital signatures, transaction hash, state hash, receipt hash, and block header hash.

1 / 1 point

8.Question 8

What is the purpose of using a digital signature?

It supports user authentication

It supports the integrity of messages

It supports both user authentication and integrity of messages

None of the above.

Correct

That’s correct. A valid digital signature gives a recipient reason to believe that the message was created by a known sender (authentication), that the sender cannot deny having sent the message, and that the message was not altered in transit (integrity).

1 / 1 point

9.Question 9

Encryption of a message provides ____.

security

nonrepudiation

integrity

authentication

Correct

Correct.

1 / 1 point

10.Question 10

A public key is derived from the ____.

hash of the first transaction by the account

genesis block hash

private Key

a different public key

Correct

Correct!