Algorithms & Techniques - Week 3

LATEST SUBMISSION GRADE

100%

1. The transaction Merkle Tree root value in a Bitcoin block is calculated using ____. **1 / 1 point**

- ○ number of transactions
- ◉ hash of transactions
- ○ none
- ○ previous block's hash

✓ **Correct**
Correct.

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.** **1 / 1 point**

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

00000000000000000d4c8b9d5388e42bf084e29546357c63cba8324ed4ec8bf

✓ **Correct**
Correct

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.** **1 / 1 point**

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

- ◉ Private Key
- ○ Inverted Public Key
- ○ Public Key
- ○ Both Public key and Private key

✓ **Correct**
Correct

4. What type of hashing algorithm does Bitcoin blockchain use to determine the hash of a block? **1 / 1 point**

- ○ SHA-512
- ◉ SHA-256
- ○ MD5
- ○ SHA-1

✓ **Correct**
That's correct. Bitcoin uses: SHA256(SHA256(Block_Header))

5. In Ethereum, which algorithm is applied to the private key in order to get a unique public key. **1 / 1 point**

- (•) ECC
- ( ) SHA 256
- ( ) RSA
- ( ) 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.

6. Which of the following methods can be used to obtain the original message from its generated hash message using SHA-256? **1 / 1 point**

- ( ) Hashing the generated hash again
- ( ) Hashing the generated hash again, twice
- ( ) Hashing the reverse of generated hash
- (•) Original message cannot be retrieved

✓ **Correct**

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

7. In Ethereum, hashing functions are used for which of the following? **1 / 1 point**

1. Generating state hash.
2. Generating account addresses.
3. Decrypting senders message.
4. Generating block header hash.

- ( ) 1,2,3
- ( ) 2,3,4
- (•) 1,2,4
- ( ) 1,3,4

✓ **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.

8. What is the purpose of using a digital signature? 1 / 1 point

- None of the above.
- It supports both user authentication and integrity of messages
- It supports user authentication
- It supports the integrity of messages

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).

9. Encryption of a message provides ____. 1 / 1 point

- authentication
- security
- nonrepudiation
- integrity

Correct
Correct.

10. A public key is derived from the ____. 1 / 1 point

- a different public key
- hash of the first transaction by the account
- genesis block hash
- private Key

Correct
Correct!