Algorithms & Techniques - Week 3

Quiz, 10 questions

10/10 points (100.00%)

Congratulations! You passed! Next Item

1 / 1 points

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

- none
- number of transactions
- hash of transactions

Correct
Correct.

- previous block's hash

1 / 1 points

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.

00000000000000000d4c8b9d5388e42bf084e29546357c63cba8324ed4ec8b

Correct Response
Correct

1 / 1 points

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?

- Public Key
- Inverted Public Key
- Private Key

Correct
Correct

- Both Public key and Private key

1 / 1 points

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

- MD5
- SHA-512
- SHA-1
- SHA-256

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

1 / 1 points

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

- Keccak
- ECC

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.

- RSA
- SHA 256

✔ 1 / 1 points

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
- 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.

- Hashing the reverse of generated hash
- Hashing the generated hash again

✔ 1 / 1 points

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.

- 1,2,4

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.

- 1,3,4
- 1,2,3
- 2,3,4

✔ 1 / 1 points

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

- It supports the integrity of messages
- It supports user authentication
- It supports both user authentication and 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).

- None of the above.

✔ 1 / 1 points

9. Encryption of a message provides ___.

- security

Correct
Correct.

- authentication
- nonrepudiation
- integrity

---

1 / 1 points

10. A public key is derived from the ___.

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

Correct
Correct!