# Algorithms & Techniques - Week 3

Quiz, 10 questions

✔ **Congratulations! You passed!**

<div>

Next Item

</div>

✔

**1 / 1
point**

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

○ number of transactions

◉ hash of transactions

**Correct**
Correct.

○ none

○ previous block's hash

✖

**0 / 1
point**

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.

Enter answer here

**Incorrect Response**
That's incorrect. Please enter the correct value from the links provided into the tool.

✔

1 / 1
point

3. **Follow the guidelines in the encryption tool at <u>this link</u> 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?

◯ Both Public key and Private key

◯ Public Key

◯ Inverted Public Key

◯ Private Key

**Correct**
Correct

---

✔

1 / 1
point

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

◯ SHA-256

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

◯ MD5

◯ SHA-1

◯ SHA-512

**✖**

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

0 / 1
point

○ SHA 256

○ Keccak

○ ECC

○ RSA

▲

**This should not be selected**
That's incorrect. Please review the lesson on "**Transaction Integrity**".

---

**✔**

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 reverse of generated hash

○ 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 generated hash again

---

**✔**

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.

   ○ 1,2,4

**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.

   ○ 2,3,4

   ○ 1,2,3

   ○ 1,3,4

---

✔

1 / 1
point

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

   ○ 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.

   ○ It supports user authentication

   ○ It supports the integrity of messages

✔

1 / 1
point

9. Encryption of a message provides ___.

○ integrity

◉ security

▲

**Correct**
Correct.

○ authentication

○ nonrepudiation

✔

1 / 1
point

10. A public key is derived from the ___.

◉ private Key

▲

**Correct**
Correct!

○ genesis block hash

○ a different public key

○ hash of the first transaction by the account

👍 💬 ⚑