Cryptographic Foundations – Quiz

Cryptoeconomics

Question 1

What is a hash function?

A. A function that encrypts data reversibly
B. A one-way function that produces a fixed-size output from any input
C. A function that generates random numbers
D. A function that compresses files

Question 1

What is a hash function?

A. A function that encrypts data reversibly
B. A one-way function that produces a fixed-size output from any input
C. A function that generates random numbers
D. A function that compresses files

Answer: B
Hash functions are deterministic, one-way functions that map arbitrary data to fixed-size outputs.

Question 2

Which hash function does Bitcoin primarily use?

A. MD5
B. SHA-256
C. SHA-1
D. Keccak-256

Question 2

Which hash function does Bitcoin primarily use?

A. MD5
B. SHA-256
C. SHA-1
D. Keccak-256

Answer: B
Bitcoin uses SHA-256 (Secure Hash Algorithm 256-bit) for mining and transaction hashing.

Question 3

What property ensures small input changes produce completely different hash outputs?

A. Collision resistance
B. Avalanche effect
C. Pre-image resistance
D. Determinism

Question 3

What property ensures small input changes produce completely different hash outputs?

A. Collision resistance
B. Avalanche effect
C. Pre-image resistance
D. Determinism

Answer: B
The avalanche effect means even a tiny change in input produces a drastically different output hash.

Question 4

What is 'collision resistance' in hash functions?

A. Resistance to network attacks
B. Difficulty of finding two different inputs with the same hash output
C. Resistance to hardware failures
D. Speed of hashing

Question 4

What is 'collision resistance' in hash functions?

A. Resistance to network attacks
B. Difficulty of finding two different inputs with the same hash output
C. Resistance to hardware failures
D. Speed of hashing

Answer: B
Collision resistance means it should be computationally infeasible to find two distinct inputs that hash to the same output.

Question 5

What algorithm does Bitcoin use for digital signatures?

A. RSA
B. ECDSA (Elliptic Curve Digital Signature Algorithm)
C. DSA
D. AES

Question 5

What algorithm does Bitcoin use for digital signatures?

A. RSA
B. ECDSA (Elliptic Curve Digital Signature Algorithm)
C. DSA
D. AES

Answer: B
Bitcoin uses ECDSA with the secp256k1 curve for signatures. Since Taproot (Nov 2021), Schnorr signatures are also supported, offering better privacy and efficiency.

Question 6

What is a public key in cryptography?

A. A password
B. A key that can be shared publicly and is used to verify signatures
C. A secret encryption key
D. A mining key

Question 6

What is a public key in cryptography?

A. A password
B. A key that can be shared publicly and is used to verify signatures
C. A secret encryption key
D. A mining key

Answer: B
The public key is derived from the private key and can be shared openly. It's used to verify signatures and derive addresses.

Question 7

What must be kept secret to control cryptocurrency funds?

A. Public key
B. Private key
C. Wallet address
D. Transaction ID

Question 7

What must be kept secret to control cryptocurrency funds?

A. Public key
B. Private key
C. Wallet address
D. Transaction ID

Answer: B
The private key must be kept secret as it allows signing transactions and spending funds.

Question 8

What is a digital signature used for?

A. Encrypting messages
B. Proving ownership and authorizing transactions
C. Hiding transaction amounts
D. Mining blocks

Question 8

What is a digital signature used for?

A. Encrypting messages
B. Proving ownership and authorizing transactions
C. Hiding transaction amounts
D. Mining blocks

Answer: B
Digital signatures prove the sender owns the private key and has authorized the transaction.

Question 9

What is the relationship between a Bitcoin address and a public key?

A. They are identical
B. The address is derived from hashing the public key
C. The public key is derived from the address
D. They are unrelated

Question 9

What is the relationship between a Bitcoin address and a public key?

A. They are identical
B. The address is derived from hashing the public key
C. The public key is derived from the address
D. They are unrelated

Answer: B
A Bitcoin address is created by hashing the public key (RIPEMD-160 of SHA-256) and encoding it.

Question 10

What is 'pre-image resistance'?

A. Resistance to viewing images
B. Difficulty of finding an input that produces a specific hash output
C. Resistance to network attacks
D. Speed of hashing

Question 10

What is 'pre-image resistance'?

A. Resistance to viewing images
B. Difficulty of finding an input that produces a specific hash output
C. Resistance to network attacks
D. Speed of hashing

Answer: B
Pre-image resistance means given a hash output, it's computationally infeasible to find the original input.

Question 11

What is the output size of SHA-256?

A. 128 bits
B. 256 bits
C. 512 bits
D. 64 bits

Question 11

What is the output size of SHA-256?

A. 128 bits
B. 256 bits
C. 512 bits
D. 64 bits

Answer: B
SHA-256 always produces a 256-bit (32-byte) output regardless of input size.

Question 12

What is asymmetric cryptography?

A. Using the same key for encryption and decryption
B. Using a key pair (public and private) for cryptographic operations
C. Using no keys at all
D. Using only hash functions

Question 12

What is asymmetric cryptography?

A. Using the same key for encryption and decryption

B. Using a key pair (public and private) for cryptographic operations

C. Using no keys at all

D. Using only hash functions

Answer: B

Asymmetric cryptography uses a mathematically related key pair: a private key for signing/decrypting and a public key for verifying/encrypting.

Question 13

What is a 'seed phrase' or 'mnemonic phrase'?

A. A password for exchanges
B. A series of words that can regenerate all private keys in a wallet
C. A transaction description
D. A mining configuration

Question 13

What is a 'seed phrase' or 'mnemonic phrase'?

A. A password for exchanges

B. A series of words that can regenerate all private keys in a wallet

C. A transaction description

D. A mining configuration

Answer: B

A seed phrase (typically 12 or 24 words) encodes entropy that can deterministically generate all wallet keys.

Question 14

What is the secp256k1 curve?

A. A mining algorithm
B. The specific elliptic curve used in Bitcoin's ECDSA
C. A hash function
D. A network protocol

Question 14

What is the secp256k1 curve?

A. A mining algorithm
B. The specific elliptic curve used in Bitcoin's ECDSA
C. A hash function
D. A network protocol

Answer: B
secp256k1 is the elliptic curve parameters Bitcoin uses for its public key cryptography.

Question 15

Why can't you derive a private key from a public key?

A. It's illegal
B. The mathematical operation (discrete logarithm) is computationally infeasible
C. They are stored separately
D. Public keys are encrypted

Question 15

Why can't you derive a private key from a public key?

A. It's illegal
B. The mathematical operation (discrete logarithm) is computationally infeasible
C. They are stored separately
D. Public keys are encrypted

Answer: B
Deriving a private key from a public key requires solving the elliptic curve discrete logarithm problem, which is computationally infeasible.

Question 16

What does 'deterministic' mean for hash functions?

A. The output is random
B. The same input always produces the same output
C. The function runs at a fixed speed
D. The output size varies

Question 16

What does 'deterministic' mean for hash functions?

A. The output is random
B. The same input always produces the same output
C. The function runs at a fixed speed
D. The output size varies

Answer: B
Deterministic means identical inputs will always produce identical outputs, with no randomness involved.

Question 17

What is Keccak-256 used for?

A. Bitcoin mining
B. Ethereum's hash function
C. File compression
D. Network encryption

Question 17

What is Keccak-256 used for?

A. Bitcoin mining
B. Ethereum's hash function
C. File compression
D. Network encryption

Answer: B
Keccak-256 (basis of SHA-3) is the hash function used in Ethereum for addresses and state.

Question 18

What is a 'hash pointer'?

A. A type of mouse cursor
B. A pointer that also contains a hash of the data it points to
C. A mining reward
D. A wallet type

Question 18

What is a 'hash pointer'?

A. A type of mouse cursor

B. A pointer that also contains a hash of the data it points to

C. A mining reward

D. A wallet type

Answer: B

A hash pointer contains both the location of data and a cryptographic hash of that data, enabling tamper detection.

Question 19

What makes hash functions useful for proof-of-work?

A. They are reversible
B. Output is unpredictable, requiring trial and error to find valid hashes
C. They are slow
D. They produce large outputs

Question 19

What makes hash functions useful for proof-of-work?

A. They are reversible
B. Output is unpredictable, requiring trial and error to find valid hashes
C. They are slow
D. They produce large outputs

Answer: B
The unpredictability of hash outputs means miners must try many nonces to find one producing a hash below the target.

Question 20

What is 'second pre-image resistance'?

A. Resistance to viewing images
B. Difficulty of finding another input with the same hash as a given input
C. Resistance to double-spending
D. Network security

Question 20

What is 'second pre-image resistance'?

A. Resistance to viewing images
B. Difficulty of finding another input with the same hash as a given input
C. Resistance to double-spending
D. Network security

Answer: B
Second pre-image resistance means given an input and its hash, it's hard to find a different input with the same hash.

Question 21

Alice writes her 24-word seed phrase on paper and stores it in a safe. Her laptop is stolen with her wallet software. What should she do?

A. Her funds are lost forever since the laptop was stolen

B. Install wallet software on a new device, enter the seed phrase, and immediately transfer funds to a new wallet with a new seed phrase

C. Contact the blockchain administrator to freeze her account

D. The seed phrase is useless without the original laptop

Question 21

Alice writes her 24-word seed phrase on paper and stores it in a safe. Her laptop is stolen with her wallet software. What should she do?

A. Her funds are lost forever since the laptop was stolen

B. Install wallet software on a new device, enter the seed phrase, and immediately transfer funds to a new wallet with a new seed phrase

C. Contact the blockchain administrator to freeze her account

D. The seed phrase is useless without the original laptop

Answer: B

The seed phrase can regenerate all private keys on any compatible wallet software. However, if the laptop was compromised before theft, the thief might have copied the seed phrase or keys. Best practice is to recover funds to a new wallet with a new seed phrase generated on a secure device. The beauty and risk of cryptocurrency is that the seed phrase IS the funds - no administrator can help.

Question 22

A blockchain explorer shows a transaction signature: (r, s). To verify this signature, what do you need?

A. Only the private key
B. The public key, the message (transaction data), and the signature (r, s)
C. The seed phrase
D. The wallet password

Question 22

A blockchain explorer shows a transaction signature: (r, s). To verify this signature, what do you need?

A. Only the private key

B. The public key, the message (transaction data), and the signature (r, s)

C. The seed phrase

D. The wallet password

Answer: B

Signature verification is a public operation. Anyone can verify a signature using: (1) the public key of the claimed signer, (2) the message that was signed (transaction data), and (3) the signature itself (r, s). The verification algorithm confirms the signature could only have been created by someone possessing the corresponding private key, without revealing that key.

Question 23

Bob generates a Bitcoin private key by flipping a coin 256 times. Carol uses a brain wallet, converting her password 'Bitcoin123' to a private key. Who has better security?

A. Carol, because her password is easier to remember

B. Bob, because truly random entropy is more secure than a human-chosen password

C. Both are equally secure

D. Neither method is valid for generating Bitcoin keys

Question 23

Bob generates a Bitcoin private key by flipping a coin 256 times. Carol uses a brain wallet, converting her password 'Bitcoin123' to a private key. Who has better security?

A. Carol, because her password is easier to remember

B. Bob, because truly random entropy is more secure than a human-chosen password

C. Both are equally secure

D. Neither method is valid for generating Bitcoin keys

Answer: B

Bob's method provides 256 bits of true entropy (if the coin is fair). Carol's password has far less entropy - passwords are predictable and easily brute-forced. Brain wallets are notoriously insecure; attackers precompute keys from common passwords and phrases. Bitcoin's secp256k1 requires 256 bits of entropy for security. Proper key generation uses cryptographically secure random number generators (CSPRNG), not human-chosen strings.

Question 24

A hardware wallet signs transactions without exposing the private key to the computer. What cryptographic property makes this possible?

A. Hash functions allow signing without revealing the key

B. Digital signatures can be generated from the private key and transaction data, then transmitted separately to the computer

C. The computer generates the signature and sends it to the hardware wallet

D. Hardware wallets don't actually use cryptography

Question 24

A hardware wallet signs transactions without exposing the private key to the computer. What cryptographic property makes this possible?

A. Hash functions allow signing without revealing the key

B. Digital signatures can be generated from the private key and transaction data, then transmitted separately to the computer

C. The computer generates the signature and sends it to the hardware wallet

D. Hardware wallets don't actually use cryptography

Answer: B

Hardware wallets leverage asymmetric cryptography: the computer sends transaction data to the hardware wallet, which signs it internally using the stored private key and returns only the signature. The private key never leaves the secure element. The computer can then broadcast the signed transaction. This is possible because signature generation only requires the private key and message, while signature verification only requires the public key and signature.

Question 25

Two Bitcoin transactions are created simultaneously spending the same UTXO to different recipients. Both signatures are valid. What determines which transaction is accepted?

A. The transaction with the higher fee is always accepted

B. Both transactions can be included in the blockchain since both signatures are valid

C. Whichever transaction gets included in a block first; the other becomes invalid (double-spend prevented by consensus)

D. The blockchain accepts the transaction with the earlier timestamp

Question 25

Two Bitcoin transactions are created simultaneously spending the same UTXO to different recipients. Both signatures are valid. What determines which transaction is accepted?

A. The transaction with the higher fee is always accepted

B. Both transactions can be included in the blockchain since both signatures are valid

C. Whichever transaction gets included in a block first; the other becomes invalid (double-spend prevented by consensus)

D. The blockchain accepts the transaction with the earlier timestamp

Answer: C

This is the double-spend problem. While both signatures may be cryptographically valid, blockchain consensus ensures only one transaction can spend a UTXO. Miners/validators will include one transaction in a block; once confirmed, the UTXO is spent and the other transaction becomes invalid. Higher fees increase likelihood of faster inclusion, but ultimately ordering is determined by which transaction enters the blockchain first. Cryptography proves authorization; consensus determines ordering.

Question 26 (True/False)

SHA-256 always produces a 256-bit output regardless of input size.

A. True
B. False

Question 26 (True/False)

SHA-256 always produces a 256-bit output regardless of input size.

A. True

B. False

Answer: True

SHA-256 is a cryptographic hash function that always produces a fixed-size 256-bit (32-byte) output, no matter how large or small the input is.

Question 27 (True/False)

Public keys should be kept secret to protect cryptocurrency funds.

A. True
B. False

Question 27 (True/False)

Public keys should be kept secret to protect cryptocurrency funds.

A. True

B. False

Answer: False

Public keys can be shared openly and are used to verify signatures and derive addresses. It's the private key that must be kept secret.

Question 28 (True/False)

Hash functions are reversible, allowing you to find the input from the output.

A. True
B. False

Question 28 (True/False)

Hash functions are reversible, allowing you to find the input from the output.

A. True

B. False

Answer: False

Hash functions are one-way functions. It's computationally infeasible to reverse a hash output to find the original input (pre-image resistance).

Question 29 (True/False)

Digital signatures prove the authenticity and integrity of a message.

A. True
B. False

Question 29 (True/False)

Digital signatures prove the authenticity and integrity of a message.

A. True

B. False

Answer: True

Digital signatures prove that a message was signed by the holder of the private key and that the message hasn't been altered since signing.

Question 30 (True/False)

Symmetric encryption uses the same key for both encryption and decryption.

A. True
B. False

Question 30 (True/False)

Symmetric encryption uses the same key for both encryption and decryption.

A. True

B. False

Answer: True

Symmetric encryption uses a single shared secret key for both encrypting and decrypting data, unlike asymmetric encryption which uses a key pair.

Question 31 (True/False)

A Bitcoin address is identical to the public key.

A. True
B. False

Question 31 (True/False)

A Bitcoin address is identical to the public key.

A. True

B. False

Answer: False

A Bitcoin address is derived from the public key through hashing (RIPEMD-160 of SHA-256) and encoding, but is not the same as the public key itself.

Question 32 (True/False)

The avalanche effect means small changes in input produce dramatically different hash outputs.

A. True
B. False

Question 32 (True/False)

The avalanche effect means small changes in input produce dramatically different hash outputs.

A. True

B. False

Answer: True

The avalanche effect is a property of good hash functions where changing even a single bit in the input results in a completely different output hash.

Question 33 (Fill in the Blank)

SHA-256 produces a ___-bit hash output. *Hint: The number is in the name...*

Question 33 (Fill in the Blank)

SHA-256 produces a ___-bit hash output. *Hint: The number is in the name...* **Answer: 256**

SHA-256 always produces a 256-bit (32-byte) output regardless of input size.

Question 34 (Fill in the Blank)

A digital ___ proves message authenticity. *Hint: Like signing a document...*

Question 34 (Fill in the Blank)

A digital ___ proves message authenticity. *Hint: Like signing a document...* **Answer: signature**

Digital signatures prove that a message was signed by the holder of the private key and hasn't been altered.

Question 35 (Fill in the Blank)

The ___ key is used to decrypt messages. *Hint: It must be kept secret...*

Question 35 (Fill in the Blank)

The ___ key is used to decrypt messages. *Hint: It must be kept secret...* **Answer: private**

In asymmetric cryptography, the private key decrypts messages that were encrypted with the corresponding public key.