Quiz: Hash Functions

Instructions: 10 multiple choice questions — Select the best answer — Answers revealed after each question

Quiz (1–5)

Q1. What is the output size of SHA-256?
A) 128 bits B) 160 bits C) 256 bits D) 512 bits

Quiz (1–5)

Q1. What is the output size of SHA-256?
A) 128 bits B) 160 bits C) 256 bits D) 512 bits
Answer: C – SHA-256 always produces 256-bit (64 hex character) output.

Q2. The avalanche effect means:
A) Hash grows exponentially B) 1-bit change flips 50% output C) Hash cascades D) Network congests

Quiz (1–5)

Q1. What is the output size of SHA-256?
A) 128 bits B) 160 bits C) 256 bits D) 512 bits
Answer: C – SHA-256 always produces 256-bit (64 hex character) output.

Q2. The avalanche effect means:
A) Hash grows exponentially B) 1-bit change flips 50% output C) Hash cascades D) Network congests
Answer: B – Small input change causes large, unpredictable output change.

Q3. Which hash algorithm is used by Bitcoin?
A) MD5 B) SHA-1 C) SHA-256 D) SHA-3

Quiz (1–5)

Q1. What is the output size of SHA-256?
A) 128 bits B) 160 bits C) 256 bits D) 512 bits
Answer: C – SHA-256 always produces 256-bit (64 hex character) output.

Q2. The avalanche effect means:
A) Hash grows exponentially B) 1-bit change flips 50% output C) Hash cascades D) Network congests
Answer: B – Small input change causes large, unpredictable output change.

Q3. Which hash algorithm is used by Bitcoin?
A) MD5 B) SHA-1 C) SHA-256 D) SHA-3
Answer: C – Bitcoin uses double SHA-256 for block hashes.

Q4. Preimage resistance means:
A) Fast computation B) Cannot reverse hash to find input C) Fixed output size D) No collisions

Quiz (1–5)

Q1. What is the output size of SHA-256?
A) 128 bits B) 160 bits C) 256 bits D) 512 bits
Answer: C – SHA-256 always produces 256-bit (64 hex character) output.

Q2. The avalanche effect means:
A) Hash grows exponentially B) 1-bit change flips 50% output C) Hash cascades D) Network congests
Answer: B – Small input change causes large, unpredictable output change.

Q3. Which hash algorithm is used by Bitcoin?
A) MD5 B) SHA-1 C) SHA-256 D) SHA-3
Answer: C – Bitcoin uses double SHA-256 for block hashes.

Q4. Preimage resistance means:
A) Fast computation B) Cannot reverse hash to find input C) Fixed output size D) No collisions
Answer: B – Given hash output, infeasible to find any matching input.

Q5. How many hashes verify a tx in 1,024-tx block using Merkle proof?
A) 5 B) 10 C) 512 D) 1,024

Quiz (1–5)

Q1. What is the output size of SHA-256?
A) 128 bits B) 160 bits C) 256 bits D) 512 bits
Answer: C – SHA-256 always produces 256-bit (64 hex character) output.

Q2. The avalanche effect means:
A) Hash grows exponentially B) 1-bit change flips 50% output C) Hash cascades D) Network congests
Answer: B – Small input change causes large, unpredictable output change.

Q3. Which hash algorithm is used by Bitcoin?
A) MD5 B) SHA-1 C) SHA-256 D) SHA-3
Answer: C – Bitcoin uses double SHA-256 for block hashes.

Q4. Preimage resistance means:
A) Fast computation B) Cannot reverse hash to find input C) Fixed output size D) No collisions
Answer: B – Given hash output, infeasible to find any matching input.

Q5. How many hashes verify a tx in 1,024-tx block using Merkle proof?
A) 5 B) 10 C) 512 D) 1,024
Answer: B – $\log_2 1024 = 10$ hashes for Merkle proof.

Quiz (6–10)

Q6. The birthday paradox implies collision attacks need:
A) 2^n attempts B) $2^{n/2}$ attempts C) n attempts D) $\log n$ attempts

Quiz (6–10)

Q6. The birthday paradox implies collision attacks need:
A) 2^n attempts B) $2^{n/2}$ attempts C) n attempts D) $\log n$ attempts
Answer: B – Birthday bound: $2^{n/2}$ for n-bit hash (SHA-256: 2^{128}).

Q7. Which hash algorithm is considered broken?
A) SHA-256 B) SHA-3 C) MD5 D) BLAKE2

Quiz (6–10)

Q6. The birthday paradox implies collision attacks need:
A) 2^n attempts B) $2^{n/2}$ attempts C) n attempts D) $\log n$ attempts
Answer: B – Birthday bound: $2^{n/2}$ for n-bit hash (SHA-256: 2^{128}).

Q7. Which hash algorithm is considered broken?
A) SHA-256 B) SHA-3 C) MD5 D) BLAKE2
Answer: C – MD5 collisions can be found in seconds; deprecated.

Q8. Merkle trees enable:
A) Faster mining B) Efficient transaction verification C) Larger blocks D) Privacy

Quiz (6–10)

Q6. The birthday paradox implies collision attacks need:
A) 2^n attempts B) $2^{n/2}$ attempts C) n attempts D) $\log n$ attempts
Answer: B – Birthday bound: $2^{n/2}$ for n-bit hash (SHA-256: 2^{128}).

Q7. Which hash algorithm is considered broken?
A) SHA-256 B) SHA-3 C) MD5 D) BLAKE2
Answer: C – MD5 collisions can be found in seconds; deprecated.

Q8. Merkle trees enable:
A) Faster mining B) Efficient transaction verification C) Larger blocks D) Privacy
Answer: B – Merkle proofs verify tx inclusion with $O(\log n)$ hashes.

Q9. Why does Bitcoin use double SHA-256?
A) More secure B) Faster C) Prevents length extension attacks D) Smaller output

Quiz (6–10)

Q6. The birthday paradox implies collision attacks need:
A) 2^n attempts B) $2^{n/2}$ attempts C) n attempts D) $\log n$ attempts
Answer: B – Birthday bound: $2^{n/2}$ for n-bit hash (SHA-256: 2^{128}).

Q7. Which hash algorithm is considered broken?
A) SHA-256 B) SHA-3 C) MD5 D) BLAKE2
Answer: C – MD5 collisions can be found in seconds; deprecated.

Q8. Merkle trees enable:
A) Faster mining B) Efficient transaction verification C) Larger blocks D) Privacy
Answer: B – Merkle proofs verify tx inclusion with $O(\log n)$ hashes.

Q9. Why does Bitcoin use double SHA-256?
A) More secure B) Faster C) Prevents length extension attacks D) Smaller output
Answer: C – Double hashing prevents length extension attacks on SHA-256.

Q10. A collision occurs when:
A) Hash fails B) Two inputs produce same hash C) Output is too long D) Network splits

Quiz (6–10)

Q6. The birthday paradox implies collision attacks need:
A) 2^n attempts B) $2^{n/2}$ attempts C) n attempts D) $\log n$ attempts
Answer: B – Birthday bound: $2^{n/2}$ for n-bit hash (SHA-256: 2^{128}).

Q7. Which hash algorithm is considered broken?
A) SHA-256 B) SHA-3 C) MD5 D) BLAKE2
Answer: C – MD5 collisions can be found in seconds; deprecated.

Q8. Merkle trees enable:
A) Faster mining B) Efficient transaction verification C) Larger blocks D) Privacy
Answer: B – Merkle proofs verify tx inclusion with $O(\log n)$ hashes.

Q9. Why does Bitcoin use double SHA-256?
A) More secure B) Faster C) Prevents length extension attacks D) Smaller output
Answer: C – Double hashing prevents length extension attacks on SHA-256.

Q10. A collision occurs when:
A) Hash fails B) Two inputs produce same hash C) Output is too long D) Network splits
Answer: B – Collision: $H(m_1) = H(m_2)$ where $m_1 \neq m_2$.