◇ EASY (Q1–Q10)

Q1. The primary purpose of a cryptographic hash function is to ensure:
A. Confidentiality
B. Integrity
C. Availability
D. Authentication

Q2. Which property ensures that the same input always produces the same hash output?
A. Collision resistance
B. Determinism
C. Pre-image resistance
D. Avalanche effect

Q3. Which hashing algorithm is considered broken and unsuitable for security use?
A. SHA-256
B. SHA-512
C. MD5
D. SHA-3

Q4. A cryptographic hash function produces output of:
A. Variable length
B. Fixed length
C. Increasing length
D. Input-dependent length

Q5. Which hash property makes it computationally infeasible to find the original message from a hash?
A. Collision resistance
B. Deterministic output
C. Pre-image resistance
D. Diffusion

Q6. Which SHA variant produces a 256-bit message digest?
A. SHA-1
B. SHA-224
C. SHA-256
D. SHA-384

Q7. HMAC is primarily used to provide:
A. Confidentiality only
B. Integrity and authentication
C. Encryption
D. Key exchange

Q8. Which component does HMAC add to a hash function to improve security?
A. Public key
B. Random nonce
C. Secret key
D. Certificate

Q9. Which algorithm family is currently recommended for general-purpose hashing?
A. MD family
B. SHA-1
C. SHA-2
D. CRC

Q10. Which term refers to two different inputs producing the same hash?
A. Pre-image
B. Avalanche
C. Collision
D. Salting

◇ MEDIUM (Q11–Q25)

Q11. Which property of hash functions protects against finding any two different messages with the same hash?
A. Pre-image resistance
B. Second pre-image resistance
C. Collision resistance
D. Determinism

Q12. Why is hashing preferred over encryption for password storage?
A. Hashing is reversible
B. Hashing is faster to decrypt
C. Hashing is one-way
D. Hashing uses larger keys

Q13. What is the primary purpose of adding salt to password hashes?
A. Increase hash length
B. Prevent replay attacks
C. Defend against rainbow table attacks
D. Improve encryption speed

Q14. Which SHA algorithm was officially deprecated due to collision attacks?
A. SHA-256
B. SHA-384
C. SHA-512
D. SHA-1

Q15. Which structure is used internally by SHA-256?
A. Feistel network
B. Merkle–Damgård construction
C. Substitution–Permutation network
D. Sponge construction

Q16. Which SHA family introduced the sponge construction?
A. SHA-1
B. SHA-2
C. SHA-3
D. SHA-256

Q17. Why is plain hashing insufficient for message authentication?
A. Hashing is slow
B. Hashing can be reversed
C. Anyone can recompute the hash
D. Hash output is too long

Q18. Which cryptographic mechanism prevents length extension attacks?
A. Plain SHA-256
B. MD5
C. HMAC
D. CRC

Q19. Which scenario BEST illustrates a collision attack risk?
A. Guessing a password
B. Finding two different files with the same hash
C. Encrypting the same message twice
D. Reusing a symmetric key

Q20. Which hash function output size provides higher collision resistance?
A. 128-bit
B. 160-bit
C. 256-bit
D. 192-bit

Q21. Which component of HMAC is applied in both inner and outer hashing?
A. Public key
B. Initialization vector
C. Padding constants (ipad/opad)
D. Digital certificate

Q22. Which cryptographic service does HMAC NOT provide?
A. Integrity
B. Authentication

C. Non-repudiation
D. Data origin verification

Q23. Which application commonly uses HMAC-SHA256?
A. Disk encryption
B. API request authentication
C. Key exchange
D. Password cracking

Q24. Which hash property ensures small input changes produce large output changes?
A. Determinism
B. Avalanche effect
C. Collision resistance
D. Pre-image resistance

Q25. Which factor MOST influences resistance to brute-force collision attacks?
A. Hash algorithm name
B. Hash output length
C. Password length
D. CPU speed

◇ HARD (Q26–Q40)

Q26. Why are MD5 and SHA-1 unsuitable for digital signatures?
A. They are slow
B. They lack encryption
C. They are vulnerable to collision attacks
D. They produce variable-length output

Q27. Which attack exploits the Merkle–Damgård structure of certain hash functions?
A. Replay attack
B. Length extension attack
C. Side-channel attack
D. Padding oracle attack

Q28. How does HMAC mitigate weaknesses in underlying hash functions?
A. By encrypting the hash
B. By using dual hashing with a secret key
C. By increasing output length
D. By adding random salts per message

Q29. Which security property is MOST critical when verifying software downloads using hashes?
A. Confidentiality

B. Availability
C. Integrity
D. Authentication

Q30. Which hashing approach is MOST suitable for password storage in modern systems?
A. SHA-1
B. SHA-256 without salt
C. MD5 with salt
D. Slow, salted key-derivation functions

Q31. Which cryptographic failure would MOST likely occur if a secret HMAC key is exposed?
A. Hash collisions
B. Loss of message authentication
C. Loss of confidentiality
D. Replay prevention failure

Q32. Which scenario BEST demonstrates second pre-image resistance?
A. Finding any two messages with same hash
B. Finding another message matching a specific hash
C. Reversing a hash to get original message
D. Encrypting a hash

Q33. Which hashing misuse could allow attackers to bypass integrity checks?
A. Using strong hash algorithms
B. Hashing without salting
C. Using broken hash functions
D. Long hash outputs

Q34. Which cryptographic mechanism ensures integrity and authentication without public-key cryptography?
A. Digital signatures
B. HMAC
C. TLS
D. Encryption

Q35. Why is SHA-3 considered more resilient to certain attacks than SHA-2?
A. Larger block size
B. Different internal design (sponge construction)
C. Faster performance
D. Mandatory salting

Q36. Which factor MOST determines the security of HMAC?
A. Hash output size alone
B. Strength of the underlying hash and secrecy of key
C. Algorithm popularity
D. Message length

Q37. Which hash-related attack becomes easier as computational power increases?
A. Replay attack
B. Brute-force collision attack
C. MITM attack
D. Side-channel attack

Q38. Which cryptographic mistake MOST threatens data integrity verification systems?
A. Encrypting hashes
B. Using unsigned hashes
C. Using strong hash functions
D. Long keys

Q39. Which use case MOST benefits from combining hashing with encryption?
A. Password storage
B. Secure file transfer
C. API authentication
D. Key exchange

Q40. Which statement BEST summarizes the role of hashing in cryptography?
A. Hashing replaces encryption
B. Hashing ensures integrity, not confidentiality
C. Hashing provides authentication by itself
D. Hashing enables key exchange