◇ EASY (Q1–Q10)

Q1. Which mathematical concept underpins most modern public-key cryptosystems?
A. Linear algebra only
B. One-way mathematical functions
C. Sorting algorithms
D. Data compression

Q2. Which operation is fundamental to block ciphers?
A. Hash chaining
B. Substitution and permutation
C. Base64 encoding
D. Data framing

Q3. Which cryptographic primitive provides data integrity?
A. Encryption
B. Hash function
C. Key exchange
D. Encoding

Q4. In cryptography, a nonce is primarily used to:
A. Encrypt messages
B. Store keys
C. Ensure freshness and prevent replay
D. Increase key length

Q5. Which cipher uses the same key for encryption and decryption?
A. RSA
B. ECC
C. Symmetric cipher
D. Hash function

Q6. Which asymmetric algorithm is based on integer factorization?
A. AES
B. DES
C. RSA
D. Diffie–Hellman

Q7. Which cryptographic protocol is primarily used for secure web communication?
A. FTP
B. SMTP
C. TLS
D. SNMP

Q8. Which component converts plaintext into ciphertext?
A. Key

B. Algorithm
C. Hash
D. Certificate

Q9. Which cryptographic goal ensures data has not been altered?
A. Confidentiality
B. Integrity
C. Availability
D. Authorization

Q10. Which algorithm is commonly used for key exchange rather than data encryption?
A. AES
B. RSA
C. Diffie–Hellman
D. SHA-256

◇ MEDIUM (Q11–Q25)

Q11. Which statement BEST describes a cryptographic protocol?
A. A single encryption algorithm
B. A set of rules governing secure communication
C. A hardware security device
D. A type of malware

Q12. Why are asymmetric algorithms typically slower than symmetric algorithms?
A. They use smaller keys
B. They involve complex mathematical operations
C. They encrypt less data
D. They avoid hashing

Q13. Which property ensures that encrypted data cannot be decrypted without the correct key?
A. Collision resistance
B. Non-repudiation
C. Computational infeasibility
D. Availability

Q14. In a hybrid cryptosystem, asymmetric encryption is mainly used to:
A. Encrypt bulk data
B. Hash messages
C. Exchange symmetric keys
D. Compress data

Q15. Which protocol feature protects against replay attacks?
A. Static keys

B. Timestamps or nonces
C. Long passwords
D. Key reuse

Q16. Which cipher mode turns a block cipher into a stream-like cipher?
A. ECB
B. CBC
C. CTR
D. ECB-MAC

Q17. Which cryptographic primitive provides non-repudiation when combined with PKI?
A. Hashing
B. Symmetric encryption
C. Digital signatures
D. Encoding

Q18. Which weakness is MOST associated with ECB mode?
A. Padding oracle attacks
B. Pattern leakage
C. High latency
D. Key exhaustion

Q19. Which cryptographic protocol component authenticates the server in TLS?
A. Shared secret
B. Digital certificate
C. Session key
D. MAC

Q20. Which algorithm relies on discrete logarithm problems over finite fields or curves?
A. RSA
B. DES
C. Diffie–Hellman
D. AES

Q21. Why are random numbers critical in cryptography?
A. They speed up encryption
B. They reduce storage
C. They prevent predictability
D. They simplify algorithms

Q22. Which cryptographic service is NOT directly provided by encryption alone?
A. Confidentiality
B. Integrity
C. Availability
D. Privacy

Q23. Which protocol step establishes shared secrets securely over an insecure channel?
A. Hashing
B. Key exchange
C. Encoding
D. Compression

Q24. Which algorithm is MOST appropriate for encrypting real-time streaming data?
A. RSA
B. DES
C. AES in CTR/GCM mode
D. SHA-1

Q25. Which factor MOST influences the security strength of a cryptographic system?
A. Algorithm secrecy
B. Key length and key management
C. File size
D. Network speed

◇ HARD (Q26–Q40)

Q26. Which cryptographic failure would MOST likely occur if predictable IVs are reused?
A. Collision attack
B. Chosen-plaintext attack
C. Replay attack
D. Key escrow

Q27. In Diffie–Hellman, security is primarily based on the difficulty of:
A. Integer factorization
B. Discrete logarithm problem
C. Hash inversion
D. Prime generation

Q28. Which scenario BEST illustrates a man-in-the-middle risk during key exchange?
A. Using strong AES keys
B. Using unauthenticated Diffie–Hellman
C. Using RSA signatures
D. Using certificate pinning

Q29. Why is RSA rarely used to encrypt large files directly?
A. It is insecure
B. It lacks integrity
C. It is computationally expensive
D. It cannot use large keys

Q30. Which cryptographic protocol property ensures both parties verify each other's identity?
A. Confidentiality
B. Mutual authentication
C. Forward secrecy
D. Collision resistance

Q31. Which attack exploits weaknesses in cryptographic protocol design rather than algorithms?
A. Brute-force attack
B. Side-channel attack
C. Protocol downgrade attack
D. Key length attack

Q32. Which protocol improvement in TLS 1.3 MOST enhances security?
A. Support for legacy ciphers
B. Mandatory forward secrecy
C. Static RSA key exchange
D. Longer certificates

Q33. Which cryptographic mechanism ensures past session keys remain secure if a long-term key is compromised?
A. Hash chaining
B. Forward secrecy
C. Key escrow
D. Key reuse

Q34. Which mistake MOST compromises cryptographic protocol security?
A. Using open standards
B. Implementing custom cryptography
C. Using hardware acceleration
D. Using strong randomness

Q35. Which scenario BEST demonstrates protocol-level encryption?
A. Encrypting a ZIP file
B. HTTPS communication
C. Password hashing
D. Disk encryption

Q36. Which cryptographic protocol element prevents message tampering in transit?
A. Plain encryption
B. MAC or AEAD
C. Encoding
D. Key exchange

Q37. Which cryptographic design principle discourages reliance on algorithm secrecy?
A. Defense in depth
B. Kerckhoffs's principle

C. Least privilege
D. Zero trust

Q38. Which cryptographic weakness MOST likely leads to replay attacks?
A. Weak hash function
B. Missing freshness checks
C. Short key length
D. Poor entropy source

Q39. Which cryptographic protocol error allowed early SSL attacks like POODLE?
A. Weak hashing
B. Poor padding handling
C. Insecure certificates
D. Key reuse

Q40. Which factor MOST determines whether a cryptographic protocol is secure in practice?
A. Mathematical elegance
B. Implementation correctness
C. Algorithm age
D. Programming language