◇ EASY (Q1–Q10)

Q1. DES operates on a block size of:
A. 32 bits
B. 56 bits
C. 64 bits
D. 128 bits

Q2. Which algorithm replaced DES as the U.S. federal standard?
A. RSA
B. AES
C. RC5
D. Blowfish

Q3. AES supports which block size?
A. 64 bits
B. 96 bits
C. 128 bits
D. Variable

Q4. Which encryption category does AES belong to?
A. Asymmetric
B. Symmetric
C. Hash-based
D. Stream

Q5. RSA security is primarily based on:
A. Discrete logarithm problem
B. Elliptic curve mathematics
C. Integer factorization problem
D. Hash collisions

Q6. Which algorithm is known for variable rounds and key sizes?
A. DES
B. AES
C. RC5
D. RSA

Q7. ECC achieves similar security to RSA using:
A. Larger keys
B. Smaller keys
C. Identical key sizes
D. No keys

Q8. Which AES key size is considered the strongest?
A. 128-bit

B. 160-bit
C. 192-bit
D. 256-bit

Q9. DES uses how many effective key bits?
A. 64
B. 56
C. 48
D. 32

Q10. Which algorithm is MOST suitable for encrypting large volumes of data?
A. RSA
B. ECC
C. AES
D. DSA

◇ MEDIUM (Q11–Q25)

Q11. Which structural design is used by DES and AES?
A. Feistel network
B. Substitution–Permutation Network
C. Hash chain
D. Stream cipher

Q12. Why is DES considered insecure today?
A. Weak hash function
B. Small block size
C. Short key length
D. Poor padding

Q13. Which AES operation provides diffusion?
A. SubBytes
B. ShiftRows
C. MixColumns
D. AddRoundKey

Q14. Which AES operation introduces non-linearity?
A. MixColumns
B. SubBytes
C. ShiftRows
D. KeyExpansion

Q15. How many rounds does AES-128 use?
A. 8

B. 10
C. 12
D. 14

Q16. RC5 encryption strength depends primarily on:
A. Block size only
B. Key size only
C. Number of rounds, key size, block size
D. Hash function

Q17. Which property makes AES resistant to linear and differential cryptanalysis?
A. Key length
B. SPN structure
C. Block size
D. Hardware acceleration

Q18. In RSA, which key is used for encryption in confidentiality use cases?
A. Sender’s private key
B. Receiver’s public key
C. Receiver’s private key
D. Sender’s public key

Q19. Which RSA operation ensures non-repudiation?
A. Encryption with public key
B. Hashing
C. Signing with private key
D. Symmetric encryption

Q20. Why is ECC preferred in mobile and IoT environments?
A. Faster hashing
B. Lower memory and CPU usage
C. Simpler mathematics
D. Larger block size

Q21. Which AES mode provides both confidentiality and integrity?
A. ECB
B. CBC
C. CTR
D. GCM

Q22. Which weakness is MOST associated with ECB mode?
A. Padding oracle
B. Pattern leakage
C. Replay attack
D. Side-channel leakage

Q23. Which mathematical operation underlies ECC?
A. Modular exponentiation
B. Prime factorization
C. Elliptic curve point multiplication
D. XOR operations

Q24. Which key size is generally considered the minimum secure RSA key today?
A. 512 bits
B. 1024 bits
C. 2048 bits
D. 4096 bits

Q25. Which symmetric algorithm is standardized and widely hardware-accelerated (AES-NI)?
A. DES
B. RC5
C. AES
D. Blowfish

◇ HARD (Q26–Q40)

Q26. Which attack made DES practically breakable in real time?
A. Differential cryptanalysis
B. Linear cryptanalysis
C. Brute-force using dedicated hardware
D. Side-channel attack

Q27. Why is Triple DES slower than AES?
A. Smaller block size
B. Multiple encryption rounds
C. Larger keys
D. Hash dependency

Q28. Which AES round transformation is omitted in the final round?
A. SubBytes
B. ShiftRows
C. MixColumns
D. AddRoundKey

Q29. Which scenario BEST justifies using ECC over RSA?
A. Desktop file encryption
B. High-performance servers
C. Constrained IoT devices
D. Offline backups

Q30. Which RSA vulnerability arises from poor padding implementation?
A. Birthday attack
B. Timing attack
C. Padding oracle attack
D. Collision attack

Q31. Why is RSA not used for bulk data encryption?
A. Weak security
B. Large ciphertext expansion
C. Computational inefficiency
D. Lack of integrity

Q32. Which ECC advantage MOST directly impacts network bandwidth usage?
A. Faster hashing
B. Smaller public keys
C. Larger signatures
D. More rounds

Q33. Which key management issue MOST affects asymmetric cryptography?
A. Key rotation
B. Key escrow
C. Private key protection
D. Session key reuse

Q34. Which design choice makes RC5 flexible across platforms?
A. Fixed block size
B. Fixed rounds
C. Parameterized structure
D. Stream-based operation

Q35. Which cryptographic principle is violated if DES is reused despite known weaknesses?
A. Kerckhoffs's principle
B. Defense in depth
C. Security by obscurity
D. Least privilege

Q36. Which AES key length provides security roughly equivalent to RSA-3072?
A. AES-128
B. AES-192
C. AES-256
D. AES-512

Q37. Which ECC failure would MOST likely result from poor random number generation?
A. Key collision
B. Private key leakage

C. Hash collision
D. Replay attack

Q38. Which attack targets information leaked through power consumption or timing?
A. Brute force
B. Side-channel attack
C. Replay attack
D. MITM

Q39. Which symmetric algorithm design allows efficient implementation in both hardware and software?
A. DES
B. AES
C. RC5
D. One-time pad

Q40. Which cryptographic deployment BEST follows industry best practice?
A. RSA for all encryption needs
B. AES for data + RSA/ECC for key exchange
C. ECC for file encryption
D. DES with longer passwords