◇ EASY (Q1–Q10)

Q1. Diffie–Hellman is primarily used for:
A. Data encryption
B. Digital signatures
C. Secure key exchange
D. Hash generation

Q2. Which cryptographic problem underpins Diffie–Hellman security?
A. Integer factorization
B. Discrete logarithm
C. Hash collision
D. Lattice reduction

Q3. Which value must be kept secret in Diffie–Hellman?
A. Prime number
B. Generator
C. Public key
D. Private key

Q4. Which attack is POSSIBLE if Diffie–Hellman is used without authentication?
A. Brute-force attack
B. Man-in-the-middle attack
C. Side-channel attack
D. Replay attack

Q5. Which type of attack attempts to guess the encryption key directly?
A. Replay attack
B. Brute-force attack
C. MITM attack
D. Traffic analysis

Q6. Which term refers to exploiting information leaked through timing or power usage?
A. Cryptanalysis
B. Side-channel attack
C. Chosen-plaintext attack
D. Replay attack

Q7. Weak encryption keys primarily affect which security property?
A. Availability
B. Confidentiality
C. Non-repudiation
D. Authentication

Q8. Which attack reuses captured authentication data to gain access?
A. Phishing

B. Replay attack
C. Dictionary attack
D. Spoofing

Q9. Which cryptographic issue arises from poor random number generation?
A. Hash collision
B. Key predictability
C. Ciphertext expansion
D. Padding error

Q10. Which attack involves injecting faults to extract cryptographic secrets?
A. Brute force
B. Fault injection attack
C. Replay attack
D. MITM

◇ MEDIUM (Q11–Q25)

Q11. Which Diffie–Hellman variant provides forward secrecy?
A. Static DH
B. Anonymous DH
C. Ephemeral DH (DHE)
D. Weak DH

Q12. Forward secrecy ensures that:
A. Keys are never reused
B. Past session keys remain secure if long-term keys are compromised
C. Encryption is faster
D. Authentication is optional

Q13. Which cryptographic attack assumes the attacker can choose plaintexts to encrypt?
A. Known-plaintext attack
B. Chosen-plaintext attack
C. Ciphertext-only attack
D. Replay attack

Q14. Which scenario BEST illustrates a side-channel attack?
A. Guessing passwords
B. Observing power consumption of a smart card
C. Sniffing network traffic
D. Modifying ciphertext

Q15. Why is authenticated Diffie–Hellman preferred in TLS?
A. Faster encryption

B. Smaller keys
C. Prevention of MITM attacks
D. Reduced certificate usage

Q16. Which cryptographic weakness is MOST likely if the same key is reused across sessions?
A. Forward secrecy loss
B. Collision resistance
C. Availability failure
D. Encoding error

Q17. Which attack targets weaknesses in encryption implementation rather than algorithms?
A. Brute-force attack
B. Side-channel attack
C. Mathematical cryptanalysis
D. Dictionary attack

Q18. Which cryptographic issue is addressed by salting passwords?
A. Replay attacks
B. Rainbow table attacks
C. MITM attacks
D. Traffic analysis

Q19. Which Diffie–Hellman parameter selection MOST improves security?
A. Small prime numbers
B. Fixed generator
C. Large safe primes
D. Short private keys

Q20. Which cryptographic failure allows attackers to decrypt traffic retroactively?
A. Weak hashing
B. Lack of forward secrecy
C. Poor certificate validation
D. Key escrow

Q21. Which attack manipulates protocol messages to downgrade security settings?
A. Replay attack
B. Downgrade attack
C. Collision attack
D. Side-channel attack

Q22. Which encryption attack exploits predictable padding patterns?
A. Brute force
B. Padding oracle attack
C. Replay attack
D. Fault injection

Q23. Which cryptographic principle discourages designing proprietary algorithms?
A. Defense in depth
B. Kerckhoffs's principle
C. Zero trust
D. Least privilege

Q24. Which attack is MOST effective against short symmetric keys?
A. MITM
B. Replay
C. Brute force
D. Side-channel

Q25. Which cryptographic issue arises when encryption keys are hard-coded in software?
A. Availability loss
B. Key compromise
C. Collision
D. Replay

◇ HARD (Q26–Q40)

Q26. Why is unauthenticated Diffie–Hellman insecure in hostile networks?
A. Weak encryption
B. Susceptible to MITM attacks
C. Small key size
D. No hashing

Q27. Which attack extracts cryptographic secrets by inducing hardware errors?
A. Replay attack
B. Fault injection attack
C. Chosen-ciphertext attack
D. Dictionary attack

Q28. Which cryptographic failure MOST contributed to early SSL vulnerabilities?
A. Weak hash functions
B. Poor random number generation
C. Lack of encryption
D. Oversized keys

Q29. Which scenario BEST demonstrates lack of forward secrecy?
A. Session keys regenerated every login
B. Compromise of server private key exposes past sessions
C. Use of ephemeral keys
D. Perfect randomness

Q30. Which attack exploits statistical patterns in encrypted traffic?
A. Traffic analysis
B. Padding oracle
C. Replay attack
D. MITM

Q31. Which cryptographic countermeasure BEST mitigates side-channel attacks?
A. Longer keys
B. Constant-time implementations
C. Stronger algorithms
D. Larger block sizes

Q32. Which Diffie–Hellman misuse leads to small subgroup attacks?
A. Weak prime selection
B. Long private keys
C. Certificate-based authentication
D. Salting

Q33. Which cryptographic issue MOST often results from developers rolling their own crypto?
A. Improved performance
B. Subtle implementation flaws
C. Stronger security
D. Better interoperability

Q34. Which attack combines interception and modification of key exchange messages?
A. Replay attack
B. Brute-force attack
C. Man-in-the-middle attack
D. Dictionary attack

Q35. Which cryptographic design goal is violated when a system relies on secret algorithms?
A. Confidentiality
B. Kerckhoffs's principle
C. Availability
D. Authentication

Q36. Which failure allows attackers to exploit encrypted backups years later?
A. Key rotation
B. No forward secrecy
C. Salting
D. Hashing

Q37. Which cryptographic vulnerability arises from predictable nonces?
A. Collision resistance failure
B. Replay and forgery attacks

C. Availability issues
D. Encoding errors

Q38. Which attack uses partial knowledge of plaintext to break encryption?
A. Ciphertext-only attack
B. Known-plaintext attack
C. Replay attack
D. Traffic analysis

Q39. Which secure implementation practice MOST reduces cryptographic risks?
A. Longer passwords
B. Using standard, well-reviewed libraries
C. Custom algorithms
D. Proprietary protocols

Q40. Which cryptographic issue MOST threatens long-term confidentiality of encrypted data?
A. Weak user passwords
B. Algorithm aging and cryptanalytic advances
C. Network latency
D. Encoding errors