◇ EASY (Q1–Q10)

Q1. PKCS stands for:
A. Public Key Cipher System
B. Private Key Cryptography Standard
C. Public Key Cryptography Standards
D. Protected Key Communication System

Q2. Which organization originally developed PKCS standards?
A. ISO
B. NIST
C. RSA Laboratories
D. IEEE

Q3. PKCS standards primarily relate to:
A. Symmetric encryption only
B. Network protocols
C. Public-key cryptography
D. Operating systems

Q4. Which PKCS standard defines RSA cryptography?
A. PKCS #5
B. PKCS #7
C. PKCS #1
D. PKCS #11

Q5. Which PKCS standard specifies password-based encryption (PBE)?
A. PKCS #1
B. PKCS #5
C. PKCS #7
D. PKCS #12

Q6. FIPS 140-2 is a standard related to:
A. Network security architecture
B. Cryptographic module security
C. Application development
D. Blockchain compliance

Q7. Which authority publishes FIPS standards?
A. ISO
B. IEEE
C. NIST
D. IETF

Q8. Which device is commonly used to store cryptographic keys securely?
A. Smart switch

B. Firewall
C. Hardware Security Module (HSM)
D. Load balancer

Q9. Which PKCS standard defines cryptographic token interfaces?
A. PKCS #7
B. PKCS #11
C. PKCS #12
D. PKCS #1

Q10. FIPS 140-2 compliance is MOST required in which sector?
A. Gaming
B. Government & defense
C. Entertainment
D. Social media

◇ MEDIUM (Q11–Q25)

Q11. Which PKCS standard defines the Cryptographic Message Syntax (CMS)?
A. PKCS #1
B. PKCS #5
C. PKCS #7
D. PKCS #11

Q12. PKCS #12 is commonly used for:
A. Key exchange
B. Secure storage of private keys and certificates
C. Hashing passwords
D. Token authentication

Q13. Which FIPS 140-2 level requires tamper-evident physical security?
A. Level 1
B. Level 2
C. Level 3
D. Level 4

Q14. Which PKCS standard enables applications to use cryptographic hardware without knowing device specifics?
A. PKCS #1
B. PKCS #7
C. PKCS #11
D. PKCS #12

Q15. Which security service is directly enforced by FIPS 140-2?
A. Availability
B. Cryptographic key protection
C. Network routing
D. Access logging

Q16. Which PKCS standard is MOST relevant for secure email (S/MIME)?
A. PKCS #1
B. PKCS #5
C. PKCS #7
D. PKCS #11

Q17. Which cryptographic module requirement is mandatory at all FIPS 140-2 levels?
A. Tamper resistance
B. Role-based authentication
C. Approved algorithms
D. Physical shielding

Q18. Which FIPS level provides the highest physical security?
A. Level 1
B. Level 2
C. Level 3
D. Level 4

Q19. Which PKCS standard defines private key information syntax?
A. PKCS #1
B. PKCS #8
C. PKCS #11
D. PKCS #7

Q20. Which compliance requirement MOST benefits from using an HSM?
A. Faster encryption
B. Key lifecycle management
C. Data compression
D. Network optimization

Q21. Which industry commonly mandates FIPS 140-2 validated modules?
A. Banking & finance
B. Healthcare only
C. Education
D. Retail

Q22. Which FIPS 140-2 level introduces identity-based authentication?
A. Level 1
B. Level 2

C. Level 3
D. Level 4

Q23. Which PKCS standard is used for password-protected key containers (.pfx)?
A. PKCS #7
B. PKCS #8
C. PKCS #11
D. PKCS #12

Q24. Which cryptographic risk is reduced by FIPS validation?
A. Phishing
B. Weak or non-approved algorithms
C. Social engineering
D. Malware infection

Q25. Which component ensures cryptographic operations occur inside secure hardware?
A. Software keystore
B. TPM / HSM
C. File system
D. Hypervisor

◇ HARD (Q26–Q40)

Q26. Which PKCS standard is MOST critical for secure interoperability between cryptographic applications and hardware?
A. PKCS #1
B. PKCS #7
C. PKCS #11
D. PKCS #12

Q27. Which FIPS 140-2 level requires protection against environmental attacks (temperature, voltage)?
A. Level 1
B. Level 2
C. Level 3
D. Level 4

Q28. Why do enterprises prefer FIPS-validated cryptographic modules?
A. They are open source
B. They guarantee absolute security
C. They meet regulatory and compliance requirements
D. They eliminate key management

Q29. Which PKCS standard would MOST likely be involved in code-signing workflows?
A. PKCS #1
B. PKCS #7
C. PKCS #11
D. PKCS #12

Q30. Which failure would MOST violate FIPS 140-2 requirements?
A. Use of AES-256
B. Use of non-approved random number generator
C. Key rotation
D. HSM usage

Q31. Which PKCS component enables separation of key storage and application logic?
A. PKCS #1
B. PKCS #5
C. PKCS #11
D. PKCS #12

Q32. Which scenario BEST justifies using an HSM?
A. Encrypting test files
B. Protecting root CA private keys
C. Storing user passwords
D. Compressing backups

Q33. Which cryptographic issue is MOST mitigated by hardware-based key storage?
A. Hash collision
B. Private key extraction
C. Replay attacks
D. Network sniffing

Q34. Which PKCS standard defines syntax for encrypted private keys?
A. PKCS #1
B. PKCS #7
C. PKCS #8
D. PKCS #11

Q35. Which FIPS 140-2 misconception is INCORRECT?
A. FIPS validation applies to cryptographic modules, not systems
B. FIPS guarantees perfect security
C. FIPS specifies approved algorithms
D. FIPS enforces operational requirements

Q36. Which PKCS standard is MOST relevant for TLS private key storage?
A. PKCS #1
B. PKCS #7

C. PKCS #8
D. PKCS #11

Q37. Which compliance risk remains EVEN with FIPS-validated modules?
A. Weak cryptographic algorithms
B. Poor operational security
C. Lack of key protection
D. Use of HSM

Q38. Which factor MOST influences FIPS validation scope?
A. Programming language
B. Cryptographic module boundary
C. Network topology
D. CPU speed

Q39. Which cryptographic architecture BEST supports regulatory audits?
A. Custom crypto libraries
B. Software-only key storage
C. FIPS-validated HSM deployment
D. Ad-hoc encryption

Q40. Which statement BEST summarizes PKCS & FIPS 140-2 roles?
A. They replace encryption algorithms
B. They define implementation and compliance standards
C. They eliminate security risks
D. They enforce network security policies