◇ EASY (Q1–Q10)

Q1. A Certificate Authority (CA) is responsible for:
A. Encrypting user data
B. Issuing and signing digital certificates
C. Managing symmetric keys
D. Monitoring network traffic

Q2. Which trust model is MOST commonly used on the Internet?
A. Web-of-Trust
B. Peer-to-peer
C. Hierarchical
D. Decentralized

Q3. Which entity validates identity before certificate issuance?
A. End user
B. Relying party
C. Registration Authority
D. Root CA

Q4. Which certificate revocation mechanism uses a query-response model?
A. CRL
B. OCSP
C. CSR
D. CA bundle

Q5. Which certificate is typically installed in browsers by default?
A. Server certificate
B. Intermediate certificate
C. Root certificate
D. Client certificate

Q6. Which certificate type is used to secure email communication?
A. Code-signing certificate
B. SSL/TLS certificate
C. S/MIME certificate
D. Client authentication certificate

Q7. Which trust model is used by PGP?
A. Hierarchical trust
B. Centralized trust
C. Web-of-Trust
D. Hybrid trust

Q8. Certificate revocation is required when:
A. Certificate expires

B. Private key is compromised
C. Certificate is renewed
D. Hash algorithm is strong

Q9. Which protocol reduces client-side OCSP lookup latency?
A. CRL distribution
B. OCSP stapling
C. Key escrow
D. Certificate pinning

Q10. Which certificate field identifies the certificate owner?
A. Issuer
B. Serial number
C. Subject
D. Signature algorithm

◇ MEDIUM (Q11–Q25)

Q11. Which CA type signs end-entity certificates directly?
A. Root CA
B. Intermediate CA
C. Cross CA
D. Bridge CA

Q12. Why is the root CA kept offline in many PKI deployments?
A. To improve performance
B. To reduce network latency
C. To minimize risk of compromise
D. To simplify certificate validation

Q13. Which certificate revocation method is more scalable for large PKIs?
A. Static CRL
B. Delta CRL
C. OCSP
D. Manual revocation

Q14. Which trust model allows organizations to establish mutual trust without a single root?
A. Hierarchical
B. Web-of-Trust
C. Bridge trust
D. Centralized

Q15. Which step occurs AFTER identity verification in certificate issuance?
A. CSR generation

B. Key pair generation
C. Certificate signing
D. Certificate request

Q16. Which certificate attribute restricts a CA's ability to issue certificates?
A. Subject
B. Basic Constraints
C. Key Usage
D. SAN

Q17. Which mechanism allows clients to verify certificate status without downloading CRLs?
A. Certificate pinning
B. OCSP
C. CSR
D. Key escrow

Q18. Which certificate type verifies the identity of an organization behind a website?
A. Domain Validation (DV)
B. Organization Validation (OV)
C. Extended Validation (EV)
D. Self-signed

Q19. Which PKI component publishes CRLs?
A. Registration Authority
B. End entity
C. Certificate Authority
D. Relying party

Q20. Which attack exploits compromised or malicious CAs?
A. Brute-force attack
B. Supply-chain attack
C. Trust chain attack
D. Replay attack

Q21. Which certificate lifecycle phase involves replacing an expiring certificate?
A. Revocation
B. Suspension
C. Renewal
D. Validation

Q22. Which mechanism binds multiple domain names to a single certificate?
A. CN
B. Key Usage
C. SAN
D. Issuer

Q23. Which trust model MOST simplifies enterprise certificate management?
A. Web-of-Trust
B. Hierarchical
C. Peer-based
D. Decentralized

Q24. Which certificate is used for authenticating users to enterprise systems?
A. Server certificate
B. Client authentication certificate
C. Code-signing certificate
D. Root certificate

Q25. Which certificate revocation drawback applies MOST to CRLs?
A. Real-time validation
B. High network overhead
C. Strong authentication
D. Fast response

◇ HARD (Q26–Q40)

Q26. Which PKI compromise would have the MOST widespread impact?
A. End-entity private key compromise
B. Intermediate CA compromise
C. Root CA compromise
D. Client certificate expiry

Q27. Which trust model BEST supports cross-organization PKI interoperability?
A. Hierarchical
B. Web-of-Trust
C. Bridge trust
D. Centralized

Q28. Which scenario MOST justifies certificate revocation instead of expiration?
A. Certificate nearing end date
B. Hash algorithm upgrade
C. Private key theft
D. Routine renewal

Q29. Which OCSP deployment risk is mitigated by OCSP stapling?
A. Replay attacks
B. Privacy leakage
C. Certificate spoofing
D. Key compromise

Q30. Which PKI weakness can be exploited in “rogue CA” attacks?
A. Weak encryption
B. Trust anchor compromise
C. Short key length
D. Hash collision

Q31. Which certificate class provides the highest level of user-visible trust?
A. DV
B. OV
C. EV
D. Self-signed

Q32. Which PKI control MOST directly supports non-repudiation?
A. Certificate revocation
B. Secure private key storage
C. Certificate renewal
D. CRL publication

Q33. Which certificate attribute ensures certificates cannot be used beyond intended purposes?
A. Issuer
B. Serial number
C. Key Usage / Extended Key Usage
D. Subject

Q34. Which revocation method is BEST for high-frequency, real-time status checking?
A. Full CRL
B. Delta CRL
C. OCSP
D. Manual revocation

Q35. Which PKI operational mistake MOST increases attack surface?
A. Using intermediate CAs
B. Keeping root CA offline
C. Overly long certificate validity
D. Certificate renewal automation

Q36. Which trust failure allows attackers to impersonate any website?
A. Expired end certificate
B. Misconfigured SAN
C. Compromised root CA
D. OCSP timeout

Q37. Which cryptographic operation forms the basis of certificate chaining?
A. Hashing
B. Symmetric encryption

C. Digital signature verification
D. Encoding

Q38. Which enterprise PKI feature MOST improves scalability?
A. Single CA deployment
B. Multiple root CAs
C. Intermediate CAs
D. Manual issuance

Q39. Which PKI risk arises from long-lived certificates?
A. Faster encryption
B. Reduced CPU usage
C. Extended exposure window
D. Better performance

Q40. Which statement BEST summarizes CA trust models?
A. Web-of-Trust is simpler than hierarchical PKI
B. Hierarchical trust centralizes and simplifies validation
C. Bridge trust eliminates the need for CAs
D. Trust models replace cryptography