

## ◊ EASY (Q1–Q10)

**Q1.** The primary purpose of Public Key Infrastructure (PKI) is to:

- A. Encrypt all network traffic
- B. Manage and distribute symmetric keys
- C. Establish trust using public-key cryptography
- D. Replace firewalls

**Q2.** Which entity issues and signs digital certificates?

- A. Registration Authority
- B. Certificate Authority
- C. End Entity
- D. Relying Party

**Q3.** Which cryptographic primitive is essential for digital signatures?

- A. Symmetric encryption
- B. Hash functions
- C. Encoding
- D. Compression

**Q4.** A digital signature primarily ensures:

- A. Confidentiality only
- B. Integrity and authentication
- C. Availability
- D. Anonymity

**Q5.** Which key is used to create a digital signature?

- A. Sender's public key
- B. Receiver's public key
- C. Sender's private key
- D. Receiver's private key

**Q6.** Which standard defines the format of digital certificates?

- A. PKCS #1
- B. X.509
- C. TLS
- D. ASN.1

**Q7.** Which PKI component verifies the identity of a certificate requester?

- A. Certificate Authority
- B. Registration Authority
- C. Root CA
- D. OCSP responder

**Q8.** Which security service ensures a sender cannot deny sending a message?

- A. Confidentiality

- B. Integrity
- C. Non-repudiation
- D. Availability

**Q9.** A self-signed certificate is typically issued by:

- A. A trusted public CA
- B. An intermediate CA
- C. The certificate owner itself
- D. A registration authority

**Q10.** Which element binds an identity to a public key?

- A. Hash
  - B. Digital certificate
  - C. Session key
  - D. Symmetric cipher
- 

## ◊ MEDIUM (Q11–Q25)

**Q11.** Which PKI trust model is MOST commonly used on the Internet?

- A. Web-of-Trust
- B. Hierarchical trust model
- C. Peer-to-peer trust
- D. Distributed trust

**Q12.** In PKI, what is the primary role of an intermediate CA?

- A. Store certificates
- B. Reduce risk to the root CA
- C. Validate user passwords
- D. Generate symmetric keys

**Q13.** Which step occurs FIRST in digital signature generation?

- A. Encrypting the message
- B. Hashing the message
- C. Exchanging keys
- D. Verifying the certificate

**Q14.** Which digital signature property ensures message integrity?

- A. Encryption
- B. Hash comparison
- C. Certificate expiration
- D. Key escrow

**Q15.** What does a Certificate Signing Request (CSR) primarily contain?

- A. Private key only

- B. Public key and identity information
- C. Session key
- D. Encrypted message

**Q16.** Which certificate field specifies how the certificate can be used (e.g., signing, encryption)?

- A. Issuer
- B. Subject
- C. Key Usage
- D. Serial Number

**Q17.** Which mechanism is used to check whether a certificate has been revoked?

- A. Key escrow
- B. OCSP or CRL
- C. CSR
- D. TLS handshake

**Q18.** Which attack becomes possible if certificate validation is skipped?

- A. Brute-force attack
- B. Man-in-the-Middle attack
- C. Replay attack
- D. Side-channel attack

**Q19.** Which algorithm is commonly used for digital signatures in modern systems?

- A. AES
- B. SHA-1
- C. RSA or ECDSA
- D. Diffie–Hellman

**Q20.** Why are hash functions used in digital signatures instead of signing entire messages?

- A. To increase confidentiality
- B. To reduce computational overhead
- C. To avoid key exchange
- D. To encrypt data

**Q21.** Which certificate type is typically used to secure HTTPS websites?

- A. Code-signing certificate
- B. Client authentication certificate
- C. SSL/TLS server certificate
- D. Email certificate

**Q22.** Which PKI component publishes Certificate Revocation Lists?

- A. Registration Authority
- B. End entity
- C. Certificate Authority
- D. Relying party

**Q23.** Which scenario BEST demonstrates non-repudiation?

- A. Encrypted email transmission
- B. Digitally signed contract
- C. Hashed password storage
- D. VPN tunnel establishment

**Q24.** Which property ensures that a modified signed message is detected?

- A. Confidentiality
- B. Integrity
- C. Availability
- D. Authorization

**Q25.** Which trust failure has the MOST severe impact on PKI?

- A. Expired end-entity certificate
  - B. Compromised intermediate CA
  - C. Compromised root CA
  - D. Missing CSR
- 

## ◊ HARD (Q26–Q40)

**Q26.** Which sequence correctly represents digital signature verification?

- A. Decrypt message → hash → compare
- B. Hash message → decrypt signature → compare hashes
- C. Encrypt hash → compare ciphertext
- D. Decrypt certificate → hash message

**Q27.** Which failure MOST likely leads to fraudulent certificates being accepted globally?

- A. Weak hash algorithm
- B. Compromised root CA
- C. Expired certificate
- D. Short key length

**Q28.** Why are private keys of CAs often stored in Hardware Security Modules (HSMs)?

- A. To improve network speed
- B. To prevent unauthorized key extraction
- C. To simplify certificate issuance
- D. To encrypt user data

**Q29.** Which digital signature property relies on asymmetric cryptography?

- A. Integrity only
- B. Authentication only
- C. Non-repudiation
- D. Availability

**Q30.** Which attack exploits improper certificate chain validation?

- A. Dictionary attack
- B. Downgrade attack
- C. Man-in-the-Middle attack
- D. Brute-force attack

**Q31.** Which PKI design choice MOST improves scalability and security?

- A. Single root CA issuing all certificates
- B. Hierarchical CA structure
- C. Web-of-Trust only
- D. Self-signed certificates

**Q32.** Which scenario BEST illustrates certificate revocation necessity?

- A. Certificate nearing expiry
- B. Private key compromise
- C. New employee onboarding
- D. Hash algorithm upgrade

**Q33.** Which cryptographic guarantee does a digital certificate itself NOT provide?

- A. Identity binding
- B. Public key authenticity
- C. Confidentiality of messages
- D. Trust establishment

**Q34.** Which certificate extension allows multiple domain names in one certificate?

- A. Key Usage
- B. Subject Alternative Name (SAN)
- C. Issuer Alternative Name
- D. Basic Constraints

**Q35.** Which PKI weakness can lead to “trust on first use” risks?

- A. CRL usage
- B. Self-signed certificates
- C. OCSP stapling
- D. Intermediate CAs

**Q36.** Which digital signature misuse could invalidate non-repudiation?

- A. Using strong hash functions
- B. Sharing private keys
- C. Certificate validation
- D. Time-stamping

**Q37.** Which mechanism provides proof that a signature existed at a specific time?

- A. Certificate chain
- B. Time-stamping authority

- C. OCSP
- D. Key escrow

**Q38.** Which cryptographic operation links certificate trust transitively?

- A. Hashing
- B. Encryption
- C. Certificate signing
- D. Encoding

**Q39.** Which enterprise security requirement MOST depends on PKI?

- A. Network segmentation
- B. Identity authentication
- C. Data compression
- D. Load balancing

**Q40.** Which statement BEST summarizes PKI's role in security architectures?

- A. PKI encrypts all data
- B. PKI replaces symmetric encryption
- C. PKI establishes trust for secure communication
- D. PKI prevents all cyber attacks