◇ EASY (Q1–Q10)

Q1. SSL and TLS are primarily used to provide security at which layer?
A. Application layer
B. Transport layer
C. Network layer
D. Data link layer

Q2. Which protocol is the successor to SSL?
A. HTTPS
B. SSH
C. TLS
D. IPsec

Q3. Which cryptographic approach is used by TLS?
A. Only symmetric encryption
B. Only asymmetric encryption
C. Hybrid cryptography
D. Hashing only

Q4. Which protocol is MOST commonly used to secure web traffic?
A. FTP
B. SMTP
C. TLS
D. SNMP

Q5. PGP is primarily designed to secure:
A. Network routing
B. Disk storage
C. Email communication
D. Web sessions

Q6. S/MIME relies on which trust mechanism?
A. Web-of-Trust
B. Hierarchical PKI
C. Peer trust
D. Blockchain trust

Q7. Which SSL/TLS component authenticates the server?
A. Session key
B. Digital certificate
C. Hash function
D. MAC address

Q8. Which protocol provides end-to-end email encryption?
A. TLS

B. PGP
C. HTTP
D. FTP

Q9. Which SSL version is considered insecure and deprecated?
A. SSL 3.0
B. TLS 1.3
C. TLS 1.2
D. HTTPS

Q10. Which email security standard is widely used in enterprises?
A. PGP
B. S/MIME
C. POP3
D. IMAP

◇ MEDIUM (Q11–Q25)

Q11. Which TLS feature ensures past sessions remain secure even if long-term keys are compromised?
A. Encryption
B. Integrity
C. Forward secrecy
D. Compression

Q12. Which algorithm is MOST commonly used for bulk data encryption in TLS?
A. RSA
B. ECC
C. AES
D. SHA-256

Q13. Which TLS handshake step involves exchanging supported cipher suites?
A. ServerHello
B. ClientHello
C. Certificate
D. Finished

Q14. Why is SSL no longer recommended for secure communication?
A. Lack of encryption
B. Vulnerabilities and weak design
C. Large key sizes
D. Poor performance

Q15. Which PGP feature eliminates the need for a centralized CA?
A. Symmetric encryption
B. Web-of-Trust
C. Digital certificates
D. HMAC

Q16. Which cryptographic operation provides integrity in TLS records?
A. Encryption
B. MAC / AEAD
C. Key exchange
D. Encoding

Q17. Which S/MIME component binds an email address to a public key?
A. Hash
B. Session key
C. Digital certificate
D. OTP

Q18. Which protocol uses X.509 certificates by default?
A. PGP
B. TLS
C. Both TLS and S/MIME
D. PGP and SSH

Q19. Which PGP key is used to decrypt the session key?
A. Sender's public key
B. Sender's private key
C. Receiver's public key
D. Receiver's private key

Q20. Which TLS improvement was introduced in TLS 1.3?
A. Support for SSL
B. Static RSA key exchange
C. Reduced handshake latency
D. Optional encryption

Q21. Which attack exploited SSL padding weaknesses (e.g., POODLE)?
A. Replay attack
B. Padding oracle attack
C. Brute-force attack
D. Side-channel attack

Q22. Which email security approach is easier to manage in large organizations?
A. PGP
B. S/MIME

C. Plain TLS
D. SMTP

Q23. Which TLS component verifies message integrity and authenticity?
A. Certificate chain
B. MAC / AEAD
C. Public key
D. Session ID

Q24. Which protocol secures data only in transit, not end-to-end?
A. PGP
B. S/MIME
C. TLS
D. OpenPGP

Q25. Which cryptographic function is used by PGP before signing a message?
A. Encryption
B. Hashing
C. Encoding
D. Compression

◇ HARD (Q26–Q40)

Q26. Which failure MOST undermines TLS security despite strong encryption?
A. Long key sizes
B. Improper certificate validation
C. Hardware acceleration
D. Strong randomness

Q27. Why does PGP scale poorly in enterprise environments?
A. Weak encryption
B. Complex key and trust management
C. Lack of hashing
D. Short key lengths

Q28. Which TLS key exchange mechanism provides forward secrecy?
A. RSA
B. Static DH
C. ECDHE
D. DSA

Q29. Which S/MIME weakness MOST affects deployment cost?
A. Weak algorithms
B. Certificate management overhead

C. Lack of integrity
D. No encryption

Q30. Which attack becomes feasible if certificate chains are not verified correctly?
A. Brute force
B. Man-in-the-Middle
C. Replay attack
D. Side-channel attack

Q31. Which PGP design choice complicates revocation?
A. Asymmetric encryption
B. Web-of-Trust
C. Hashing
D. Compression

Q32. Which TLS 1.3 change improves privacy against passive observers?
A. Plaintext certificates
B. Encrypted handshake messages
C. Static session keys
D. Optional MAC

Q33. Which security property does S/MIME provide that plain TLS email does NOT?
A. Transport security
B. End-to-end non-repudiation
C. Faster delivery
D. Compression

Q34. Which cryptographic misuse would MOST invalidate non-repudiation in PGP?
A. Strong hashing
B. Sharing private keys
C. Using large key sizes
D. Encrypting attachments

Q35. Which protocol-level decision MOST improves TLS performance?
A. Longer certificates
B. Session resumption
C. Larger RSA keys
D. More handshake rounds

Q36. Which email security model allows users to decide whom to trust?
A. Hierarchical PKI
B. Centralized CA
C. Web-of-Trust
D. Bridge CA

Q37. Which TLS implementation mistake MOST exposes users to downgrade attacks?
A. Strong cipher suites
B. Allowing legacy protocol fallback
C. Certificate pinning
D. Forward secrecy

Q38. Which cryptographic property ensures emails cannot be altered undetected in S/MIME?
A. Confidentiality
B. Availability
C. Integrity
D. Anonymity

Q39. Which combined deployment BEST secures enterprise email communication?
A. TLS only
B. PGP only
C. S/MIME with PKI
D. SMTP with passwords

Q40. Which statement BEST summarizes SSL/TLS vs PGP/S/MIME?
A. All provide end-to-end encryption
B. TLS secures transport; PGP/S/MIME secure content
C. PGP replaces TLS
D. SSL is still recommended