

❖ EASY (Q1–Q10)

Q1. The CIA triad in information security stands for:

- A. Control, Inspection, Authorization
- B. Confidentiality, Integrity, Availability
- C. Cryptography, Identity, Authentication
- D. Control, Integrity, Audit

Q2. Which encryption type uses the same key for encryption and decryption?

- A. Asymmetric
- B. Symmetric
- C. Hashing
- D. Encoding

Q3. Which protocol secures web traffic?

- A. FTP
- B. SMTP
- C. TLS
- D. SNMP

Q4. Which algorithm is used for secure hashing?

- A. AES
- B. RSA
- C. SHA-256
- D. DES

Q5. Which entity issues digital certificates?

- A. Registration Authority
- B. Certificate Authority
- C. UIDAI
- D. TSA

Q6. Which authentication factor is “something you are”?

- A. Password
- B. Smart card
- C. Fingerprint
- D. OTP

Q7. Which IT Act section covers unauthorized system access?

- A. Section 43
- B. Section 67
- C. Section 79
- D. Section 66F

Q8. LDAP is mainly used for:

- A. Encryption

- B. Directory services
- C. Blockchain mining
- D. Web hosting

Q9. Blockchain ensures data integrity using:

- A. Symmetric encryption
- B. Hashing
- C. Encoding
- D. Compression

Q10. Which PKCS standard defines RSA cryptography?

- A. PKCS #5
 - B. PKCS #7
 - C. PKCS #1
 - D. PKCS #11
-

◊ MEDIUM (Q11–Q25)

Q11. Which attack primarily affects availability?

- A. Phishing
- B. DoS
- C. SQL injection
- D. Sniffing

Q12. Which AES mode provides confidentiality and integrity?

- A. ECB
- B. CBC
- C. CTR
- D. GCM

Q13. Diffie–Hellman is vulnerable to MITM if it lacks:

- A. Hashing
- B. Authentication
- C. Encryption
- D. Salting

Q14. Which hash property prevents finding two inputs with the same hash?

- A. Determinism
- B. Pre-image resistance
- C. Collision resistance
- D. Avalanche effect

Q15. Which PKI component verifies user identity before certificate issuance?

- A. CA

- B. RA
- C. TSA
- D. OCSP

Q16. Which authentication protocol uses tickets?

- A. OAuth
- B. LDAP
- C. Kerberos
- D. RADIUS

Q17. Which OAuth token is used to access APIs?

- A. ID token
- B. Refresh token
- C. Access token
- D. Session cookie

Q18. Which TLS feature protects past sessions if keys are compromised?

- A. Encryption
- B. Integrity
- C. Forward secrecy
- D. Compression

Q19. Which certificate revocation mechanism is real-time?

- A. CRL
- B. Delta CRL
- C. OCSP
- D. CSR

Q20. Which Aadhaar feature improves privacy?

- A. Central storage
- B. Biometric reuse
- C. Virtual ID
- D. OTP reuse

Q21. Which AD object applies security policies?

- A. Forest
- B. Domain
- C. OU
- D. Global Catalog

Q22. Which blockchain consensus does Bitcoin use?

- A. PoS
- B. PBFT
- C. PoW
- D. PoA

Q23. Which PKCS standard defines cryptographic token interfaces?

- A. PKCS #7
- B. PKCS #11
- C. PKCS #12
- D. PKCS #8

Q24. Which authentication method is MOST phishing-resistant?

- A. Password
- B. SMS OTP
- C. Hardware security key
- D. Security questions

Q25. Which SSO protocol uses XML assertions?

- A. OAuth
 - B. OpenID Connect
 - C. SAML
 - D. Kerberos
-

◊ HARD (Q26–Q40)

Q26. Which failure MOST undermines TLS security?

- A. Long keys
- B. Poor certificate validation
- C. AES encryption
- D. Hardware acceleration

Q27. Which cryptographic issue causes permanent data loss in EFS?

- A. Weak algorithm
- B. Certificate/key loss
- C. Small file size
- D. Hash collision

Q28. Which attack exploits power consumption or timing?

- A. MITM
- B. Replay
- C. Side-channel
- D. Brute force

Q29. Which PKI compromise has global impact?

- A. End-user key leak
- B. Intermediate CA compromise
- C. Root CA compromise
- D. Certificate expiry

Q30. Which Zero Trust principle replaces perimeter security?

- A. Trust internal network
- B. Assume breach
- C. Encrypt everything
- D. Static ACLs

Q31. Which blockchain attack occurs if one entity controls majority mining power?

- A. Sybil
- B. Eclipse
- C. 51% attack
- D. Replay

Q32. Which cryptographic practice MOST supports non-repudiation?

- A. Encryption
- B. Hashing
- C. Digital signatures
- D. Encoding

Q33. Which IT Act challenge affects cross-border cybercrime?

- A. Weak hashing
- B. Jurisdiction
- C. Encryption strength
- D. PKI absence

Q34. Which FIPS 140-2 level provides highest physical security?

- A. Level 1
- B. Level 2
- C. Level 3
- D. Level 4

Q35. Which FIDO feature prevents credential reuse across sites?

- A. Long passwords
- B. Origin-bound keys
- C. Central storage
- D. Encryption only

Q36. Which LDAP security issue arises from plaintext binds?

- A. Replay
- B. Credential sniffing
- C. Hash collision
- D. DoS

Q37. Which cryptographic failure allows downgrade attacks?

- A. Strong ciphers
- B. Legacy protocol fallback

- C. Forward secrecy
- D. Certificate pinning

Q38. Which blockchain property conflicts with “right to be forgotten”?

- A. Transparency
- B. Decentralization
- C. Immutability
- D. Scalability

Q39. Which enterprise key should ALWAYS be stored in an HSM?

- A. User session key
- B. Root CA private key
- C. Password hash
- D. OTP secret

Q40. Which statement BEST summarizes the full syllabus?

- A. Cryptography alone ensures security
- B. Security requires law, identity, crypto, and trust
- C. Blockchain replaces PKI
- D. Authentication replaces encryption