◇ EASY (Q1–Q10)

Q1. Aadhaar is primarily used in India as a:
A. Payment gateway
B. Digital identity system
C. Blockchain wallet
D. Email authentication system

Q2. e-Sign in India is legally recognized under which Act?
A. Companies Act
B. IT Act, 2000
C. Evidence Act
D. Cyber Security Act

Q3. Which authority issues Aadhaar numbers?
A. RBI
B. UIDAI
C. CERT-In
D. MeitY

Q4. e-Sign is based on which cryptographic principle?
A. Symmetric encryption
B. Hashing only
C. Asymmetric cryptography
D. Encoding

Q5. Which Aadhaar factor is used for biometric authentication?
A. OTP
B. PIN
C. Fingerprint / Iris
D. Password

Q6. Time Stamping Services primarily ensure:
A. Confidentiality
B. Integrity and time validity
C. Availability
D. Anonymity

Q7. Which entity provides trusted time stamps?
A. Certificate Authority
B. Time Stamping Authority (TSA)
C. Registration Authority
D. UIDAI

Q8. A time stamp proves that data:
A. Was encrypted

B. Was hashed
C. Existed at a specific time
D. Was confidential

Q9. Which cryptographic component is signed in time stamping?
A. Plaintext
B. Encrypted message
C. Hash of the data
D. Public key

Q10. Aadhaar authentication supports which mode?
A. Offline only
B. Online only
C. Both online and offline
D. Manual verification only

◇ MEDIUM (Q11–Q25)

Q11. Which Aadhaar authentication factor is classified as “knowledge-based”?
A. Fingerprint
B. Iris
C. OTP
D. Face recognition

Q12. e-Sign differs from traditional digital signatures because it:
A. Does not use PKI
B. Uses Aadhaar-based authentication
C. Is not legally valid
D. Uses symmetric encryption

Q13. Which component stores Aadhaar demographic and biometric data?
A. UID token
B. Central Identities Data Repository (CIDR)
C. Registration Authority
D. Empanelled Agency

Q14. Which e-Sign advantage MOST improves usability?
A. Offline signing
B. No physical token required
C. Manual key generation
D. Self-signed certificates

Q15. Which cryptographic hash property is MOST relevant for time stamping?
A. Determinism

B. Collision resistance
C. Reversibility
D. Compression

Q16. Which e-Sign use case is MOST common in India?
A. Email encryption
B. Government e-services
C. Cryptocurrency signing
D. VPN authentication

Q17. Which risk is MOST associated with Aadhaar-based authentication?
A. Hash collision
B. Privacy concerns
C. Replay attack only
D. Weak encryption

Q18. Which legal concept does time stamping directly support?
A. Confidentiality
B. Authorization
C. Non-repudiation
D. Availability

Q19. Which Aadhaar authentication mode does NOT require biometric data?
A. Fingerprint
B. Iris
C. OTP
D. Face authentication

Q20. Which cryptographic mechanism links time stamps with PKI trust?
A. Encoding
B. Digital signatures
C. Compression
D. Symmetric encryption

Q21. Which organization regulates e-Sign service providers in India?
A. UIDAI
B. RBI
C. Controller of Certifying Authorities (CCA)
D. CERT-In

Q22. Which attack can be mitigated using trusted time stamps?
A. Replay attack
B. Dispute over document creation time
C. Brute-force attack
D. Side-channel attack

Q23. Which Aadhaar feature supports privacy by minimizing data exposure?
A. Central storage
B. Virtual ID (VID)
C. Biometric capture
D. CIDR

Q24. Which cryptographic element ensures e-Sign signatures cannot be forged?
A. Hash length
B. Private key protection
C. Encoding scheme
D. Key reuse

Q25. Which property ensures time stamps remain verifiable in the future?
A. Encryption strength
B. Trusted TSA signature
C. Short key length
D. Offline storage

◇ HARD (Q26–Q40)

Q26. Which scenario BEST demonstrates legal validity of e-Sign?
A. Password-protected PDF
B. Aadhaar-authenticated digitally signed agreement
C. Scanned handwritten signature
D. Encrypted email

Q27. Which failure would MOST undermine trust in Aadhaar-based e-Sign?
A. Network latency
B. Compromise of authentication mechanism
C. Large key size
D. Hash collision resistance

Q28. Which cryptographic weakness could allow falsified time stamps?
A. Strong hashing
B. Compromised TSA private key
C. Long hash output
D. Multiple TSAs

Q29. Which privacy risk arises if Aadhaar authentication logs are misused?
A. Data corruption
B. Identity profiling
C. Denial of service
D. Encryption failure

Q30. Which time stamping component ensures tamper evidence?
A. Plain timestamp value
B. Hash of data
C. TSA digital signature
D. System clock

Q31. Which cryptographic service does Aadhaar-based e-Sign NOT directly provide?
A. Authentication
B. Integrity
C. Non-repudiation
D. Confidentiality

Q32. Which attack becomes feasible if Aadhaar OTPs are intercepted?
A. Collision attack
B. Replay or impersonation attack
C. Side-channel attack
D. Padding oracle attack

Q33. Which principle ensures Aadhaar data usage is limited to intended purpose?
A. Least privilege
B. Purpose limitation
C. Defense in depth
D. Zero trust

Q34. Which cryptographic dependency makes time stamping legally defensible?
A. Symmetric encryption
B. PKI trust chain
C. Encoding standards
D. Compression algorithms

Q35. Which misuse MOST threatens citizen trust in Aadhaar ecosystem?
A. Strong authentication
B. Excessive data collection
C. Use of PKI
D. Time stamping

Q36. Which scenario BEST demonstrates non-repudiation using time stamping?
A. Encrypted file storage
B. Digitally signed contract with TSA timestamp
C. Hashed password database
D. VPN login record

Q37. Which cryptographic lifecycle issue affects long-term validity of time stamps?
A. Key expiration of TSA
B. Network bandwidth

C. Hash size
D. File format

Q38. Which Aadhaar design choice MOST improves security against identity theft?
A. Centralized storage
B. Multi-factor authentication
C. Plain ID usage
D. Static identifiers

Q39. Which compliance requirement governs Aadhaar data protection?
A. PCI-DSS
B. GDPR
C. Aadhaar Act & IT Act
D. ISO 27001 only

Q40. Which statement BEST summarizes Aadhaar & time stamping in cyber security?
A. They replace PKI
B. They provide legal trust for digital transactions
C. They ensure confidentiality of all data
D. They prevent all cyber crimes