◇ EASY (Q1–Q10)

Q1. Encryption primarily provides which security service?
A. Integrity
B. Authentication
C. Confidentiality
D. Availability

Q2. The original readable form of data before encryption is called:
A. Ciphertext
B. Hash
C. Plaintext
D. Encoded text

Q3. Which of the following is NOT a cryptographic operation?
A. Encryption
B. Hashing
C. Encoding
D. Key generation

Q4. Which technique converts data into a fixed-length value?
A. Encryption
B. Encoding
C. Hashing
D. Compression

Q5. Which Windows feature allows encryption of individual files and folders?
A. BitLocker
B. NTFS ACL
C. Encrypting File System (EFS)
D. Windows Defender

Q6. Encryption that uses the same key for encryption and decryption is called:
A. Asymmetric encryption
B. Symmetric encryption
C. Hybrid encryption
D. One-time encryption

Q7. Which file system is REQUIRED for Windows EFS to function?
A. FAT32
B. exFAT
C. NTFS
D. ext4

Q8. Which command-line utility is used to encrypt files in Windows using EFS?
A. encrypt
B. lock
C. cipher
D. secure

Q9. Encoding is mainly used for:
A. Confidentiality
B. Data integrity
C. Data representation and compatibility
D. Authentication

Q10. Which cryptographic element controls access to encrypted data?
A. Algorithm
B. Key
C. Hash
D. Certificate

◇ MEDIUM (Q11–Q25)

Q11. Which statement BEST distinguishes encryption from hashing?
A. Encryption is irreversible; hashing is reversible
B. Encryption ensures integrity; hashing ensures confidentiality
C. Encryption is reversible with a key; hashing is irreversible
D. Both require secret keys

Q12. Which encryption type is MOST suitable for encrypting large files?
A. Asymmetric
B. Symmetric
C. Hash-based
D. Encoding-based

Q13. In Windows EFS, the File Encryption Key (FEK) is protected using:
A. User’s symmetric key
B. User’s public key
C. Administrator password
D. Hash function

Q14. Which cipher command option encrypts files and subdirectories recursively?
A. /e
B. /d
C. /s
D. /x

Q15. Which scenario BEST illustrates file-level encryption?
A. Encrypting entire hard disk
B. Encrypting a database table
C. Encrypting a confidential document file
D. Encrypting network traffic

Q16. What happens if an encrypted file is copied from NTFS to FAT32?
A. Encryption remains intact
B. File becomes corrupted
C. Encryption is removed
D. Access is denied

Q17. Which cipher command option is used to back up the encryption certificate?
A. /b
B. /k
C. /x
D. /w

Q18. Which cryptographic technique is commonly used to secure data “at rest”?
A. TLS
B. File encryption
C. VPN
D. Tokenization

Q19. Which factor MOST affects encryption performance on modern systems?
A. File name length
B. CPU and hardware acceleration
C. File permissions
D. User account type

Q20. Which encryption mechanism works transparently without user interaction after setup?
A. Application-level encryption
B. File system encryption
C. Manual file encryption
D. Encoding

Q21. Which of the following is a limitation of file-level encryption?
A. Protects against malware execution
B. Protects against insider misuse
C. Depends on user credentials
D. Prevents all data leakage

Q22. Cipher command can be used to securely wipe:
A. System memory
B. Registry keys

C. Free disk space
D. Network buffers

Q23. Which option in cipher command overwrites deleted data to prevent recovery?
A. /e
B. /x
C. /w
D. /s

Q24. Which security risk occurs if an EFS certificate is lost?
A. Files can be decrypted using admin rights
B. Files become permanently inaccessible
C. Files are auto-decrypted
D. Files are backed up automatically

Q25. Which encryption method protects only selected data rather than entire storage?
A. Disk encryption
B. Volume encryption
C. File encryption
D. Transport encryption

◇ HARD (Q26–Q40)

Q26. Which principle of information security is MOST directly enforced by encryption?
A. Availability
B. Confidentiality
C. Accountability
D. Authorization

Q27. A user encrypts files using EFS and then reinstalls Windows without backing up keys. What is the outcome?
A. Files can be decrypted by admin
B. Files are auto-recovered
C. Files are permanently lost
D. Files remain encrypted but accessible

Q28. Which encryption failure is MOST likely if weak randomness is used?
A. Collision attack
B. Key prediction attack
C. Replay attack
D. Side-channel attack

Q29. Which statement about encoding is TRUE from a security perspective?
A. Encoding hides data from attackers

B. Encoding prevents data tampering
C. Encoding provides no security guarantees
D. Encoding replaces encryption

Q30. In EFS, which component ensures only the intended user can decrypt the FEK?
A. Hash value
B. User's private key
C. Symmetric algorithm
D. File permissions

Q31. Which attack can still succeed even if file encryption is correctly implemented?
A. Offline brute-force attack
B. Insider misuse under valid user context
C. Disk theft
D. Cold boot attack

Q32. Why is symmetric encryption preferred over asymmetric for file encryption?
A. Better authentication
B. Smaller key size
C. Faster performance
D. Easier key exchange

Q33. Which command-line practice is MOST appropriate before encrypting sensitive folders?
A. Disable firewall
B. Backup encryption certificates
C. Change file permissions
D. Rename files

Q34. Which encryption deployment MOST improves usability while maintaining security?
A. Manual encryption of every file
B. Transparent file system encryption
C. Password-protected ZIP files
D. Encoding with Base64

Q35. Which scenario BEST demonstrates misuse of encryption?
A. Encrypting confidential files
B. Encrypting backups
C. Encrypting system files unnecessarily
D. Encrypting laptops

Q36. Which encryption approach provides protection even if the storage medium is stolen?
A. Encoding
B. File encryption
C. Access control lists
D. Logging

Q37. Cipher command execution requires which minimum privilege?
A. Guest access
B. File ownership or permission
C. Domain admin rights
D. System privileges

Q38. Which factor MOST influences the effectiveness of file encryption as a control?
A. Algorithm name
B. Key management practices
C. File size
D. Folder depth

Q39. Which encryption mistake MOST often leads to data loss rather than data breach?
A. Weak algorithm selection
B. Certificate/key backup failure
C. Poor performance tuning
D. File permission misconfiguration

Q40. Which encryption approach is BEST aligned with the principle of least privilege?
A. Encrypting entire disk for all users
B. Encrypting only sensitive files per user
C. Encrypting network traffic
D. Encoding shared files