## **Practice Q&A (Tutorial-Based)**

### **❓ Conceptual**

1. **Why is RSA insecure against quantum computers?** Shor’s algorithm allows efficient factoring of large integers, the core of RSA security.
2. **How does Grover’s algorithm affect symmetric encryption?** It reduces brute-force search time from O(n) to O(√n), requiring larger key sizes (e.g., AES-256 becomes AES-128 effective).
3. **Which PQC approach is best for digital signatures with small size?** **FALCON** and **Dilithium** are preferred for efficiency.
4. **Why is SPHINCS+ unique among signature schemes?** It’s based only on hash functions and does not rely on structure, giving high confidence in post-quantum security.
5. **What does the “shelf-life vs migration” diagram warn about?** Data encrypted today may be decrypted in the future if quantum computers emerge before migration finishes.

## **✅ 6. Active Recall Exercises**

### **🧠 MCQs**

1. **Which quantum algorithm breaks RSA?** a) Grover  
    b) Shor ✅  
    c) AES  
    d) BB84
2. **Which post-quantum algorithm is hash-based?** a) Dilithium  
    b) Kyber  
    c) SPHINCS+ ✅  
    d) McEliece
3. **Which key exchange method is part of ML-KEM?** a) FALCON  
    b) Kyber ✅  
    c) RSA  
    d) SIDH

### **✍ Fill-in-the-Blanks**

1. Shor’s algorithm can break RSA by \_\_\_\_\_\_\_ large integers.  
    → **factoring**
2. Grover’s algorithm weakens symmetric-key crypto by reducing search time to \_\_\_\_\_.  
    → **√n**
3. NIST selected CRYSTALS-Kyber as the basis for the \_\_\_\_\_\_\_ standard.  
    → **ML-KEM**

### **📝 Short Answer**

1. **Why are lattice problems promising for PQC?** They are believed to be hard even for quantum computers and offer efficient implementation.
2. **How does SPHINCS+ avoid structural attacks?** It uses only hash functions, making it stateless and resistant to structure-specific attacks.
3. **What makes quantum-safe migration urgent?** Data intercepted today could be decrypted later when quantum computers are available ("Harvest now, decrypt later").