## **✅ Practice Q&A (based on Tutorial 4)**

**Q1: What are the main services provided by TLS?** **A:** Confidentiality, integrity, and authentication.

**Q2: How is forward secrecy achieved in TLS?** **A:** By using ephemeral key exchanges (DHE/ECDHE), new keys are generated per session.

**Q3: What is the role of the Certificate Authority (CA)?** **A:** It verifies identities and signs certificates to establish trust.

**Q4: Why is the ChangeCipherSpec message important?** **A:** It marks the transition to encrypted communication using the negotiated keys.

## **✅ MCQs, Fill-in-the-Blanks & Short Answer**

### **🧠 MCQs**

**1. Which of the following cipher suites provides forward secrecy?** a. RSA  
 b. ECDHE  
 c. DHE  
 d. Both b and c  
 ✅ **Answer:** d

**2. Which layer does the TLS record protocol operate at?** a. Application  
 b. Transport  
 c. Network  
 d. Presentation  
 ✅ **Answer:** b

### **📝 Fill-in-the-Blanks**

**1. TLS uses the \_\_\_\_\_\_\_ protocol to ensure message integrity.** ✅ HMAC

**2. In TLS handshake, the server proves its identity using a \_\_\_\_\_\_\_.** ✅ Digital Certificate (X.509)

**3. The shared session key is derived from the \_\_\_\_\_\_\_ and random values.** ✅ Pre-Master Secret

### **💡 Short Answer**

**Q: Why are digital certificates essential in TLS?** **A:** They enable clients to verify the server’s identity via a trusted CA, preventing impersonation.

**Q: How does TLS ensure integrity of transmitted data?** **A:** Through MACs (e.g., HMAC-SHA256), applied to the plaintext before encryption.