## **📄 Practice Q&A (from lecture logic, no tutorial this week)**

### **🧠 Fill-in-the-Blanks**

1. The purpose of network security is to ensure **\_\_\_\_\_\_\_\_**, **\_\_\_\_\_\_\_\_**, **\_\_\_\_\_\_\_\_**, and **\_\_\_\_\_\_\_\_**.
2. A **\_\_\_\_\_\_\_\_ attack** is when an attacker modifies a legitimate message.
3. **Symmetric encryption** uses the \_\_\_\_\_\_\_\_\_ key for both encryption and decryption.

### **❓ Short Answer Questions**

1. Explain the difference between active and passive attacks with examples.
2. What roles does a Trusted Third Party play in secure communications?
3. Why is hashing important in ensuring message integrity?

## **🧠 Evaluation, Comparison, and Recommendation Questions**

These questions test your **analytical ability** using your foundational understanding of network security principles.

### **🔍 1. Evaluation Questions**

1. **Identify and evaluate** the risks involved in using an unencrypted protocol like **Telnet** over the internet.
2. What are the limitations of using **only symmetric encryption** in securing communications between two parties who have never met before?
3. Why is relying solely on **firewalls** insufficient for securing distributed applications?

### **⚖️ 2. Comparison Questions**

1. Compare **SSL/TLS** and **IPSec** in terms of:  
   * Layer of the OSI model where they operate
   * Use cases
   * Strengths and weaknesses
2. Differentiate between:  
   * Passive vs Active Attacks
   * Hashing vs Encryption
   * Kerberos vs Public Key Infrastructure (PKI)
3. What are the differences between **MAC-based** and **Digital Signature-based** message integrity mechanisms?

### **🧭 3. Recommendation Questions**

1. You’re tasked with securing a file-sharing system in an enterprise network. Which protocols and tools would you recommend, and why? (e.g., SFTP vs FTP, IPSec, Kerberos)
2. Recommend a security solution for mobile devices accessing sensitive data over public Wi-Fi.
3. How would you design a secure login system that prevents eavesdropping, replay, and impersonation?

## **🔧 Bonus Section: Making an Unsecure Protocol Secure**

### **🎯 Key Idea:**

Secure an insecure protocol (e.g., HTTP, FTP, Telnet) by **wrapping it in secure mechanisms**.

### **❓ Questions:**

1. **Case Study**: HTTP is inherently insecure. How does **HTTPS** (HTTP + TLS) address its vulnerabilities? What roles do:  
   * Server certificates
   * Key exchange
   * Encryption  
      play?
2. Telnet sends passwords in plaintext. Describe **two secure alternatives** and how they provide protection against sniffing and replay attacks.
3. Suppose you're given a proprietary protocol that lacks authentication. Describe how you would:  
   * Integrate a **challenge-response authentication**
   * Ensure **confidentiality and integrity**
   * Defend against **MITM attacks**
4. You're required to add confidentiality to DNS lookups. What protocol(s) or techniques would you recommend (e.g., DNSSEC, DoH, DoT), and why?