## **✅ Practice Q&A (From Tutorial 3)**

### **Short Answers**

1. **How many email addresses in SMTP?** Two: sender and receiver.
2. **Does SMTP require password?** No. No authentication by default.
3. **Who can read a basic email in transit?** Both sender’s and receiver’s mail servers.
4. **How to send an anonymous email using symmetric key (K)?** Encrypt hash of message and sender’s ID using K. Leave sender field blank.
5. **Why sign-then-encrypt?** Provides authentication, non-repudiation, and confidentiality. Signature is protected.

## **✅ Active Recall: MCQs, Fill-in-the-Blanks, SAQs**

### **🔲 Fill-in-the-Blanks**

1. PGP converts binary email to ASCII using \_\_\_\_\_\_\_\_\_\_\_\_.  
    → **Radix-64 (Base64)**
2. In Kerberos, the \_\_\_\_\_\_\_\_\_\_\_\_ issues short-lived tickets for specific services.  
    → **Ticket Granting Server (TGS)**
3. S/MIME uses \_\_\_\_\_\_\_\_\_\_\_\_ certificates for key management.  
    → **X.509 v3**
4. SSH uses \_\_\_\_\_\_\_\_\_\_\_\_ key exchange for establishing a shared secret.  
    → **Diffie-Hellman**

### **🔘 Multiple Choice Questions**

1. Which protocol does PGP use to compress messages?  
    a) GZIP  
    b) RAR  
    ✅ **c) ZIP** d) BZIP2
2. What’s the encryption order in PGP?  
    a) Compress → Encrypt → Sign  
    ✅ **b) Sign → Compress → Encrypt** c) Encrypt → Sign → Compress  
    d) Sign → Encrypt → Compress
3. Which of the following uses a Web of Trust model?  
    a) X.509  
    ✅ **b) PGP** c) Kerberos  
    d) TLS

### **💬 Short Answer Questions**

1. Describe two weaknesses of SMTP.
2. What is the purpose of a Key Ring in PGP?
3. How does SSH ensure data confidentiality?
4. Why is Sign-Then-Encrypt preferred over Encrypt-Then-Sign?
5. How does Kerberos avoid replay attacks?