## **❓ Practice Q&A**

### **Multiple Choice Questions**

1. **Which component of PKI is responsible for verifying user identities before certificate issuance?**
   * A) Certificate Authority (CA)
   * B) Registration Authority (RA)
   * C) Digital Certificate
   * D) Public Key
2. **Answer**: B) Registration Authority (RA)
3. **What is the primary purpose of a Certificate Revocation List (CRL)?**
   * A) To list all valid certificates.
   * B) To provide encryption keys to users.
   * C) To list certificates that are no longer trustworthy.
   * D) To issue new certificates.
4. **Answer**: C) To list certificates that are no longer trustworthy.

### **Fill-in-the-Blanks**

1. **A digital certificate binds a public key to an entity's \_\_\_\_\_\_\_\_\_\_.** **Answer**: identity
2. **In the X.509 certificate structure, the field that specifies the certificate's expiration date is called \_\_\_\_\_\_\_\_\_\_.** **Answer**: Not After

### **Short Answer Questions**

1. **Explain the role of a Certificate Authority (CA) in PKI.** **Answer**: A CA is a trusted entity that issues digital certificates after verifying the identity of the requester. It signs the certificate with its private key, allowing others to trust the binding between the public key and the entity's identity.
2. **What is cross-certification, and why is it important in PKI?** **Answer**: Cross-certification is the process where one CA signs the certificate of another CA, establishing trust between different PKI domains. It enables users in one domain to trust certificates issued by another CA, facilitating broader interoperability.