1. Explain the differences between symmetric and asymmetric cryptography.
2. What does Initialization Vector mean? where is it normally used?
3. What is pseudorandom number? How can it be used to encrypt data?
4. How can one user send a confidential message to another user with the help of asymmetric cryptography?
5. Why is it difficult for an attacker to calculate the private key in RSA if they only have the public key?
6. What are the problems with asymmetric key distribution compared to symmetric key distribution?
7. Why may certificate revocation be required? How is it accomplished?
8. What is a Message Authenticity Code (MAC)?
9. How is the integrity of a message verified using a MAC?
10. What is meant by message integrity and why is it necessary?