Chapter 04 Homework Assignment: Advanced Cryptography

Instructions: Answer each question. Be clear and concise, using your own words.

1. What is the purpose of a digital certificate, and how does it help verify identity?

2. Explain the role of certificate authorities (CAs) and registration authorities (RAs) in issuing a digital certificate.

3. Under what circumstances might a digital certificate be revoked?

4. What is the function of the Online Certificate Status Protocol (OCSP), and how is OCSP stapling different?

5. What is certificate chaining and why is it important in validating digital certificates?

6. Describe the difference between domain validation and extended validation digital certificates.

7. What are some specific uses of hardware and software digital certificates?

8. What is the X.509 standard, and what key information does an X.509 digital certificate contain?

9. Define Public Key Infrastructure (PKI). Why is it important in cybersecurity?

10. Compare the hierarchical, distributed, and bridge trust models.

11. What are the four main phases in the lifecycle of a digital certificate?

12. Why might private keys be stored in hardware devices rather than software?

13. What is the difference between escrow and recovery in key management?

14. Explain the main function of Transport Layer Security (TLS). What is a cipher suite?

15. What are the two encryption modes supported by IPSec and how do they differ?

16. Identify one use case for each of the following secure protocols:
- HTTPS
- SSH
- S/MIME
- SRTP

17. What factors contribute to the strength of a cryptographic key?

18. Why is relying on secret algorithms not a recommended practice in cryptography?

19. List and briefly explain two common block cipher modes of operation.