Long Questions

1. Explain the process of symmetric key distribution using symmetric encryption and its security implications.
2. Describe how asymmetric encryption is utilized in the distribution of symmetric keys.
3. What are the challenges associated with the distribution of public keys and how are they addressed?
4. Discuss the role and functionality of Kerberos in managing secure, distributed authentication.
5. Explain the X.509 Authentication Service and its application in secure communications.
6. Define Public-Key Infrastructure (PKI) and outline its components and how it secures communications.
7. How does symmetric key distribution differ from asymmetric key distribution in terms of security and efficiency?
8. Describe the processes involved in setting up a PKI system and the roles of its various components.
9. What mechanisms are in place to ensure the integrity and authenticity of public keys in a PKI?
10. Discuss the use of certificates in the X.509 framework and how they enhance security.
11. How does Kerberos prevent replay attacks and ensure the integrity of communications within a network?
12. Explain the significance of certificate authorities (CAs) in PKI and their responsibilities.
13. Describe the process of certificate revocation in PKI and its impact on network security.
14. How are trust relationships managed in a PKI environment?

15. Discuss the security challenges and solutions in symmetric key distribution using asymmetric encryption.
16. What are the key considerations for web security?
17. Explain the functions and security features of Secure Socket Layer (SSL).
18. Describe the differences between SSL and Transport Layer Security (TLS).
19. How does HTTPS enhance web security compared to HTTP?
20. What is Secure Shell (SSH) and how does it secure network communications?
21. Discuss the process of establishing an SSL/TLS session.
22. Explain the role of certificates in SSL/TLS.
23. How does TLS improve upon the security features of SSL?
24. What vulnerabilities are associated with SSL and how can they be mitigated?
25. Describe the cryptographic methods used in SSL/TLS for ensuring data integrity and confidentiality.
26. What are the primary security concerns in wireless networks?
27. Explain the security mechanisms in place in IEEE 802.11 Wireless LANs.
28. Describe the enhancements made in IEEE 802.11i for wireless LAN security.
29. Discuss the challenges of mobile device security.
30. How do security protocols in wireless networks differ from those in wired networks?
31. What strategies are used to secure mobile devices accessing corporate networks?
32. How does IEEE 802.11i address the vulnerabilities in earlier 802.11 protocols?
33. Explain the importance of encryption in wireless communications.

34. What are the common attack vectors for wireless networks and how are they mitigated?
35. Discuss the security implications of using public Wi-Fi networks.
36. Explain the functionality and security features of Pretty Good Privacy (PGP).
37. Describe how S/MIME enhances email security.
38. What are the differences between PGP and S/MIME?
39. How does PGP use the concept of a 'web of trust'?
40. Discuss the importance of digital signatures in email security.
41. Explain the process of encrypting and decrypting emails using S/MIME.
42. What vulnerabilities exist in email communication and how do PGP and S/MIME address them?
43. How does key management work in PGP?
44. Discuss the challenges of implementing widespread email encryption.
45. What role does certificate management play in S/MIME?
46. Provide an overview of IP Security and its components.
47. Describe the IP Security architecture.
48. What is the Authentication Header in IP Security and what does it do?
49. Explain the purpose and function of the Encapsulating Security Payload in IP Security.
50. Discuss the process of combining security associations in IP Security.
51. What is Internet Key Exchange and how does it function within IP Security?
52. How does IP Security provide confidentiality, integrity, and authentication?
53. Compare and contrast the roles of the Authentication Header and Encapsulating Security Payload.
54. Explain how IP Security can be used in virtual private networks (VPNs).
55. What are the limitations of IP Security in network communications?

56. Explain the concept of Secure Multiparty Computation and its applications.
57. Discuss the cryptographic challenges and solutions in virtual elections.
58. What is Single Sign-On and how does it enhance security and user experience?
59. Describe the security mechanisms involved in Secure Inter-branch Payment Transactions.
60. Explain the vulnerabilities associated with Cross-Site Scripting and its impact on web security.
61. How can cryptographic techniques secure multiparty calculations in a distributed environment?
62. Discuss the use of cryptography in ensuring the integrity of electronic voting systems.
63. Explain how Single Sign-On can be vulnerable to security breaches and the measures to protect it.
64. What are the typical security considerations in designing secure payment systems for financial institutions?
65. Discuss the measures to mitigate Cross-Site Scripting attacks in web applications.
66. How does the use of Transport Layer Security (TLS) protocols in HTTP/2 enhance the security of web communications over its predecessor, HTTP/1.1?
67. Discuss the role of elliptic curve cryptography in enhancing the security of transport-level protocols like TLS and SSH.
68. What are the specific security benefits of using SSH tunnels for remote communications compared to traditional VPN solutions?
69. How does the dynamic nature of mobile device security complicate the implementation of traditional security measures used in fixed networks?

70. Evaluate the effectiveness of current wireless security protocols in protecting against advanced persistent threats (APTs).
71. Explain the concept of quantum key distribution and its potential impact on the security of public key infrastructures.
72. How do modern implementations of IP Security support the notion of zero-trust architectures in network security?
73. Discuss the practical security considerations when implementing digital signature algorithms in large-scale voting systems.
74. What are the challenges of integrating blockchain technology with traditional cryptographic techniques for secure multiparty computation?
75. Examine the security implications of AI-driven predictive typing features in encrypted messaging applications.