Review Exercises

Chapter 5

1. Explain the meaning of “Authentication”, “Authorization”, “Integrity”, “Confidentiality”, “Availability”, and “Non-repudiation” in network security.
2. List the possible network security attacks.
3. What is “Transposition Ciphering”? What is “Substitution Ciphering”?
4. Briefly explain how public-key encryption algorithm works.
5. Briefly explain how Message Digest 5 (MD5) works.
6. What is “Digital Signature”? What is Public-Key Infrastructure (PKI)?
7. What are the major purposes of Security Association (SA) in IPsec?
8. For IPsec in IPv4/IPv6, draw the original packet format and the format after applying AH in both transport mode and tunnel mode.
9. For IPsec in IPv4/IPv6, draw the original packet format and the format after applying ESP in both transport mode and tunnel mode.
10. Describe the functions of the relay agent, proxy agent, redirect agent, and translation agent in Diameter.
11. Draw the figure of Globe Challenge in IS-41 by using the CAVE algorithm.
12. Draw the figure of GSM security by using A3, A5, and A8 algorithms.
13. What is *“Visibility and Configurability”* in 3GPP security?
14. Draw a high-level figure to show 3GPP AKA.
15. How *mutual authentication* is achieved in 3GPP?
16. How *Network Domain Security* is achieved in 3GPP?
17. Compare the security mechanisms in GSM and 3GPP.
18. How *Authentication and Key Agreement (AKA)* is executed in 3GPP2?