Questions (from Computer Networking a Top-Down Approach 6th Edition – Chapter 8):

R1. What are the differences between message confidentiality and message integrity? Can you have confidentiality without integrity? Can you have integrity without confidentiality? Justify your answer. (3 points)
Solution:
"*Message Confidentiality"* is a process where two or more hosts communicate securely using encryption and the attacker cannot determine the original message (plain text) when he attacks a cipher text.
"Message integrity" is a process where the receiver can detect if the message sent was altered in transit.
However, both the entities are independent of each other (message integrity and message confidentiality) as they are two different concepts. Sending a message confidentially does not does not guarantee data integrity. Let us consider that the cipher text is altered during the transmission of data and there is no message integrity because of the security issues. Even in such case message confidentiality is maintained since the hacker cannot determine the original plain text.

R7. Suppose n = 10,000, a = 10,023, and b = 10,004. Use an identity of modular arithmetic to calculate in your head (a • b) mod n. (2 points)
Solution:
Given that n = 10,000, a=10,023 and b = 10,004; a mod n = 23; b mod n = 04;
(a • b) mod n = 92;
Hint: [(a mod n) • (b mod n)] mod n = (a • b) mod n;

R9. In what way does a hash provide a better message integrity check than a checksum (such as the Internet checksum)? (2 points)
Solution:
An internet checksum (TCP checksum or IP checksum) are generally designed to detect the errors quickly and efficiently. Internet checksum does not prevent collision. Whereas hash provides better message integrity because it has less collision compared to internet checksum. When there's collision, there are more ways to produce the same sum. Like this by preventing the number of collisions hash provides a better message integrity compared to checksum.

R15. Suppose Alice has a message that she is ready to send to anyone who asks. Thousands of people want to obtain Alice's message, but each wants to be sure of the integrity of the message. In this context, do you think a MAC-based or a digital-signature-based integrity scheme is more suitable? Why? (2 points)
Solution:
In a MAC-based scheme, a private key is generated between the sender and the receiver. This will provide an authentication to both sender and receiver. In the above scenario Alice is ready to send message to thousands of people which makes the MAC method not suitable since shared key has to be generated every time to every recipient. In digital-signature-based integrity

scheme, Alice can use the same digital signature for each recipient thereby reducing the complexity of generating various private keys. Hence, digital-signature-based integrity is suitable in the given scenario.

R20. In the SSL record, there is a field for SSL sequence numbers. True or False? (2 points)
Solution:
False. In SSL (Secure socket layer), both sides maintain sequence number independently. SSL uses implicit sequence numbers.

R27. WEP for 802.11 uses a stream cipher for encryption. Suppose that the data is 10101100 and the keystream is 1111000. What is the resulting cipher text? (2 points)
Solution:
The resulting cipher text is: 01011100

P8. Consider RSA with p = 5 and q = 11.
a. What are n and z? (2 points)
Solution:
Step 1: n = p*q;
Step 2: Given: p=5, q= 11; Hence, p*q = 5*11 = 55;
i.e. **n = 55**
Step 3: z = (p-1) (q-1);
Step 4: (p-1) = (5-1) = 4; (q-1) = (11-1); Hence, z = 4 * 10 = 40;
i.e. **z = 40**

b. Let 'e' be 3. Why is this an acceptable choice for 'e'? (1 point)
Solution:
Value 3 for 'e' is acceptable because it has no common factor with 'z' and it is less than 'n'.

c. Find 'd' such that de = 1 (mod z) and d < 160. (1 point)
Solution:
The value of 'd' must be (de-1) divisible by z;
i.e. (de-1)/z = (3*d-1)/40; i.e. **'d' = 27.**

d. Encrypt the message m = 8 using the key (n, e). Let c denote the corresponding cipher text. Show all work. (3 points)
Solution:
Step 1: Given m = 8 and e = 3;
Step 2: m^e = 8^3 = 512;
Step 3: From calculation, n = p*q = 55;
c = m^e mod n; i.e. c = 512 mod 55 =17
Hence, the corresponding cipher text **'c' is 17.**
Hint: To simplify the calculations, use the fact:
[(a mod n) • (b mod n)] mod n = (a • b) mod n