44100113: COMPUTER NETWORKS
HOMEWORK 5: CHAPTER 8 Security in Computer Networks
SOLUTIONS

Notes: All exercises are in accordance with the 6^{th} edition (International Edition). We change data values in some problems, which are highlighted.

Exercise 1 (R1)

Confidentiality is the property that the original plaintext message can not be determined by an attacker who intercepts the ciphertext-encryption of the original plaintext message. Message integrity is the property that the receiver can detect whether the message sent (whether encrypted or not) was altered in transit. The two are thus different concepts, and one can have one without the other. An encrypted message that is altered in transmit may still be confidential (the attacker can not determine the original plaintext) but will not have message integrity if the error is undetected. Similarly, a message that is altered in transit (and detected) could have been sent in plaintext and thus would not be confidential..

Exercise 2 (R3)

One important difference between symmetric and public key systems is that in symmetric key systems both the sender and receiver must know the same (secret) key. In public key systems, the encryption and decryption keys are distinct. The encryption key is known by the entire world (including the sender), but the decryption key is known only by the receiver

Exercise 3 (R9)

One requirement of a message digest is that given a message M, it is very difficult to find another message M' that has the same message digest and, as a corollary, that given a message digest value it is difficult to find a message M'' that has that given message digest value. We have "message integrity" in the sense that we have reasonable confidence that given a message M and its signed message digest that the message was not altered since the message digest was computed and signed. This is not true of the Internet checksum, where we saw in Figure 8.8 that it easy to find two messages with the same Internet checksum.

Exercise 4 (P8)

p = 5, q = 11

a) n = p*q = 55, z = (p-1)(q-1) = 40

b) e = 3 is less than n and has no common factors with z.

c) d = 27

d) m = 8, me = 512, Ciphertext c= me mod n = 17