44100113: COMPUTER NETWORKS
HOMEWORK 5: CHAPTER 8

Notes:
1. All exercises are in accordance with the 6th edition (International Edition). We change data values in some problems, which are highlighted.
2. These limited exercises are not enough to cover all the knowledge required in our course. You should read the textbook by yourselves.

Chapter 8: Security in Computer Networks

Exercise 1 (R1, CHAPTER 8)
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.

Exercise 2 (R3, CHAPTER 8)
From a service perspective, what is an important difference between a symmetric-key system and a public-key system?

Exercise 3 (R9, CHAPTER 8)
In what way does a hash provide a better message integrity check than a checksum (such as the Internet checksum)?

Exercise 4 (P8, CHAPTER 8)
Consider RSA with $p = 5$ and $q = 11$.
a. What are n and z?
b. Let e be 3. Why is this an acceptable choice for e?
c. Find d such that $de = 1 \pmod{z}$ and $d < 160$.
d. Encrypt the message $m = 8$ using the key (n, e). Let c denote the corresponding ciphertext. Show all work. *Hint: To simplify the calculations, use the fact:*

$$[(a \bmod n) \bullet (b \bmod n)] \bmod n = (a \bullet b) \bmod n$$