**IoT Security and Privacy**

**Assignment 1 - Introduction to Security and Privacy (20 points)**

### Instructions:

1. Note: Blue text points to a web link. Ctrl + Click to follow link.
2. This is an individual assignment.
3. Answers to all questions must be put into **ONE** document. That is, every time, each student can only submit one report document, answering all questions of this assignment.
4. Students must put answers following each question in this assignment. The instructor will not grade a report with only answers in it and the student gets zero for such an assignment. An assignment report must include original questions.
5. Students MUST submit the finished assignment in either Microsoft Word or pdf format to Blackboard. The doc must be submitted as ONE standalone file and cannot be tarred or zipped into a container.
6. Refer to [Print screen](http://en.wikipedia.org/wiki/Print_screen) on how to take a screenshot. Pressing the Alt key in combination with PrtSc will capture the currently selected window.

**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)

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)

R9. In what way does a hash provide a better message integrity check than a checksum (such as the Internet checksum)? (2 points)

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)

R20. In the SSL record, there is a field for SSL sequence numbers. True or False? (2 points)

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 ciphertext? (2 points)

P8. Consider RSA with p = 5 and q = 11.

a. What are n and z ? (2 points)

b. Let e be 3. Why is this an acceptable choice for e ? (1 point)

c. Find d such that de = 1 (mod z ) and d < 160. (1 point)

d. Encrypt the message m = 8 using the key (n , e ). Let c denote the corresponding ciphertext. Show all work. (3 points)   
  
Hint: To simplify the calculations, use the fact:

[(a mod n ) • (b mod n )] mod n = (a • b ) mod n