RFID INFOSEC Homework #4, ver. 1.0  
Tag Layer  
Assigned Oct. 21 and Due Oct. 28, 2009

Name: ________________________________  
ID: ________________________________

35 pts.

Show all your work. Without proper justification and details of steps, correct answers alone may not carry full credit.

Notes:
- Minus 3 points if your homework is not stapled in the upper left-hand corner.
- Minus 2 points if you use the back of your paper. Please only use a single side.
- Minus 2 points if you present the worked problems out of order. In other words, please present the problems in the order assigned, 1, 2, 3, ...

1. Describe the difference between Class-1 and Class-2 tags. Circle the difference that affects security the most. (5 pts.)

2. What group of circuits extracts energy from the antenna to power the tag? (2 pts.)

3. What group of circuits converts the ASK signal from the antenna to digital signals used by the digital logic? (2 pts.)

4. If a reader wants to access the 32-bit Access Password stored in the tag memory, what parameter(s) does it need to provide to the tag? (5 pts.)

5. Describe the three basic operations between readers and tags. (3 pts.)

6. Describe one of the purposes of sessions in Gen2. (3 pts.)

7. What is the first piece of information that a tag backscatters to a reader during a round? (2 pts.)

8. What is the system purpose of the tag slot counter? (3 pts.)

9. List the three general mitigation techniques for preventing counterfeiting of tags. (3 pts.)

10. Describe the encryption described by Gen2. (3 pts.)

11. List the four different types of side-channel attacks. (4 pts.)