Name: ________________________________

ID: ________________________________

37 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 differences between Class-1 and Class-2 tags as described in the Gen2 specification. Circle the difference that affects security the most. (5 pts.)

2. What group of circuits on a tag receives the signal from the antenna and extracts the information from the modulated signal to provide to the digital logic? (2 pts.)

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

4. Are there an odd or even number of inverters in the ring oscillator on a tag? Why? (3 pts.)

5. 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? Locate and review the Gen2 specification to answer this question. (5 pts.)

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

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

8. In Gen2, the tag picks a random number from what range of numbers when preloading the slot counter after the tag receives the Query command with Q=4 from the reader? (3 pts.)

9. A Gen2 tag begins with the session S2 flag set to A. After 7 seconds of the tag being powered on by the reader carrier, the reader has not refreshed the S2 flag. What is the flag for S2? (2 pts.)

10. Describe a physical unclonable function (PUF). (3 pts.)

11. List one mitigation technique for the replay attack. (2 pts.)

12. Describe a technique used in Gen2 tags to protect the integrity of the data on a tag. (2 pts.)

13. Describe the power analysis side-channel attack. (2 pts.)