RFID INFOSEC Homework #2, ver. 1.0
Assigned Sep. 24 and Due Oct. 1, 2008

Name: ________________________________
ID: ________________________________

48 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. For each threat below, what principle of security is violated? (1 pt. each)
   a. Tag cloning
   b. Skimming
   c. Coupling

2. Server A has a mean time between failures of 720 hours. When it does fail, assume it takes an administrator 7 hours on average to fix it. Server B has a mean time between failures of 7 hours. However, this system can automatically detect the failure and reboot the system in 25 seconds fixing the problem. Answer the following questions.
   a. What is the availability of server A? (2 pts.)
   b. What is the availability of server B? (2 pts.)
   c. Which server, A or B, is more available? (1 pt.)

3. Describe the relay attack. Draw a diagram. What security principle is violated? (5 pts.)

4. Group the 14 threats discussed in class into a smaller number of categories and label the categories with a descriptive keyword. (10 pts.)

5. My public key was generated with gpg on turing.uark.edu and is available at the following website. Using gpg on turing.uark.edu, import my public key, encrypt a secret message to me, ASCII armor it, and email the ciphertext to me at drt@uark.edu. (5 pts.)

http://comp.uark.edu/~drt/keys/key_drt.asc

6. Look up the construction of HMAC.
   a. What RFC describes HMAC? (2 pts.)
   b. Provide the formula for HMAC. (3 pts.)
7. List 2 symmetric-key encryption algorithms. (2 pts.)

8. List 2 asymmetric-key encryption algorithms. (2 pts.)

9. Describe the difference between symmetric- and asymmetric-key cryptography. (3 pts.)

10. Refer to the authentication protocol figure below.
    a. Describe the major flaw of the authentication protocol shown below. (3 pts.)
    b. Describe how to fix this flaw. (5 pts.)