EECE 412, Fall 2007

Quiz #1

Your Family name: ____________________________
Your Given name: ____________________________
Your student ID: ____________________________

Name of your nearest left neighbor: ____________________________
Name of your nearest right neighbor: ____________________________

Questions:

1. (4 points) CIA properties are not equally important for all systems.

Provide an example of a system, in which confidentiality is more important than integrity or availability. Explain why.

Provide an example of a system, in which integrity is more important than the other two properties. Explain why.

2. (2 points) Define when a crypto system is secure.

3. (2 points) Give an example of two crypto systems A & B such that A is secure, according to the definition of a secure cryptosystem, and B is not, yet an attack on A is less computationally expensive than the best attack on B.

4. (5 points) True or False?

[ ] Keystream is used for encrypting plain text stream using one-time pad.
[ ] AES uses both transposition and diffusion.
[ ] AES uses only permutation and transposition.
[ ] The key to attacking double transposition cipher is to use frequency analysis.
[ ] Most protection mechanisms are broad.

5. (2 points) What does the Kerckhoff's Principle state?

6. (3 points) Give an example of a system, computer-based or not, in which even though threats and vulnerabilities are significant, the overall risk is very low. Explain how it could be.

7. (4 points) Imagine that you have a fancy car. Consider the risk of your car being stolen while it's parked on campus during this quiz. For each of the four ways of managing this risk, give one example of what you could have done. Be specific.

1.

2.

3.

4.

8. (3 points) Explain the difference between authentication and authorization.

9. (3 points) What are the required properties of good <u>hash function</u>? Select all applicable.

A. collision resistance
B. efficient
C. invertible
D. the key should not be reused
E. "one-wayness"

Answers: ____________________