EECE 412, Fall 2008

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. (3 points) Explain how it can be that for two crypto systems A & B, 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.

2. (2 points) The basic assumption in cryptography (a.k.a. Kerckhoff's Principle) states which of the following? (select one most appropriate)

[ ] Security should be achieved through obscurity.

[ ] The key(s) should be assumed publicly known but the system design can be assumed secret.

[ ] Both system design and the keys can be assumed secret.

[ ] The system design should be assumed publicly known but the key(s) can be assumed secret.

[ ] Neither system design or the keys can be assumed secret.

3. (2 points) Give an example of a system, computer-based or not, in which even though value of the assets and vulnerabilities are significant, the overall risk is very low. Explain how it could be.

4. (2) What are the two types of operations that are used in ciphers? For each type, give at least one example of a classic cipher that operates using that type.

1. Operation type: _____ cipher example: _____

2. Operation type: _____ cipher example: _____

5. (2) Give an example of a historic (i.e., not modern) cipher, which is

1. Block cipher: _____

2. Stream cipher: _____

5. (4 points) Consider the risk of your belongings being stolen from your house or apartment 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.

6. (2 points) Explain the difference between access control and data protection. Illustrate your answer with an example.

7. (3 points) Explain what the Elf needs to do with the dice and the script in order to implement a random (a.k.a. hash) function.