EECE 412, Fall 2005

Quiz #1

Your Family name: _____
Your Given name: _____
Your student ID: _____

Name of your left neighbor: _____
Name of your right neighbor: _____

Questions:

1. (3 points) Define the terms confidentiality, integrity, and availability.

2. (3 points) Define the terms secure protection mechanism, precise protection mechanism, and broad protection mechanism.

3. (5 points) **T**rue or **F**alse?

[ ] An important property of random permutation is few collisions.
[ ] Cæsar is a transposition cipher and its key weakness is that the key is too short.
[ ] The key to attacking Vigenere cipher is to find out the period of the key.
[ ] Public key algorithms are based on mathematical functions rather than on substitution and permutation.
[ ] The most appropriate for protecting message integrity and authenticity is DES.

4. (1 point) What class of threats does “repudiation of origin” belongs to? Select one.

A. Disclosure
B. Deception
C. Disruption
D. Usurpation
E. Snooping

Answer: _____

5. (5 point) You are asked to select a hash function for implementing the following authentication scheme:

1. The server and the client share a 16-byte key K.
2. The server sends a randomly generated 16-byte challenge N to the client.
3. The client sends back H = hash(N|K)
4. Since the server knows N and K, it computes hash(N|K) and compares it with H received from the client.

Prioritize the properties of hash functions in the order of their importance for the above authentication scheme, from “essential” to “least important”. Explain why you ordered the properties in your way.

6. (2 points) For encrypting multimedia stream sent from a mobile device to an Internet server, which mode of operation would be most appropriate? Select one.

A. Electronic Code Book (ECB)
B. Cipher Block Chaining (CBC)
C. Output Feedback (OFB)
D. Counter Encryption

Answer: _____

7. (3 points) For each of the following statements, give an example of a situation in which the statement is true.

a. Prevention is more important than detection and recovery.
b. Detection is more important than prevention and recovery.
c. Recovery is more important than prevention and detection.

8. (3 points) If one-time pads are provably secure, why are they so rarely used in practice?

9. (4 points) What are the main requirements of a public key cryptosystem?

10. (3 points) Is Electronic Code Book (ECB) suitable for message authentication code (MAC)? Clearly explain in no more than 5 sentences why or why not.

11. (1 point) What is the correct spelling of this course instructor's name?

12. (1 point) What is the correct spelling of this course teaching assistant's name?