EECE 412, Spring 2007

Quiz #1

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

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

total = 28 points

Questions:

1. (2 points) Shoulder surfing attacks compromise which of the following properties of the information input into bank machines or public Internet kiosks? Mark any applicable.

- ☑ confidentiality
- ☐ integrity
- ☐ availability

2. (4 points) True or False?

T [ ] An important property of random permutation is being invertible.
T [ ] Cæsar is a substitution cipher and the easiest attack on it is exhaustive search in the key space.
F [ ] The key to attacking Vigenere cipher is to start with frequency analysis.
T [ ] The key to attacking monoalphabetic cipher invented by Arabs and discussed in the class is to start with frequency analysis.

3. (4 points) What are the goals of computer security? Select all applicable.

A. Prevention
B. Investigation
C. Assurance
D. Detection
E. Deterrence
F. Protection
G. Insurance
H. Safety
I. Authorization
J. Recovery

Answers: _____

4 points

4. (~~1 point~~) For each of the following threat classes, provide an example of a threat that belongs to that class. Do not use the same threat more than in one example.

A. Disclosure

B. Deception

C. Disruption

D. Usurpation

5. (2 points) What computer security policies are concerned with? Select one.

A. Confidentiality
B. Safety
C. Availability
D. Integrity
E. Deterrence
F. Recovery
G. All of the above
H. A, C, D
I. A, C, D, F
J. A, C, D, E

Answer: _____

6. (3 points) Which of the following functionalities would you use to prevent a compromise of the integrity and confidentiality of your assignment #2 for 412 on your personal computer before it is submitted? Select all applicable.

A. Design and implementation assurance of your computer hardware
B. Access control on the assignment files
D. Non-repudiation of the assignment files
C. Data protection of the assignment files
E. Service continuity of the assignment files

Answers: _____

7. (3 points) Give 1-2 examples that illustrate the difference between access control and data protection mechanisms. Explain

8. (2 points) What are the required properties of good <u>hash function</u>? Select all applicable.

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

Answers: _____

9. (2 points) What are the required properties of good <u>stream cipher</u>? Select all applicable.

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

Answers: _____

10. (2 points) What are the required properties of good <u>block cipher</u>? Select all applicable.

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

Answers: _____