EECE 412, Fall 2004

Quiz #1

Your Family name: ____________________________
Your First name: ____________________________
Your student ID: ____________________________

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

1. What is "Computer Security"? Select one

A. It's authentication, access control, virus protection, and audit.
B. It's safety and freedom from worry when using computers.
C. It's a set of mechanisms for preventing bad things from happening, detecting such things, and recovering from them.
D. It's confidentiality, integrity, and availability of the data and services accessible through computers.

Answer: _____

2. What are the goals of computer security? Select all applicable.

A. Prevention
B. Assurance
C. Detection
D. Insurance
E. Safety
F. Recovery

Answers: ____________________

3. Which are the correct limitations of the fortress analogy applied to computer security? Select all applicable.

A. Fortress security is about protecting the insiders from outsiders, whereas computer security is about protecting the system and its assets from outsiders as well as insiders.
B. Fortress protection requires a lot of resources to create the defense layers and maintain them, whereas computer security does not require substantial resources.
C. Computers have to be kept usable even when they are under attack, whereas fortresses can concentrate on the defense and postpone normal service, while under attack.
D. Fortress defense mechanisms cannot be changed, whereas

computer security mechanisms have to protect from new types of attacks.

Answers: ____________________

4. What computer security policies are concerned with? Select one.

A. Confidentiality
B. Safety
C. Availability
D. Integrity
E. All of the above
F. A, C, D

Answer: _____

5. What are the major groups of security functionality that comprise protection? Select all applicable.

A. Cryptography
B. Assurance
C. Availability
D. Non-repudiation
E. Authorization
F. Authentication
G. Access Control
H. Accountability
I. Data protection
J. Audit
K. Recovery

Answers: ____________________

6. When should access control mechanisms be used? Select one.

A. When there is no way to check the rules
B. When there no trust to enforce the rules
C. When it is possible to enforce and check the rules

Answer: _____

7. Which of the following functionalities would you use to prevent a compromise of the integrity and confidentiality of wireless communications? Select all applicable.

A. Design, implementation, and operation assurance
B. Access control
C. Data protection
D. Non-repudiation

E. Disaster recovery

Answers: ____________________

8. If you have to collect evidence about malicious behavior or breach of contract by another entity for presenting in court, which accountability mechanism would you prefer to use? Select one.

A. Non-repudiation
B. Security audit

Answer: _____

9. Most computer security mechanisms are (Select all applicable):

A. Precise
B. Secure
C. Broad

Answers: ____________________

10. The value of risk depends on which of the following factors? Select all applicable.

A. The level of assurance
B. Value of assets to be secured
C. Threats
D. Vulnerabilities

Answers: ____________________

11. What class of threats does spoofing belong to? Select all applicable.

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

Answers: ____________________

12. What are the most effective ways to break Caesar Cipher? Select all applicable.

A. Differential cryptanalysis
B. Key recovery through exhaustive search
C. Statistical cryptanalysis

D. Linear cryptanalysis
E. Distance factoring

Answers: ____________________

13. What are the most effective ways to break Vigenere Cipher? Select all applicable.

A. Differential cryptanalysis
B. Key recovery through exhaustive search
C. Statistical cryptanalysis
D. Linear cryptanalysis
E. Distance factoring

Answers: ____________________

14. Which of the following ciphers are provably unbreakable? Select all applicable.

A. Caesar cipher
B. Monoalphabetic cipher
C. One-time Pad
D. Vigenere Cipher
E. DES
F. Rail-Fence Cipher

Answers: ____________________

15. What are the required properties of good random function? Select all applicable.

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

Answers: ____________________

16. What are the required properties of good random generator (stream cipher)? Select all applicable.

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

Answers: ____________________

17. What are the required properties of good random permutation (block cipher)? Select all applicable.

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

Answers: ____________________

18. A good block cipher should consist of (Select all applicable):

A. substitutions
B. transpositions
C. permutations
D. substitutions and permutations
E. transpositions and permutations

Answer: _____

19. Main techniques for breaking S-boxes are (Select all applicable)

A. frequency analysis
B. statistical analysis
C. linear cryptanalysis
D. black-box testing
E. differential cryptanalysis

Answers: ____________________

20. For encrypting PIN, 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: _____

21. For encrypting a file, 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: _____

22. For encrypting a video stream, 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: _____

23. The most appropriate for protecting message integrity and authenticity is (select one):

A. SHA-1
B. MD5
C. HMAC
D. AES
E. DES

Answer: _____

24. Backward security can be achieved with any of the following (Select all applicable):

A. message hashing
B. autokeying
C. time stamping
D. key updating

Answers: ____________________

25. Forward security can be achieved with any of the following (Select all applicable):

A. message hashing
B. autokeying
C. time stamping
D. key updating

Answers: ____________________