1. 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

2. 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

3. 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

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

a. substitutions
b. transpositions
c. permutations
*d. substitutions and permutations
e. transpositions and permutations

5. Most modern encryption algorithms encrypt digital data at which level?

*a. Bit level
b. Byte level
c. Alpha-numeric level
d. Block level

6. Under certain circumstances, which of the following methods could encrypt identical plaintext to produce identical cyphertext? (pick one)

a. Vigenere's Cipher
b. One Time Pad
c. Caesar's Cipher
d. A and C from above
*e. A, B, and C from above

7. What makes it more difficult to brute force search multiple passwords at once, but does not make it more difficult to brute force search a single password hash? (pick one)

a. Shadowing
*b. Salting
c. Password Hiding
d. Pepper
e. Paprika

8. One wayness is a trait that is most useful to which of the following? (pick one)

a. Symmetric Encryption
b. Public Key Encryption
*c. Hash Functions
d. A and B from above
e. A, B, and C from above

9. Which of the following encipherment techniques is based on the use of prime numbers? (pick all applicable)

a. Diffie / Hellman
*b. RSA
c. One Time Pads

10. Which of the following (select all applicable ) conditions must a public key cryptosystems meet?

*a. It must be computationally easy to encipher or decipher a message given the appropriate key.
*b. It must be computationally infeasible to derive the private key from the public key.
*c. It must be computationally infeasible to determine the private key from a chosen plaintext attack.
d. It must be computationally infeasible to derive the public key from the private key.

11. Why is ORCON a separate type of access control?

a. It's a separate type due to the historical reasons.
b. It deals with digital rights management.
*c. Unlike DAC, ORCON allows the control over the information to its creator, not owner. It does not use mandatory rules of MAC.
d. DAc is for academic domain, MAC is for military and government. ORCON is for neither.

12. Compare and contrast the assumptions made in the design of the hierarchical X.509/X.500 PKI and the PGP Web of trust.

13. An X.509 certificate revocation list contains a field specifying when the next such list is expected to be issued. Why is this field present?

14. What weakness of Needham-Schroeder key exchange protocol did the introduction of a time stamp by Denning-Sacco address? (pick one)

a. Needham-Schroeder protocol was weak against message replay attacks.
b. Nonces could be accidentally re-used by the exchanging parties.
c. Time stamps help to distinguish between concurrent sessions.
*d. A recovered session key could later be used to start a new session.

15. If you were to deploy Kerberos at UBC, what service ticket life-time would be the most appropriate? (pick one)

a. 30 seconds
b. 1 minute
*c. 5 minutes
d. 1 hour
e. 1 day

16. You are ECE IT manager and are asked to provide secure access to the department POP and SMTP services for users who need access to them from the outside of the UBC intranet. Which of the two options, TLS vs. IPSec, would you choose and why?

17. Even if you secure access to the ECE mail services using TLS or IPSec the services are still vulnerable to online password guessing attacks. Which of the following countermeasures would you employ against such attacks? Select all applicable

a. Salting
b. Pronounceable passwords
c. Violator imprisoning
*d. "jailing"
*e. account disabling
f. user firing
*g. disconnection
h. physical security of the services
*i. backoff strategies

18. Why is it generally better to use multi-factor authentication instead of one-factor authentication?

19. "The information in this mid-term exam key file should not be accessible to this course students until after the exam is over." Which one of the following properties pertaining to the mid-term exam key file is the above statement about?

a. accountability
*b. confidentiality
c. availability
d. integrity
e. assurance