Week 8 Assignment B

1. Digital signature properties:
   a. authentication
   b. non-repudiation
   c. integrity
   d. confidentiality
   e. non-repudiation

   a. proves small block of data
   b. proves message integrity
   c. does not guarantee data
   d. is used for confidentiality

3. To authenticate the data origin, one needs:
   a. Message Digest Code (MD5)
   b. Message Authentication Code (MAC)
   c. signature for the data
   d. all of the above

4. Authorization issues:
   a. verification of user identification
   b. verification of the data
   c. confidentiality
   d. integrity
   e. non-repudiation

5. Digest created by a hash function is normally called:
   a. encryption code
   b. message integrity code
   c. message authentication code
   d. message hash
   e. digital signature

6. When data must arrive at a receiver exactly or they are lost, it is called:
   a. message reliability
   b. message integrity
   c. message encryption
   d. message non-repudiation
   e. message confidentiality

7. La-Dee-Dah-Dee is a key exchange protocol, if two parties are not authenticated to create other files. One step in the security of the protocol:
   a. use the key in the attack
   b. encrypt the key
   c. discover the attack
   d. use of the middle attack
   e. none of the above

8. Hash function is a function which usually takes as arbitrary size of data and
   a. creates a small and fixed size of data
   b. creates a small and random size of data
   c. creates a large size of input data
   d. creates a ciphertext

9. Electronic signatures are:
   a. used to be faster than RSA signatures
   b. less secure than RSA signatures
   c. more efficient than RSA signatures
   d. not secure
   e. none of the above

10. What can be the technique to avoid collisions in a hash function?
    a. use the hash function
    b. use the chaining method
    c. use another hash function
    d. all of the above