## Quiz Questions

1. Which of the following statements pertaining to message digests is incorrect?
   1. The original file cannot be created from the message digest.
   2. Two files should not have the same message digest.
   3. The message digest should be calculated using at least 128 bytes of the file.
   4. Messages digests are usually of fixed size.
2. A public key algorithm that does both encryption and digital signature is which of the following?
   1. RSA
   2. DES
   3. IDEA
   4. Diffie-Hellman
3. Which of the following statements is most accurate regarding a digital signature?
   1. It is a method used to encrypt confidential data.
   2. It is the art of transferring handwritten signature to electronic media.
   3. It allows the recipient of data to prove the source and integrity of data.
   4. It can be used as a signature system and a cryptosystem.
4. Which of the following identifies the encryption algorithm selected by NIST for the new Advanced Encryption Standard?
   1. Twofish
   2. Serpent
   3. RC6
   4. Rijndael
5. What principle involves encryption keys being separated into two components, each of which does not reveal the other?
   * + 1. Dual control
       2. Separation of duties
       3. Split knowledge
       4. Need to know
6. Cryptography does not concern itself with:
   1. Availability
   2. Integrity
   3. Confidentiality
   4. Authenticity
7. How many rounds are used by DES?
   1. 16
   2. 32
   3. 64
   4. 48
8. What can be defined as secret communications where the very existence of the message is hidden?
   1. Clustering
   2. Steganography
   3. Cryptology
   4. Vernam cipher
9. A Public Key Infrastructure (PKI) is:
   1. An infrastructure for handling escrowed keys.
   2. Cheaper to built and maintain in-house that using 3rd-party certificates.
   3. It is responsible for: issuing, locating, validating, renewing, and revoking certificates.
   4. Private Key Infrastructure.
10. Which of the following is best provided by symmetric cryptography?
    1. Confidentiality
    2. Integrity
    3. Availability
    4. Non-repudiation

## Homework

1. Read chapters 9 and 10 in the Sybex textbook if you haven’t done so already.
2. Write a **one page** summary for the Cryptography Domain to use for studying.
3. Make time to do lots of sample questions… and do them!

## Preparing for Lesson 9 – Application Security

1. Read chapters 7 and 8 in the Sybex textbook if you haven’t done so already.