Chapter 4- Quiz

1.What is the name of the method in which letters are rearranged to create the ciphertext?

- enigma
- substitution
- transposition
- one-time pad

Explanation: Ciphertext can be created by using the following:

Transposition – letters are rearranged

Substitution – letters are replaced

One-time pad – plaintext combined with a secret key creates a new character, which then combines with the plaintext to produce ciphertext

2.Which 128-bit block cipher encryption algorithm does the US government use to protect classified information?

- Vignere
- AES
- Caesar
- 3DES
- Skipjack

Explanation: The Advanced Encryption Standard (AES) is used to protect classified information by the U.S. government and is a strong algorithm that uses longer key lengths.

3. Which term describes the technology that protects software from unauthorized access or modification?

- copyright
- access control
- trademark
- watermarking

Explanation: Software watermarking inserts a secret message into the program as proof of ownership and protects software from unauthorized access or modification.

4.Which three devices represent examples of physical access controls? (Choose three.)

- swipe cards
- firewalls
- locks
- routers
- servers
- video cameras

Explanation:

Physical access controls include but are not limited to the following:Guards

Fences

Motion detectors

Laptop locks

Locked doors

Swipe cards

Guard dogs

Video cameras

Mantraps

Alarms

5.What term is used to describe the technology that replaces sensitive information with a nonsensitive version?

- retracting
- hiding
- blanking
- whiteout
- masking

Explanation: Data masking replaces sensitive information with nonsensitive information. After replacement, the nonsensitive version looks and acts like the original.

6.Which type of cipher is able to encrypt a fixed-length block of plaintext into a 128-bit block of ciphertext at any one time?

- transform
- hash
- symmetric
- stream
- block

Explanation: Block ciphers transform a fixed-length block of plaintext into a block of ciphertext. To decrypt the ciphertext, the same secret key to encrypt is used in reverse.

7.What encryption algorithm uses the same pre-shared key to encrypt and decrypt data?

- hash
- asymmetric
- one-time pad
- symmetric

Explanation: Symmetric encryption algorithms use the same pre-shared key to encrypt and decrypt data.

8.What type of cipher encrypts plaintext one byte or one bit at a time?

- block
- hash
- enigma
- stream
- elliptical

Explanation: Stream ciphers encrypt plaintext one byte or one bit at a time, and can be much faster than block ciphers.

9.What cryptographic algorithm is used by the NSA and includes the use of elliptical curves for digital signature generation and key exchange?

- ECC
- RSA
- AES
- El-Gamal
- IDEA

Explanation: Elliptic curve cryptography (ECC) uses elliptic curves as part of the algorithm for digital signature generation and key exchange.

10.What is the term used to describe the science of making and breaking secret codes?

- impersonation
- spoofing
- factorization
- cryptology
- jamming

Explanation: Cryptology is the science of making and breaking codes to make sure that cyber criminals cannot easily compromise protected information.

11.Which three processes are examples of logical access controls? (Choose three.)

- guards to monitor security screens
- firewalls to monitor traffic
- swipe cards to allow access to a restricted area
- fences to protect the perimeter of a building
- intrusion detection system (IDS) to watch for suspicious network activity
- biometrics to validate physical characteristics

Explanation: Logical access controls includes but is not limited to the following:

Encryption

Smart cards

Passwords

Biometrics

Access Control Lists (ACLs)

Protocols

Firewalls

Intrusion Detection Systems (IDS)

12.What term is used to describe concealing data in another file such as a graphic, audio, or other text file?

- hiding
- steganography
- obfuscation
- masking

Explanation: Steganography conceals data in a file such as a graphic, audio, or other text file and is used to prevent extra attention to the encrypted data because the data is not easily viewed.

13.What are three examples of administrative access controls? (Choose three.)

- hiring practices
- intrusion detection system (IDS)
- policies and procedures
- background checks
- guard dogs
- encryption

Explanation: Administrative access controls are defined by organizations to implement and enforce all aspects of controlling unauthorized access and include the following:

Policies

Procedures

Hiring practices

Background checks

Data classification

Security training

Reviews

14.Which three protocols use asymmetric key algorithms? (Choose three.)

- Telnet
- Secure Shell (SSH)
- Advanced Encryption Standard (AES)
- Pretty Good Privacy (PGP)
- Secure File Transfer Protocol (SFTP)
- Secure Sockets Layer (SSL)

Explanation: Four protocols use asymmetric key algorithms:

Internet Key Exchange (IKE)

Secure Socket Layer (SSL)

Secure Shell (SSH)

Pretty Good Privacy (PGP)

15.A warning banner that lists the negative outcomes of breaking company policy is displayed each time a computer user logs in to the machine. What type of access control is implemented?

- detective
- preventive
- masking
- deterrent

Explanation: Deterrents are implemented to discourage or mitigate an action or the behavior of a malicious person.

16.Which two terms are used to describe cipher keys? (Choose two.)

- key space
- key randomness
- keylogging
- key length

17.Match the type of multifactor authentication with the description.

- a security key fob ————> something you have
- a fingerprint scan ————> something you are
- a password ————> something you know

Explanation: Multi-factor authentication uses a minimum of two methods of verification and can include the following:

Something you have

Something you know

Something you are

18.Match the description with the correct term. (Not all targets are used.)

- steganography ——————> hiding data within an audio file
- steganalysis ——————> discovering that hidden information exists within a graphic file
- social steganography ——> creating a message that says one thing but means something else to a specific audience
- obfuscation ——————> making a message confusing so it is harder to understand
- Other Incorrect Match Options:
  - replacing sensitive information in a file with nonsensitive information

19.Which asymmetric algorithm provides an electronic key exchange method to share the secret key?

- WEP
- DES
- RSA
- Diffie-Hellman
- hashing

Explanation: Diffie-Hellman provides an electronic exchange method to share a secret key and is used by multiple secure protocols.

20.What encryption algorithm uses one key to encrypt data and a different key to decrypt data?

- asymmetric
- one-time pad
- transposition
- symmetric

Explanation: Asymmetric encryption uses one key to encrypt data and a different key to decrypt data.