Calendar

Question 1

Correct

Mark 2.00 out of 2.00

Flag question

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

Select one:

- transposition ✔
- enigma
- substitution
- one-time pad

Refer to curriculum topic: 4.1.1
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

The correct answer is: transposition

Question 2

Correct

Mark 2.00 out of 2.00

Flag question

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

Select one or more:

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

Refer to curriculum topic: 4.1.4
Four protocols use asymmetric key algorithms:

- Internet Key Exchange (IKE)

Show one page at a time Finish review

Question **3**

Correct

Mark 2.00 out of 2.00

Flag question

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

Select one:

- (•) steganography ✔
- ( ) masking
- ( ) hiding
- ( ) obfuscation

Refer to curriculum topic: 4.3.2
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.

The correct answer is: steganography

Question **4**

Correct

Mark 2.00 out of 2.00

Flag question

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

Select one or more:

- [ ] firewalls
- [ ] servers
- [x] swipe cards ✔
- [ ] routers
- [x] video cameras ✔
- [x] locks ✔

Refer to curriculum topic: 4.2.1
Physical access controls include but are not limited to the following:

- Guards
- Fences

Question **5**

Correct

Mark 2.00 out of 2.00

Flag question

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

Select one:

- asymmetric
- one-time pad
- symmetric ✔
- hash

Refer to curriculum topic: 4.1.1
Symmetric encryption algorithms use the same pre-shared key to encrypt and decrypt data.

The correct answer is: symmetric

Question **6**

Correct

Mark 2.00 out of 2.00

Flag question

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

Select one:

- El-Gamal
- ECC ✔
- IDEA
- RSA
- AES

Refer to curriculum topic: 4.1.3
Elliptic curve cryptography (ECC) uses elliptic curves as part of the algorithm for digital signature generation and key exchange.

The correct answer is: ECC

Question 7

Correct

Mark 2.00 out of 2.00

Flag question

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?

Select one:

- symmetric
- hash
- transform
- stream
- block ✔

Refer to curriculum topic: 4.1.2
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.

The correct answer is: block

Question 8

Correct

Mark 2.00 out of 2.00

Flag question

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

Select one or more:

- [ ] key randomness
- [x] key space ✔
- [ ] keylogging
- [x] key length ✔

Refer to curriculum topic: 4.1.4
The two terms used to describe keys are the following:

- **Key length -** Also called the key , this is the measure in bits.
- **Keyspace -** This is the number of possibilities that a specific key length can generate.

As key length increase, the keyspace increases exponentially.

Question **9**

Partially correct

Mark 1.00 out of 2.00

Flag question

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

steganalysis	hiding data within an audio file ✗
obfuscation	making a message confusing so it is harder to understand ✓
steganography	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 ✓

The correct answer is: steganalysis → discovering that hidden information exists within a graphic file, obfuscation → making a message confusing so it is harder to understand, steganography → hiding data within an audio file, social steganography → creating a message that says one thing but means something else to a specific audience

Question **10**

Correct

Mark 2.00 out of 2.00

Flag question

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

Select one:

- spoofing
- factorization
- impersonation
- cryptology ✓
- jamming

Refer to curriculum topic: 4.1.1
Cryptology is the science of making and breaking codes to make sure that cyber criminals cannot easily compromise protected information.

The correct answer is: cryptology

Question **11**

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

Question **11**

Correct

Mark 2.00 out of 2.00

Flag question

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

Select one:

- Caesar
- Vignere
- 3DES
- Skipjack
- AES ✔

Refer to curriculum topic: 4.1.2
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.

The correct answer is: AES

Question **12**

Correct

Mark 2.00 out of 2.00

Flag question

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

Select one:

- enigma
- block
- elliptical
- stream ✔
- hash

Refer to curriculum topic: 4.1.2
Stream ciphers encrypt plaintext one byte or one bit at a time, and can be much faster than block ciphers.

Question **13**

Incorrect

Mark 0.00 out of 2.00

Flag question

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

Select one:

- (•) symmetric ✖
- ( ) one-time pad
- ( ) asymmetric
- ( ) transposition

Refer to curriculum topic: 4.1.1
Asymmetric encryption uses one key to encrypt data and a different key to decrypt data.

The correct answer is: asymmetric

Question **14**

Correct

Mark 2.00 out of 2.00

Flag question

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

Select one or more:

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

Refer to curriculum topic: 4.2.1
Logical access controls includes but is not limited to the following:

- Encryption
- Smart cards
- Passwords

for suspicious network activity

Question **15**

Correct

Mark 2.00 out of 2.00

Flag question

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?

Select one:

- deterrent ✔
- preventive
- detective
- masking

Refer to curriculum topic: 4.2.7
Deterrents are implemented to discourage or mitigate an action or the behavior of a malicious person.

The correct answer is: deterrent

Question **16**

Correct

Mark 2.00 out of 2.00

Flag question

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

Select one:

- hiding
- blanking
- masking ✔
- retracting
- whiteout

Refer to curriculum topic: 4.3.1
Data masking replaces sensitive information with nonsensitive information. After replacement, the nonsensitive version looks and acts like the

Question **17**

Correct

Mark 2.00 out of 2.00

Flag question

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

Select one or more:

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

Refer to curriculum topic: 4.2.1
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

The correct answers are: policies and procedures, background checks, hiring practices

Question **18**

Correct

Mark 2.00 out of 2.00

Flag question

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

Select one:

- ( ) access control
- ( ) trademark
- (•) watermarking ✔

Question **19**

Correct

Mark 2.00 out of 2.00

Flag question

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

Select one:

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

Refer to curriculum topic: 4.1.3
Diffie-Hellman provides an electronic exchange method to share a secret key and is used by multiple secure protocols.

The correct answer is: Diffie-Hellman

Question **20**

Correct

Mark 2.00 out of 2.00

Flag question

Match the type of multifactor authentication with the description.

a password	something you know ✔
a fingerprint scan	something you are ✔
a security key fob	something you have ✔

Refer to curriculum topic: 4.2.4
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

The correct answer is: a password → something you know, a fingerprint scan → something you are, a security key fob → something you have