**Quiz -1**

**Your Answers:**

**Results for question 1.**

1

1 / 1 point

Which term ensures that a system operates as intended, free from both intentional and unintentional unauthorized manipulations?



Privacy

, Not Selected



Availability

, Not Selected



Data confidentiality

, Not Selected

Correct answer:



System integrity

**Results for question 2.**

2

0 / 1 point

Is the primary focus for countering passive attacks on stopping them before they happen rather than spotting them once they have?

True

Incorrect answer:

False

Correct Answer:True

**Results for question 3.**

3

1 / 1 point

Which U.S. federal institution focuses on standards, measurement science, and fostering technological advancements in the private sector?



ISO

, Not Selected



ITU-T

, Not Selected



ISOC

, Not Selected

Correct answer:



NIST

**Results for question 4.**

4

1 / 1 point

What ensures that users' identities are genuine and each input stems from a trusted source?



Confidentiality

, Not Selected

Correct answer:



Authenticity



Accountability

, Not Selected



Integrity

, Not Selected

**Results for question 5.**

5

1 / 1 point

A

Correct answer:

digital signature

 can either be data attached to, or a cryptographic transformation of a data unit, enabling the recipient to verify its source and integrity, and safeguarding against counterfeiting.

**Results for question 6.**

6

1 / 1 point

Which type of attacks are aimed at changing system resources or affecting their function?



Release of message content

, Not Selected



Passive

, Not Selected



Traffic analysis

, Not Selected

Correct answer:



Active

**Results for question 7.**

7

1 / 1 point

When designing a security mechanism or algorithm, is it essential to anticipate potential threats to it?

Correct answer:

True

False

**Results for question 8.**

8

0 / 1 point

Are pervasive security methods unrelated to any specific OSI security function or protocol tier?

True

Incorrect answer:

False

Correct Answer:True

**Results for question 9.**

9

1 / 1 point

Is a breach in confidentiality defined as the unauthorized alteration or elimination of data?

True

Correct answer:

False

**Results for question 10.**

10

0 / 1 point

In computer security, three main principles are confidentiality, availability, and

Incorrect answer:

Integrity

Correct Answer:integrity

.

The security goal requiring each entity's actions to be traceable solely to that entity is known as what?



Authenticity

, Not Selected



Integrity

, Not Selected

Correct answer:



Accountability



Privacy

, Not Selected

### Results for question 2.

2

0 / 1 point

Incorrect answer:

Encryption

Correct Answer:encipherment, encryption, cryptography

 involves the application of mathematical procedures to transform data into a scrambled format, which can then be recovered using specific algorithms and keys.

### Results for question 3.

3

1 / 1 point

Is a breach in confidentiality defined as the unauthorized alteration or elimination of data?

True

Correct answer:

False

### Results for question 4.

4

1 / 1 point

What refers to the act of stopping unauthorized resource utilization?



Authentication

, Not Selected

Correct answer:



Access control



Nonrepudiation

, Not Selected



Data confidentiality

, Not Selected

### Results for question 5.

5

1 / 1 point

Is the primary focus for countering passive attacks on stopping them before they happen rather than spotting them once they have?

Correct answer:

True

False

### Results for question 6.

6

0 / 1 point

A deliberate action, intending to bypass security measures and breach the system's security guidelines, is termed as

Incorrect answer:

malicious activity

Correct Answer:attack

.

### Results for question 7.

7

1 / 1 point

Besides replay, message modification, and denial of service, active attacks also include

Correct answer:

masquerade

 as a category.

### Results for question 8.

8

1 / 1 point

Is the purpose of data integrity to prevent unauthorized data exposure?

True

Correct answer:

False

### Results for question 9.

9

1 / 1 point

Which type of attacks are aimed at changing system resources or affecting their function?



Release of message content

, Not Selected



Passive

, Not Selected



Traffic analysis

, Not Selected

Correct answer:



Active

### Results for question 10.

10

1 / 1 point

Does data origin authentication shield against copying or altering data units?

True

Correct answer:

False

Did the advent of computers lead to an increased demand for tools to safeguard files and other stored data?

Correct answer:

True

False

### Results for question 2.

2

0 / 1 point

Within network security, the capacity to manage and restrict access to host systems via communication pathways is termed

Incorrect answer:

Network access control

Correct Answer:access control, Access Control

.

### Results for question 3.

3

1 / 1 point

Do users and system administrators often undervalue security investments until a breach happens?

Correct answer:

True

False

### Results for question 4.

4

0 / 1 point

Would you classify patient allergy details as data that has a medium priority for maintaining its accuracy?

Incorrect answer:

True

Correct Answer:False

False

### Results for question 5.

5

1 / 1 point

Which U.S. federal institution focuses on standards, measurement science, and fostering technological advancements in the private sector?



ISOC

, Not Selected

Correct answer:



NIST



ITU-T

, Not Selected



ISO

, Not Selected

### Results for question 6.

6

1 / 1 point

Is the purpose of data integrity to prevent unauthorized data exposure?

True

Correct answer:

False

### Results for question 7.

7

1 / 1 point

When designing a security mechanism or algorithm, is it essential to anticipate potential threats to it?

Correct answer:

True

False

### Results for question 8.

8

1 / 1 point

Is the primary focus for countering passive attacks on stopping them before they happen rather than spotting them once they have?

Correct answer:

True

False

### Results for question 9.

9

1 / 1 point

Correct answer:

encryption

 involves the application of mathematical procedures to transform data into a scrambled format, which can then be recovered using specific algorithms and keys.

### Results for question 10.

10

1 / 1 point

A deliberate action, intending to bypass security measures and breach the system's security guidelines, is termed as

Correct answer:

attack

In symmetric encryption, the primary challenge for security lies in safeguarding the \_\_\_\_\_\_\_\_\_.

Correct answer:

key

### Results for question 2.

2

1 / 1 point

The foundation of AES is the Feistel framework.

True

Correct answer:

False

### Results for question 3.

3

1 / 1 point

Stream ciphers dominate the list of widely utilized symmetric encryption algorithms.

True

Correct answer:

False

### Results for question 4.

4

1 / 1 point

Reusing keys is a benefit of block ciphers.

Correct answer:

True

False

### Results for question 5.

5

1 / 1 point

The algorithm responsible for various changes and conversions on the plaintext is the \_\_\_\_\_\_\_\_\_.

Correct answer:



encryption



keystream

, Not Selected



codebook

, Not Selected



cipher

, Not Selected

### Results for question 6.

6

1 / 1 point

The Data Encryption Standard algorithm incorporates a key size of \_\_\_\_\_\_\_\_\_.



168 bit

, Not Selected



128 bit

, Not Selected

Correct answer:



56 bit



32 bit

, Not Selected

### Results for question 7.

7

1 / 1 point

The compromise between encryption/decryption speed and security is affected by smaller block sizes.

True

Correct answer:

False

### Results for question 8.

8

1 / 1 point

A method that exhaustively tries every conceivable key to decode ciphertext is known as the \_\_\_\_\_\_\_\_\_ approach.



block cipher

, Not Selected



computational

, Not Selected

Correct answer:



brute-force



triple DES

, Not Selected

### Results for question 9.

9

1 / 1 point

In the \_\_\_\_\_\_\_\_ mode, a flaw in a block of transmitted ciphertext affects only its corresponding plaintext block.



TSR

, Not Selected



CBC

, Not Selected



CTS

, Not Selected

Correct answer:



ECB

### Results for question 10.

10

1 / 1 point

The security of a symmetric block cipher intensifies with the addition of more rounds.

Correct answer:

True

False