

1.Which of the following terms refers to a weakness in a system that could be exploited to compromise security?

- A) Threat
- B) Vulnerability
- C) Exploit
- D) Authentication

View answer

Answer: B) Vulnerability

Explanation: A vulnerability is a weakness in a system that could be exploited by a threat to cause harm.

2.What principle of security ensures that information is accessible only to those who are authorized to access it?

- A) Confidentiality
- B) Integrity
- C) Availability
- D) Authentication

View answer

Answer: A) Confidentiality

Explanation: Confidentiality ensures that information is not disclosed to unauthorized individuals or systems.

3.Which security principle ensures that data remains accurate and consistent over its entire lifecycle?

- A) Confidentiality

- B) Integrity
- C) Availability
- D) Authentication

View answer

Answer: B) Integrity

Explanation: Integrity ensures that data remains accurate and consistent, and has not been altered by unauthorized means.

4.Which term refers to the process of verifying the identity of a user or system?

- A) Threat
- B) Vulnerability
- C) Exploit
- D) Authentication

View answer

Answer: D) Authentication

Explanation: Authentication is the process of verifying the identity of a user or system.

5.Nonrepudiation ensures that:

- A) Data is accessible only to authorized users.
- B) Data remains accurate and consistent.
- C) Users cannot deny their actions or transactions.
- D) Systems are protected against unauthorized access.

View answer

Answer: C) Users cannot deny their actions or transactions.

Explanation: Nonrepudiation ensures that users cannot deny the authenticity of their actions or transactions.

6.Which of the following is NOT a category of security attack?

- A) Physical
- B) Logical
- C) Social
- D) Environmental

View answer

Answer: D) Environmental

Explanation: The categories of security attacks typically include physical, logical, and social attacks.

7.Which mathematical principle forms the foundation for many cryptographic algorithms?

- A) Pythagoras' Theorem
- B) Fermat's Theorem
- C) Euler's Theorem
- D) Pascal's Theorem

View answer

Answer: C) Euler's Theorem

Explanation: Euler's Theorem is fundamental in cryptography, forming the basis for various cryptographic algorithms.

8.What is the key concept behind the Euclidean Algorithm?

- A) Finding prime numbers

- B) Solving modular equations
- C) Computing greatest common divisors
- D) Calculating discrete logarithms

View answer

Answer: C) Computing greatest common divisors

Explanation: The Euclidean Algorithm is used to compute the greatest common divisor of two integers.

9.The Chinese Remainder Theorem is used for:

- A) Calculating discrete logarithms
- B) Solving systems of linear equations
- C) Factoring large integers
- D) Finding solutions to simultaneous congruences

View answer

Answer: D) Finding solutions to simultaneous congruences

Explanation: The Chinese Remainder Theorem is used to find solutions to a system of simultaneous congruences.

10.What is the significance of prime numbers in cryptography?

- A) They ensure nonrepudiation
- B) They form the basis of symmetric encryption
- C) They are used in key exchange algorithms
- D) They are difficult to factorize, making them useful in encryption schemes

View answer

Answer: D) They are difficult to factorize, making them useful in encryption schemes

Explanation: Prime numbers are crucial in cryptography because of their difficulty in factorization, which forms the basis of many encryption schemes.

Related posts:

1. Introduction to Information Security
2. Introduction to Information Security MCQ
3. Symmetric Key Cryptography MCQ
4. Asymmetric Key Cryptography MCQ
5. Authentication & Integrity MCQ
6. E-mail, IP and Web Security MCQ