1. What is the primary goal of security?
   A) Ensuring confidentiality
   B) Providing availability
   C) Maintaining integrity
   D) All of the above

View answer
Answer: D) All of the above
Explanation: Security aims to ensure confidentiality, availability, and integrity of data and resources.

2. Which of the following is NOT a basic security terminology?
   A) Threat
   B) Intrusion
   C) Exploit
   D) Analysis

View answer
Answer: D) Analysis
Explanation: Threat, intrusion, and exploit are common security terminologies, while analysis is a process.

3. Which security principle focuses on ensuring that information is only accessible to authorized parties?

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

View answer
Answer: A) Confidentiality
Explanation: Confidentiality ensures that information is protected from unauthorized access.

4. Which mathematical theorem states that every composite number has a prime factorization?
   A) Fermat’s Theorem
   B) Euler’s Theorem
   C) Fundamental Theorem of Arithmetic
   D) Chinese Remainder Theorem

View answer
Answer: C) Fundamental Theorem of Arithmetic
Explanation: The Fundamental Theorem of Arithmetic states that every composite number can be expressed uniquely as a product of prime numbers.

5. What is the process of verifying the identity of a user or system?
   A) Authorization
   B) Authentication
   C) Encryption
   D) Decryption

View answer
Answer: B) Authentication
Explanation: Authentication is the process of confirming the identity of a user or system.

6. Which security attack involves exploiting vulnerabilities to gain unauthorized access or perform malicious actions?
   A) Denial of Service (DoS)
   B) Man-in-the-Middle (MitM)
   C) Phishing
   D) Exploit

View answer
Answer: D) Exploit
Explanation: Exploits involve taking advantage of vulnerabilities to compromise security.

7. Which mathematical concept is crucial for cryptographic algorithms like RSA?
   A) Prime Number
   B) Modular Arithmetic
   C) Discrete Logarithm
   D) Chinese Remainder Theorem

View answer
Answer: A) Prime Number
Explanation: Prime numbers play a fundamental role in many cryptographic algorithms, including RSA.

8. Which security principle ensures that data is accurate and reliable?

A) Confidentiality
B) Integrity
C) Availability
D) Nonrepudiation

View answer
Answer: B) Integrity
Explanation: Integrity ensures that data remains accurate and unaltered.

9. What type of attack aims to overwhelm a system with excessive traffic, rendering it unavailable to legitimate users?
   A) Phishing
   B) Spoofing
   C) Denial of Service (DoS)
   D) Man-in-the-Middle (MitM)

View answer
Answer: C) Denial of Service (DoS)
Explanation: DoS attacks flood a system with traffic, making it inaccessible to legitimate users.

10. Which theorem states that if p is a prime number and a is any positive integer less than p, then a^(p-1) ≡ 1 (mod p)?
    A) Fermat’s Theorem
    B) Euler’s Theorem
    C) Chinese Remainder Theorem
    D) Fundamental Theorem of Arithmetic

View answer

Answer: A) Fermat’s Theorem

Explanation: Fermat’s Little Theorem is a fundamental theorem in number theory, which has applications in cryptography.

Related posts:

1. Introduction to Information Security MCQ
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