1.Modular arithmetic is primarily concerned with operations involving:
A) Real numbers
B) Complex numbers
C) Integers within a fixed range
D) Rational numbers

View answer
Answer: C) Integers within a fixed range
Explanation: Modular arithmetic deals with operations on integers within a fixed range.

2.Which algorithm is commonly used to find the modular multiplicative inverse?
A) RSA algorithm
B) Diffie-Hellman algorithm
C) ElGamal algorithm
D) Extended Euclidean Algorithm

View answer
Answer: D) Extended Euclidean Algorithm
Explanation: The Extended Euclidean Algorithm is commonly used to find the modular multiplicative inverse, which is crucial in many cryptographic algorithms.

3.Discrete logarithms are particularly relevant in:
A) Symmetric cryptography
B) Asymmetric cryptography
C) Hash functions
D) Digital signatures

View answer
Answer: B) Asymmetric cryptography
Explanation: Discrete logarithms play a significant role in asymmetric cryptography, particularly in algorithms like Diffie-Hellman and ElGamal.

4.Which of the following is NOT a fundamental principle of security?
A) Confidentiality
B) Integrity
C) Availability
D) Completeness

View answer
Answer: D) Completeness
Explanation: Completeness is not a fundamental principle of security. The principles are Confidentiality, Integrity, and Availability (CIA).

5.An example of a social engineering attack is:
A) Phishing
B) Distributed Denial of Service (DDoS)
C) SQL Injection
D) Buffer Overflow

View answer
Answer: A) Phishing
Explanation: Phishing is a type of social engineering attack that manipulates individuals into revealing sensitive information.

6.Which mathematical concept is essential for asymmetric encryption?
A) Fermat’s Little Theorem
B) Euler’s Totient Function
C) Modular Arithmetic
D) Discrete Logarithms

View answer
Answer: D) Discrete Logarithms
Explanation: Discrete logarithms are crucial in asymmetric encryption algorithms like Diffie-Hellman and ElGamal

7.The concept of nonrepudiation is closely related to which security principle?
A) Confidentiality
B) Integrity
C) Availability
D) Authenticity

View answer
Answer: D) Authenticity
Explanation: Nonrepudiation ensures the authenticity of actions or transactions, making it closely related to the principle of Authenticity.

8.A security vulnerability is:
A) An attack on a system’s availability
B) A weakness in a system that can be exploited
C) A measure of the likelihood of a security breach
D) A cryptographic algorithm used for key exchange

View answer

Answer: B) A weakness in a system that can be exploited

Explanation: A security vulnerability is a weakness in a system that could be exploited to compromise security.

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