1. What branch of mathematics forms the foundation of modern cryptography?

a) Calculus
b) Geometry
c) Abstract Algebra
d) Trigonometry

Answer: c) Abstract Algebra

Explanation: Abstract Algebra, particularly concepts like groups, rings, and fields, provides the mathematical framework used in cryptographic algorithms.

2. Which mathematical concept is used to encrypt data in the RSA algorithm?

a) Prime factorization
b) Differential equations
c) Matrix multiplication
d) Integration

Answer: a) Prime factorization

Explanation: RSA encryption relies on the difficulty of factoring large composite numbers into their prime factors.

3. What is the primary purpose of the Extended Euclidean Algorithm in cryptography?

a) Generating prime numbers
b) Finding modular inverses

c) Generating random keys
d) Performing frequency analysis

Answer: b) Finding modular inverses

Explanation: The Extended Euclidean Algorithm is used to find the modular inverse of a number, which is crucial in many cryptographic operations, such as RSA encryption and decryption.

4. Which theorem states that if p is a prime number and a is an integer not divisible by p, then (a^{p-1}) is congruent to 1 modulo p?

a) Euler's Theorem
b) Fermat's Little Theorem
c) Wilson's Theorem
d) Lagrange's Theorem

Answer: b) Fermat's Little Theorem

Explanation: Fermat's Little Theorem is a fundamental theorem in number theory that has significant applications in cryptography.

5. What is the purpose of the Euler Phi-Function in cryptography?

a) Generating prime numbers
b) Calculating modular inverses
c) Calculating the number of relatively prime integers
d) Generating random keys

Answer: c) Calculating the number of relatively prime integers

Explanation: The Euler Phi-Function ((\phi(n))) calculates the number of positive integers less than n that are relatively prime to n, which is essential in cryptographic algorithms like RSA.

6. Which classical cryptosystem uses a 5×5 grid of letters for encryption?

a) Caesar Cipher
b) Playfair Cipher
c) Vigenère Cipher
d) Atbash Cipher

Answer: b) Playfair Cipher

Explanation: The Playfair Cipher encrypts pairs of letters using a 5×5 grid of letters, known as a Playfair Square.

7. What technique is commonly used to break the substitution cipher by analyzing letter frequencies?

a) Differential cryptanalysis
b) Frequency analysis
c) Linear cryptanalysis
d) Brute-force attack

Answer: b) Frequency analysis

Explanation: Frequency analysis involves analyzing the frequency of letters or symbols in a ciphertext to deduce information about the plaintext.

8. Which of the following is NOT a block cipher?

a) AES
b) DES
c) RSA
d) Blowfish

Answer: c) RSA

Explanation: RSA is a public-key encryption algorithm, whereas AES, DES, and Blowfish are block ciphers.

9. Which mode of operation is commonly used for encrypting large files with block ciphers?

a) ECB (Electronic Codebook)
b) CBC (Cipher Block Chaining)
c) CTR (Counter)
d) OFB (Output Feedback)

Answer: b) CBC (Cipher Block Chaining)

Explanation: CBC mode is commonly used for encrypting large files because it introduces diffusion and prevents patterns in the plaintext from being apparent in the ciphertext.

10. Which encryption standard is based on the Feistel cipher structure?

a) AES
b) DES
c) RSA
d) ElGamal

Answer: b) DES

Explanation: DES (Data Encryption Standard) is based on the Feistel cipher structure, which involves multiple rounds of substitution and permutation.

11. Which cipher operates on individual characters or bits of plaintext one at a time?

a) Block Cipher
b) Stream Cipher
c) Public Key Cipher
d) Transposition Cipher

Answer: b) Stream Cipher

Explanation: Stream ciphers encrypt plaintext one bit or character at a time, typically using a keystream generator.

12. What is the key length of Triple DES (3DES)?

a) 56 bits
b) 112 bits
c) 128 bits
d) 168 bits

Answer: b) 112 bits

Explanation: Triple DES (3DES) has a key length of 112 bits, derived from its three stages of DES encryption.

13. Which mode of operation XORs the plaintext with the output of a pseudorandom keystream generator?

a) ECB (Electronic Codebook)
b) CBC (Cipher Block Chaining)
c) CTR (Counter)
d) OFB (Output Feedback)

Answer: d) OFB (Output Feedback)

Explanation: OFB mode XORs the plaintext with the output of a pseudorandom keystream generator, which is then fed back to generate subsequent keystreams.

14. In which classical cipher does each letter in the plaintext get replaced by a letter some fixed number of positions down the alphabet?

a) Caesar Cipher
b) Playfair Cipher
c) Rail Fence Cipher
d) Affine Cipher

Answer: a) Caesar Cipher

Explanation: The Caesar Cipher is a substitution cipher where each letter in the plaintext is shifted by a fixed number of positions down or up the alphabet.

15. Which type of cryptanalysis involves using known plaintext and corresponding ciphertext pairs to deduce the key?

a) Differential cryptanalysis
b) Frequency analysis
c) Known-plaintext attack
d) Chosen-plaintext attack

Answer: c) Known-plaintext attack

Explanation: Known-plaintext attacks exploit the knowledge of plaintext-ciphertext pairs to deduce information about the encryption key.

16. Which cryptographic principle states that the security of the system should not depend on keeping the algorithm secret, but rather on keeping the key secret?

a) Kerckhoffs’s Principle
b) Diffie-Hellman Principle
c) Shannon’s Principle
d) Turing’s Principle

Answer: a) Kerckhoffs’s Principle

Explanation: Kerckhoffs’s Principle states that the security of a cryptographic system should rely on the secrecy of the key rather than the secrecy of the algorithm itself.

17. Which cipher mode is vulnerable to a watermarking attack?

a) ECB (Electronic Codebook)
b) CBC (Cipher Block Chaining)
c) CTR (Counter)
d) OFB (Output Feedback)

Answer: a) ECB (Electronic Codebook)

Explanation: ECB mode encrypts identical plaintext blocks into identical ciphertext blocks, making it vulnerable to a watermarking attack where patterns in the plaintext can be discerned from the ciphertext.

18. Which mode of operation is known for its parallelizability and efficiency in hardware implementations?

a) ECB (Electronic Codebook)
b) CBC (Cipher Block Chaining)
c) CTR (Counter)
d) OFB (Output Feedback)

Answer: c) CTR (Counter)

Explanation: CTR mode turns a block cipher into a stream cipher, allowing for parallel encryption and decryption, making it efficient for hardware implementations.

19. What type of cipher uses a key to perform a series of transformations on the plaintext?

a) Symmetric Cipher
b) Asymmetric Cipher
c) Hash Function
d) Steganography

Answer: a) Symmetric Cipher

Explanation: Symmetric ciphers use the same key for both encryption and decryption to perform a series of transformations on the plaintext.

20. Which cryptographic technique ensures data integrity by generating a fixed-size hash based on the input data?

a) Encryption
b) Digital Signature
c) Key Exchange
d) Hash Function

Answer: d) Hash Function

Explanation: Hash functions generate fixed-size hash values based on the input data, which can be used to verify the integrity of the data without revealing the original content.

Related posts:

1. Introduction to Information Security
2. Introduction to Information Security MCQ
3. Introduction to Information Security MCQ

4. Symmetric Key Cryptography MCQ
5. Asymmetric Key Cryptography MCQ
6. Authentication & Integrity MCQ
7. E-mail, IP and Web Security MCQ