1.Which cryptographic technique is used for secure key exchange over insecure channels?
a) Symmetric Key Cryptography
b) Asymmetric Key Cryptography
c) Hash Functions
d) Block Ciphers

View answer
Answer: b) Asymmetric Key Cryptography
Explanation: Asymmetric key cryptography, also known as public-key cryptography, is used for secure key exchange over insecure channels, such as the Diffie-Hellman key exchange algorithm.

2.Which algorithm is commonly used for digital signatures?
a) RSA
b) Diffie-Hellman
c) AES
d) SHA-256

View answer
Answer: a) RSA
Explanation: RSA (Rivest-Shamir-Adleman) algorithm is commonly used for digital signatures as well as encryption and key exchange.

3.Diffie-Hellman key exchange is vulnerable to which type of attack?
a) Man-in-the-Middle Attack
b) Brute Force Attack
c) Side-channel Attack

d) Birthday Attack

View answer
Answer: a) Man-in-the-Middle Attack
Explanation: Diffie-Hellman key exchange is vulnerable to the man-in-the-middle attack, where an attacker intercepts and alters communication between two parties.

4.Which asymmetric key cryptography algorithm is based on the discrete logarithm problem?
a) RSA
b) ECC (Elliptic Curve Cryptography)
c) Diffie-Hellman
d) ElGamal

View answer
Answer: c) Diffie-Hellman
Explanation: Diffie-Hellman key exchange is based on the discrete logarithm problem.

5.Which asymmetric key cryptography algorithm is particularly suitable for resource-constrained devices?
a) RSA
b) ECC (Elliptic Curve Cryptography)
c) Diffie-Hellman
d) ElGamal

View answer
Answer: b) ECC (Elliptic Curve Cryptography)
Explanation: ECC is particularly suitable for resource-constrained devices due to its shorter

key lengths compared to other algorithms like RSA.

6.Which attack aims to reveal information by observing patterns in encrypted data or using statistical analysis?
a) Ciphertext-Only Attack
b) Known-Plaintext Attack
c) Chosen-Plaintext Attack
d) Frequency Analysis Attack

View answer
Answer: d) Frequency Analysis Attack
Explanation: Frequency analysis attack aims to reveal information by observing patterns in encrypted data or using statistical analysis.

7.Which type of attack exploits weaknesses in the implementation of cryptographic algorithms rather than breaking the algorithms themselves?
a) Ciphertext-Only Attack
b) Known-Plaintext Attack
c) Implementation Attack
d) Side-Channel Attack

View answer
Answer: c) Implementation Attack
Explanation: Implementation attacks exploit weaknesses in the implementation of cryptographic algorithms rather than breaking the algorithms themselves.

8.Which attack involves submitting specially crafted input to a system to exploit

vulnerabilities in its cryptographic operations?
a) Chosen-Plaintext Attack
b) Chosen-Ciphertext Attack
c) Buffer Overflow Attack
d) Birthday Attack

View answer
Answer: c) Buffer Overflow Attack
Explanation: Buffer overflow attack involves submitting specially crafted input to a system to exploit vulnerabilities in its cryptographic operations.

9.Which attack aims to exploit the fact that the same plaintext is encrypted to the same ciphertext under the same key?
a) Replay Attack
b) Birthday Attack
c) Known-Plaintext Attack
d) Ciphertext-Only Attack

View answer
Answer: a) Replay Attack
Explanation: Replay attack aims to exploit the fact that the same plaintext is encrypted to the same ciphertext under the same key.

10.Which attack attempts to determine the private key by gathering pairs of corresponding plaintext and ciphertext?
a) Ciphertext-Only Attack
b) Known-Plaintext Attack

c) Chosen-Plaintext Attack
d) Chosen-Ciphertext Attack

View answer
Answer: b) Known-Plaintext Attack
Explanation: Known-plaintext attack attempts to determine the private key by gathering pairs of corresponding plaintext and ciphertext.

11.Which asymmetric key cryptography algorithm relies on the difficulty of factoring large composite numbers?
a) RSA
b) ECC
c) ElGamal
d) Diffie-Hellman

View answer
Answer: a) RSA
Explanation: RSA relies on the difficulty of factoring large composite numbers for its security.

12.Which attack exploits information gained from observing the physical implementation of a cryptographic system, such as power consumption or electromagnetic radiation?
a) Side-Channel Attack
b) Brute Force Attack
c) Chosen-Plaintext Attack
d) Collision Attack

View answer

Answer: a) Side-Channel Attack
Explanation: Side-channel attack exploits information gained from observing the physical implementation of a cryptographic system, such as power consumption or electromagnetic radiation.

13.Which asymmetric key cryptography algorithm is based on the difficulty of solving the discrete logarithm problem in a finite field?
a) RSA
b) ECC
c) ElGamal
d) Diffie-Hellman

View answer
Answer: c) ElGamal
Explanation: ElGamal encryption algorithm is based on the difficulty of solving the discrete logarithm problem in a finite field.

14.Which type of attack involves submitting multiple queries to a cryptographic system to obtain information that can be used to compromise its security?
a) Birthday Attack
b) Chosen-Plaintext Attack
c) Chosen-Ciphertext Attack
d) Ciphertext-Only Attack

View answer
Answer: c) Chosen-Ciphertext Attack
Explanation: Chosen-ciphertext attack involves submitting multiple queries to a

cryptographic system to obtain information that can be used to compromise its security.

15.Which attack aims to find two different inputs that produce the same hash value?
a) Brute Force Attack
b) Collision Attack
c) Rainbow Table Attack
d) Dictionary Attack

View answer
Answer: b) Collision Attack
Explanation: Collision attack aims to find two different inputs that produce the same hash value.

16.Which asymmetric key cryptography algorithm is widely used for secure key exchange?
a) RSA
b) Diffie-Hellman
c) ElGamal
d) ECC

View answer
Answer: b) Diffie-Hellman
Explanation: Diffie-Hellman algorithm is widely used for secure key exchange.

17.Which attack involves intercepting and altering communication between two parties without their knowledge?
a) Replay Attack
b) Man-in-the-Middle Attack

c) Chosen-Plaintext Attack
d) Known-Plaintext Attack

View answer
Answer: b) Man-in-the-Middle Attack
Explanation: Man-in-the-middle attack involves intercepting and altering communication between two parties without their knowledge.

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. Authentication & Integrity MCQ
6. E-mail, IP and Web Security MCQ