1. Which cryptographic technique ensures the integrity and authenticity of a message by appending a unique code generated with a private key?
a) Message Authentication Code (MAC)
b) Digital Signature
c) Hash Function
d) Key Exchange

Answer: b) Digital Signature
Explanation: Digital signatures use asymmetric cryptography to sign messages with a private key, allowing recipients to verify the authenticity and integrity using the corresponding public key.

2. What is the primary purpose of a digital signature?
a) Encryption
b) Authentication
c) Compression
d) Decryption

Answer: b) Authentication
Explanation: Digital signatures primarily serve to authenticate the sender of a message and ensure the integrity of the transmitted data.

3. Which cryptographic technique is used to securely distribute encryption keys between parties?
a) Message Authentication
b) Digital Signature
c) Key Management

d) Key Exchange

Answer: d) Key Exchange
Explanation: Key exchange protocols facilitate the secure distribution of cryptographic keys between communicating parties to establish a shared secret key for encrypted communication.

4. Which type of hashing algorithm is designed to minimize the likelihood of collisions by using a randomization technique?
a) Universal Hashing
b) Cryptographic Hash Function
c) MD Hash Function
d) Secure Hash Algorithm (SHA)

Answer: a) Universal Hashing
Explanation: Universal hashing involves randomly selecting a hash function from a family of hash functions, reducing the probability of collisions.

5. Which cryptographic hash function is widely used for its security and resistance to collision attacks?
a) MD5
b) SHA-1
c) SHA-256
d) SHA-512

Answer: c) SHA-256
Explanation: SHA-256 is part of the SHA-2 family of cryptographic hash functions and is

known for its security and resistance to collision attacks.

6. Which cryptographic attack exploits the trade-off between memory and computation to reduce the time complexity of breaking a cipher?
a) Differential Cryptanalysis
b) Time-Memory Trade-off Attack
c) Birthday Attack
d) Chosen-Plaintext Attack

Answer: b) Time-Memory Trade-off Attack
Explanation: Time-memory trade-off attacks exploit the trade-off between computation and memory usage to reduce the time complexity of cryptographic attacks.

7. Which cryptographic standard is used for digital signatures in the US government and other applications requiring high levels of security?
a) Message Digest (MD)
b) Digital Signature Standard (DSS)
c) Data Encryption Standard (DES)
d) Advanced Encryption Standard (AES)

Answer: b) Digital Signature Standard (DSS)
Explanation: DSS is a standard for digital signatures, specified by the National Institute of Standards and Technology (NIST) in the United States.

8. Which cryptographic attack focuses on analyzing the differences in input and output of a cryptographic algorithm to break its security?
a) Time-Memory Trade-off Attack

b) Differential Cryptanalysis
c) Birthday Attack
d) Meet-in-the-Middle Attack

Answer: b) Differential Cryptanalysis
Explanation: Differential cryptanalysis involves studying the differences in the input and output of a cryptographic algorithm to exploit patterns and break its security.

9. Which cryptographic system provides secure authentication for network services by using tickets and a trusted third party?
a) RSA
b) AES
c) Kerberos
d) SSL/TLS

Answer: c) Kerberos
Explanation: Kerberos is a network authentication protocol that provides secure authentication by using tickets and a trusted third-party authentication server.

10. What is the primary function of a hash function in cryptography?
a) Encryption
b) Compression
c) Authentication
d) Key Exchange

Answer: c) Authentication
Explanation: Hash functions are primarily used for authentication purposes, ensuring the

integrity and authenticity of data by generating fixed-size hash values.

11. Which cryptographic algorithm is vulnerable to length extension attacks and is no longer considered secure for cryptographic purposes?
a) MD5
b) SHA-1
c) SHA-256
d) SHA-512

Answer: a) MD5
Explanation: MD5 is vulnerable to length extension attacks and is no longer considered secure for cryptographic purposes due to its susceptibility to collisions.

12. Which cryptographic technique involves the use of symmetric keys to ensure the integrity and authenticity of transmitted data?
a) Digital Signature
b) Message Authentication Code (MAC)
c) Key Exchange
d) Public Key Infrastructure (PKI)

Answer: b) Message Authentication Code (MAC)
Explanation: MACs use symmetric keys to generate authentication tags for verifying the integrity and authenticity of transmitted data.

13. Which cryptographic technique ensures the confidentiality of data by converting it into an unreadable format using a secret key?
a) Hash Function

b) Digital Signature
c) Encryption
d) Key Exchange

Answer: c) Encryption
Explanation: Encryption involves converting plaintext into ciphertext using a secret key, ensuring the confidentiality of data.

14. What is the primary objective of key management in cryptography?
a) Ensuring message integrity
b) Facilitating secure communication
c) Managing cryptographic keys securely
d) Preventing cryptographic attacks

Answer: c) Managing cryptographic keys securely
Explanation: Key management involves the secure generation, distribution, storage, and destruction of cryptographic keys to ensure the security of cryptographic systems.

15. Which cryptographic attack exploits the probability of two different inputs producing the same hash output?
a) Birthday Attack
b) Chosen-Plaintext Attack
c) Differential Cryptanalysis
d) Side-Channel Attack

Answer: a) Birthday Attack
Explanation: Birthday attacks exploit the probability of collisions in hash functions, where two

different inputs produce the same hash output.

16. Which cryptographic standard specifies the use of SHA-2 for secure hash functions?
a) Digital Signature Standard (DSS)
b) Data Encryption Standard (DES)
c) Advanced Encryption Standard (AES)
d) Secure Hash Algorithm (SHA)

Answer: a) Digital Signature Standard (DSS)
Explanation: DSS specifies the use of SHA-2 (including SHA-256, SHA-384, and SHA-512) for secure hash functions in digital signatures.

17. Which cryptographic attack focuses on exploiting weaknesses in the generation of random numbers in cryptographic systems?
a) Birthday Attack
b) Differential Cryptanalysis
c) Side-Channel Attack
d) Random Number Generation Attack

Answer: d) Random Number Generation Attack
Explanation: Random number generation attacks exploit weaknesses in the generation of random numbers in cryptographic systems to compromise their security.

18. Which cryptographic algorithm is widely used for symmetric-key encryption and decryption?
a) RSA
b) AES

c) ECC
d) Diffie-Hellman

Answer: b) AES
Explanation: Advanced Encryption Standard (AES) is widely used for symmetric-key encryption and decryption due to its efficiency and security.

19. Which cryptographic technique involves the use of mathematical functions to convert data into a fixed-size string of bytes?
a) Digital Signature
b) Message Authentication Code (MAC)
c) Hash Function
d) Key Exchange

Answer: c) Hash Function
Explanation: Hash functions are mathematical functions used to convert data into a fixed-size string of bytes, ensuring data integrity and authenticity.

20. Which cryptographic protocol provides secure communication over an insecure network through encryption, authentication, and integrity protection?
a) SSH
b) HTTP
c) FTP
d) SSL/TLS

Answer: a) SSH
Explanation: Secure Shell (SSH) protocol provides secure communication over an insecure

network through encryption, authentication, and integrity protection.

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