1.Which of the following cryptographic techniques is primarily used for ensuring message integrity?

A) MAC

B) Hash function

C) SHA

D) Digital signature

View answer

Answer: B) Hash function

Explanation: Hash functions generate fixed-size outputs for variable-size inputs, ensuring data integrity by detecting even minor changes in the data.

2.What does MAC stand for in the context of cryptography?

A) Message Authentication Code

B) Main Authentication Cipher

C) Mutual Authentication Control

D) Master Authentication Code

View answer

Answer: A) Message Authentication Code

Explanation: MAC is a cryptographic technique used to verify the integrity and authenticity of a message.

3.Which cryptographic hash function is considered more secure and commonly used: MD5 or SHA-256?

A) MD5

B) SHA-256

View answer

Answer: B) SHA-256

Explanation: SHA-256 is a more secure hash function compared to MD5, which is vulnerable to collision attacks.

4.HMAC is an extension of which cryptographic technique?

A) MAC

B) Hash function

C) Digital signature

D) Public-key cryptography

View answer

Answer: A) MAC

Explanation: HMAC (Hash-based Message Authentication Code) is a specific type of MAC that utilizes a cryptographic hash function.

5.Which cryptographic technique involves the use of asymmetric keys for verification?

A) MAC

B) Hash function

C) Digital signature

D) HMAC

View answer

Answer: C) Digital signature

Explanation: Digital signatures provide authenticity and integrity using public-key cryptography.

6.Which authentication protocol is commonly used for securing internet communication, providing secure and encrypted connections?

A) OAuth

B) SSL/TLS

C) Kerberos

D) LDAP

View answer

Answer: B) SSL/TLS

Explanation: SSL/TLS protocols provide secure communication over the internet by encrypting data and ensuring authentication.

7.What does X.509 Digital Certificate primarily ensure in a communication?

A) Message integrity

B) Authentication

C) Authorization

D) Access control

View answer

Answer: B) Authentication

Explanation: X.509 Digital Certificates are used for authentication, ensuring that the communication parties are who they claim to be.

8.Which access control mechanism grants or denies access based on the user’s identity and their permissions?

A) Discretionary Access Control (DAC)

B) Mandatory Access Control (MAC)

C) Role-Based Access Control (RBAC)
D) Attribute-Based Access Control (ABAC)

View answer
Answer: C) Role-Based Access Control (RBAC)
Explanation: RBAC grants access based on predefined roles and permissions assigned to users.

9.In cryptographic terms, what does the term “authorization” refer to?
A) Verifying the identity of communication parties
B) Ensuring the integrity of transmitted data
C) Granting or denying access to resources based on permissions
D) Generating digital signatures for authentication

View answer
Answer: C) Granting or denying access to resources based on permissions
Explanation: Authorization involves determining what actions or resources a user is allowed to access.

10.Which of the following is NOT an example of an authentication protocol?
A) Kerberos
B) OAuth
C) SAML
D) HMAC

View answer
Answer: D) HMAC

Explanation: HMAC is a cryptographic technique, not an authentication protocol.

11.Which cryptographic technique is suitable for ensuring both data integrity and authenticity?
A) Digital signature
B) HMAC
C) Hash function
D) MAC

View answer
Answer: A) Digital signature
Explanation: Digital signatures provide both data integrity and authenticity.

12.Which hash function is considered more secure between SHA-1 and SHA-256?
A) SHA-1
B) SHA-256

View answer
Answer: B) SHA-256
Explanation: SHA-256 is more secure compared to SHA-1, which is vulnerable to collision attacks.

13.Which cryptographic technique is commonly used for securing communication between a web browser and a server?
A) HMAC
B) Digital signature
C) SSL/TLS

D) Kerberos

View answer

Answer: C) SSL/TLS

Explanation: SSL/TLS protocols are commonly used for securing web communication.

14.What does HMAC stand for?

A) Hash-based Message Authentication Code

B) Highly Mutual Authentication Cipher

C) Hyper Media Authentication Control

D) Hashed MAC

View answer

Answer: A) Hash-based Message Authentication Code

Explanation: HMAC stands for Hash-based Message Authentication Code, a specific type of MAC.

15.Which digital certificate format is widely used for securing web communication?

A) X.509

B) SSL

C) TLS

D) PEM

View answer

Answer: A) X.509

Explanation: X.509 digital certificates are widely used for securing web communication.

16.Which access control mechanism is based on assigning permissions directly to users or groups?

A) Discretionary Access Control (DAC)

B) Mandatory Access Control (MAC)

C) Role-Based Access Control (RBAC)

D) Attribute-Based Access Control (ABAC)

View answer

Answer: A) Discretionary Access Control (DAC)

Explanation: DAC allows users or groups to have control over the access permissions of their own resources.

17.Which cryptographic hash function is commonly used for generating checksums and verifying file integrity?

A) MD5

B) SHA-1

C) SHA-256

D) HMAC

View answer

Answer: C) SHA-256

Explanation: SHA-256 is commonly used for file integrity verification due to its security properties.

18.Which authentication protocol is commonly used in Windows environments for single sign-on authentication?

A) OAuth

B) SAML

C) LDAP

D) Kerberos

View answer

Answer: D) Kerberos

Explanation: Kerberos is commonly used in Windows environments for single sign-on authentication.

19.Which digital certificate format is commonly used for email encryption and code signing?

A) X.509

B) SSL

C) PGP

D) TLS

View answer

Answer: C) PGP

Explanation: Pretty Good Privacy (PGP) is commonly used for email encryption and code signing.

20.Which cryptographic technique involves using both a private key and a public key for verification?

A) MAC

B) HMAC

C) Digital signature

D) Hash function

View answer

Answer: C) Digital signature
Explanation: Digital signatures use a private key for signing and a public key for verification, ensuring authenticity and integrity.

## 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. E-mail, IP and Web Security MCQ