El cifrado: mensajes secretos en internet

Nombre: _____

Fecha: _____

Puntaje: _____

1.

¿Qué hace el cifrado con los datos?

1. Los elimina permanentemente
2. Los comprime para ahorrar espacio
3. Los vuelve ilegibles para proteger la privacidad
4. Los ordena alfabéticamente

Respuesta correcta:
C.

Los vuelve ilegibles para proteger la privacidad

2.

En el cifrado simétrico, ¿qué se utiliza para cifrar y descifrar?

1. Una misma clave compartida
2. Dos claves diferentes
3. Ninguna clave

Respuesta correcta:
A.

Una misma clave compartida

3.

¿Cuál es la principal diferencia entre el cifrado simétrico y el asimétrico?

1. El asimétrico usa un par de claves (pública y privada)
2. El simétrico es más lento
3. El asimétrico no requiere clave
4. El simétrico solo cifra mensajes cortos

Respuesta correcta:
A.

El asimétrico usa un par de claves (pública y privada)

4.

El algoritmo de cifrado 'Advanced Encryption Standard' es conocido por las siglas _____.

Respuesta: _____

Respuesta correcta:

AES

5.

¿Qué protocolo de seguridad utiliza HTTPS para cifrar la comunicación entre el navegador y el servidor?

1. FTP
2. SSL/TLS
3. HTTP
4. SMTP

Respuesta correcta:
B.

SSL/TLS

6.

¿Qué proporciona una firma digital en un mensaje?

1. Confidencialidad
2. Compresión
3. Autenticidad e integridad
4. Velocidad de transmisión

Respuesta correcta:
C.

Autenticidad e integridad

7.

En el contexto del cifrado, ¿qué es una 'clave'?

1. Una contraseña
2. Un candado
3. Un dato utilizado para cifrar y descifrar información

Respuesta correcta:
C.

Un dato utilizado para cifrar y descifrar información

8.

La técnica de cifrado más antigua que desplaza las letras un número fijo de posiciones se llama cifrado _____.

Respuesta: _____

Respuesta correcta:

César

9.

¿Cuál es la función principal de un hash criptográfico?

1. Cifrar datos para mantenerlos secretos
2. Producir una salida de tamaño fijo a partir de cualquier entrada
3. Comprimir datos
4. Generar números aleatorios

Respuesta correcta:
B.

Producir una salida de tamaño fijo a partir de cualquier entrada

10.

Un hash muy común que genera un valor de 256 bits se conoce como _____.

Respuesta: _____

Respuesta correcta:

SHA-256

11.

¿Por qué es importante almacenar las contraseñas de los usuarios usando funciones hash (y no en texto plano)?

1. Para protegerlas en caso de una filtración de datos
2. Para ahorrar espacio en la base de datos
3. Para acelerar el inicio de sesión
4. Para que los usuarios no las puedan cambiar

Respuesta correcta:
A.

Para protegerlas en caso de una filtración de datos

12.

Un ataque de intermediario (man-in-the-middle) ocurre cuando:

1. El atacante se sitúa físicamente entre dos dispositivos
2. El atacante intercepta y posiblemente altera la comunicación entre dos partes
3. Se inserta un virus en el sistema
4. La conexión es lenta

Respuesta correcta:
B.

El atacante intercepta y posiblemente altera la comunicación entre dos partes

13.

La seguridad del algoritmo RSA se basa en la dificultad matemática de:

1. Calcular logaritmos discretos
2. Resolver curvas elípticas
3. Invertir funciones
4. Factorizar números grandes en primos

Respuesta correcta:
D.

Factorizar números grandes en primos

14.

¿Cuál es la función principal de una Autoridad Certificadora (CA, por sus siglas en inglés)?

1. Crear contraseñas seguras
2. Cifrar todo el tráfico de internet
3. Emitir certificados digitales que validan la titularidad de claves públicas
4. Administrar direcciones IP

Respuesta correcta:
C.

Emitir certificados digitales que validan la titularidad de claves públicas

15.

¿Cuál es la diferencia clave entre codificar y cifrar?

1. Son lo mismo
2. Codificar es reversible sin clave; cifrar requiere una clave para revertir
3. Codificar comprime datos; cifrar los expande
4. Codificar usa algoritmos; cifrar no

Respuesta correcta:
B.

Codificar es reversible sin clave; cifrar requiere una clave para revertir

16.

Un método de cifrado que utiliza una clave tan larga como el mensaje y es teóricamente irrompible se llama _____.

Respuesta: _____

Respuesta correcta:

one-time pad

17.

Agregar un valor aleatorio único a cada contraseña antes de aplicar un hash se conoce como:

1. Salting
2. Peppering
3. Sazonado
4. Codificación

Respuesta correcta:
A.

Salting

18.

¿Cuál de estos protocolos de cifrado inalámbrico se considera inseguro y fácil de descifrar?

1. WPA2
2. SSL
3. AES
4. WEP

Respuesta correcta:
D.

WEP

19.

El protocolo TLS (Transport Layer Security) se utiliza principalmente para:

1. Comprimir archivos
2. Verificar correos electrónicos
3. Asegurar la comunicación en una red informática
4. Formatear documentos

Respuesta correcta:
C.

Asegurar la comunicación en una red informática

20.

La criptografía cuántica promete ser segura porque:

1. Utiliza ordenadores extremadamente rápidos
2. Usa claves muy largas
3. Se basa en la física clásica
4. Cualquier intento de espiar la comunicación altera el estado cuántico y se detecta

Respuesta correcta:
D.

Cualquier intento de espiar la comunicación altera el estado cuántico y se detecta

Respuestas

1. **C.**

   Los vuelve ilegibles para proteger la privacidad

2. **A.**

   Una misma clave compartida

3. **A.**

   El asimétrico usa un par de claves (pública y privada)

4. AES

5. **B.**

   SSL/TLS

6. **C.**

   Autenticidad e integridad

7. **C.**

   Un dato utilizado para cifrar y descifrar información

8. César

9. **B.**

   Producir una salida de tamaño fijo a partir de cualquier entrada

10. SHA-256

11. **A.**

    Para protegerlas en caso de una filtración de datos

12. **B.**

    El atacante intercepta y posiblemente altera la comunicación entre dos partes

13. **D.**

    Factorizar números grandes en primos

14. **C.**

    Emitir certificados digitales que validan la titularidad de claves públicas

15. **B.**

    Codificar es reversible sin clave; cifrar requiere una clave para revertir

16. one-time pad

17. **A.**

    Salting

18. **D.**

    WEP

19. **C.**

    Asegurar la comunicación en una red informática

20. **D.**

    Cualquier intento de espiar la comunicación altera el estado cuántico y se detecta