Las siguientes preguntas solo tienen una respuesta correcta. Cada respuesta correcta suma 1 punto, cada incorrecta resta 0.4 y las no contestadas no puntúan. El test completo evalúa sobre 4 puntos del total del examen.

1. Sea H(x) una función hash criptográfica. ¿Qué propiedad conferimos a un mensaje M si enviamos $M \| H(M)$, donde $\|$ indica concatenación?
   - A. Autenticación
   - B. Integridad
   - **C.** Nada, porque un atacante podría interceptar el mensaje y recalcular el hash
   - D. Confidencialidad

2. ¿Qué modo de encadenamiento es vulnerable al ataque semántico?
   - A. ECB y CBC
   - **B.** Únicamente ECB
   - C. Todos los modos de cifradores simétricos
   - D. Ninguno

3. ¿Qué elementos necesita un emisor mantener secretos al cifrar un mensaje con AES CBC?
   - A. La clave de cifrado simétrica y el vector de inicialización
   - **B.** Solo la clave de cifrado
   - C. El vector de inicialización
   - D. La clave, el IV y el propio modo de encadenamiento

4. ¿Cuál es el tamaño de bloque de AES?
   - A. 128 bits
   - B. 256 bits
   - **C.** 128, 160, 192,... bits
   - D. No tiene un tamaño fijo

5. ¿Cuál es el tamaño mínimo recomendado para una clave simétrica de AES?
   - A. 128 bits
   - **B.** 256 bits
   - C. 64 bits
   - D. Ninguna de las anteriores

6. ¿Qué primitiva criptográfica garantiza el *no repudio*?
   - A. El cifrado
   - B. La integridad
   - C. RSA
   - **D.** La firma digital

7. ¿Qué clave contiene el certificado digital de una entidad?
   - **A.** Su clave pública, firmada con la privada de la CA
   - B. Su clave privada
   - C. Su clave privada, firmada con la privada de la CA
   - D. Su clave pública

8. ¿Cuál es el propósito del protocolo OCSP?
   - A. Firmar el certificado de una entidad
   - B. Comprobar la identidad de una entidad
   - **C.** Comprobar la validez de un certificado de forma interactiva
   - D. Generar listas CRLs

9. Imagina un sistema de almacenamiento de contraseñas que guarda cada contraseña c realizando la operación $H(c)$, donde $H(x)$ es la función SHA256. ¿Qué problema sufre este esquema?

A. Es vulnerable a un ataque online

B. Es vulnerable a ataques de tablas pre-computadas (Rainbow)

C. Es seguro, puesto que una función hash no se puede revertir

D. Es vulnerable a un ataque de fuerza bruta

10. Imagina una aplicación multimedia de VoIP. ¿Qué tipo de cifrado consideras más apropiado?

A. Simétrico de bloque

B. Asimétrico de bloque

C. Simétrico de flujo

D. Asimétrico de flujo