Las siguientes preguntas solo tienen una respuesta correcta. Cada respuesta correcta suma 1 punto, cada incorrecta resta 1/3 y las no contestadas no puntúan. El test completo evalúa sobre 3 puntos del total del examen.

1. ¿Qué modo de encadenamiento en el cifrado simétrico oculta las relaciones estadísticas en el texto en claro?
   - A. ECB
   - **B.** CBC
   - C. Todos los modos lo hacen
   - D. Ningún modo lo hace

2. Los cifrados de César y Vigenère son:
   - A. Cifrador de sustitución poli y monoalfabético, respectivamente
   - B. El algoritmo de César sí es un cifrador, Vigenère, no
   - **C.** Cifrador de sustitución mono y polialfabético, respectivamente
   - D. Cifrador de sustitución mono y de trasposición, respectivamente

3. A5/1 es un algoritmo de:
   - **A.** Cifrado en flujo
   - B. Cifrado en bloque
   - C. Cifrado asimétrico
   - D. Función hash

4. ¿Cuál es la probabilidad de colisión de la función hash SHA256, asumiendo que todas las entradas son equiprobables?
   - **A.** 2^{-256}
   - B. SHA256 no tiene colisiones
   - C. 2^{-128}
   - D. Dependerá de la similitud entre las entradas

5. ¿Cuál es el valor de $\phi(11)$?
   - A. 7
   - B. 8
   - C. 9
   - **D.** 10

6. ¿Qué elemento de una PKI genera las CRLs (*Certificate Revocation Lists*)?
   - A. RA
   - **B.** CA
   - C. VA
   - D. FNMT

7. ¿Qué elemento de una PKI genera las CRLs (*Certificate Revocation Lists*)?
   - A. RA
   - **B.** CA
   - C. VA
   - D. FNMT

8. El reto-respuesta es un tipo de autenticación de:
   - **A.** 3F
   - B. 2F
   - C. 1F
   - D. Ninguna de las otras respuestas es correcta

9. Aunque no sea recomendable cifrar directamente con un algoritmo asimétrico, ¿cuál sería el valor numérico máximo de un fichero que podría cifrar con RSA un usuario cuya clave pública fuera {533, 53593096303}

   A. 53593096303

   B. 533

   C. Aunque no sea recomendable, podría cifrar cualquier valor

   D. Haría falta saber el valor de la clave privada