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. ¿Qué propiedades confiere la firma digital de un mensaje?
   A. Autenticación
   B. Integridad
   C. Autenticación e integridad
   D. Confidencialidad

2. ¿Cuál es el objetivo principal del *vector de inicialización*?
   A. Servir de mezcla al bloque inicial en el modo CBC
   B. Ocultar los patrones en el texto de entrada
   C. Evitar la propagación de errores a otros bloques en el encadenamiento
   D. Aportar seguridad semántica en el modo ECB

3. ¿Cuál es el valor SHA256 de la cadena "si no conozco la respuesta correcta a esta pregunta, es que no he estudiado lo suficiente¿
   A. 946bbd2f94ba465071eb164942085e749972495f
   B. f1a79aec6c97e5fd54baabb63d665bf9
   C. 30e981d5cea2b0c6759f0b3546732f3f5f92b6a6aee963230792e138978ca9a1
   D. Es imposible responder a esta pregunta sin un ordenador

4. ¿Cuál es el tamaño mínimo recomendado para un IV?
   A. El tamaño mínimo depende de la longitud de la clave del cifrador utilizado
   B. No hay un tamaño mínimo, basta con que no sea predecible
   C. 16 bytes
   D. 32 bytes

5. En el criptosistema RSA, ¿cuál es un valor válido para d si hemos calculado que $e = 5$? Además, $p = 17$ y $q = 13$.
   A. 193
   B. 269
   C. 17
   D. No se puede determinar con estos parámetros

6. Imagina un sistema de almacenamiento de contraseñas, que utiliza salts para asegurar las mismas. Imagina que, en un momento dado, se utiliza el *salt* 'QxLU' (cada carácter se elige aleatoriamente de un alfabeto de 56 símbolos). ¿En qué factor se dificulta el ataque *offline*?
   A. 4
   B. El *salt* no dificulta el ataque *offline*
   C. 175616
   D. 9834496

7. ¿Para qué se utiliza el algoritmo PBKDF2?
   A. Para calcular valores HMAC
   B. Para generar números aleatorios
   C. Para proteger las contraseñas de los ataques online
   D. Para obtener una clave criptográfica a partir de una contraseña

8. ¿En qué problema matemático se basa el algoritmo ElGamal?
   A. En la factorización de enteros
   B. En curvas elípticas definidas sobre cuerpos finitos
   C. El logaritmo discreto
   D. Ninguno de los anteriores

9. ¿Quién verifica la identidad de una entidad en una PKI?
    A. La autoridad de certificación
    B. La autoridad de registro
    C. La autoridad de validación
    D. El servidor de destino

10. Imagina un sistema de autenticación para el control de acceso a una instalación física, basado en 'algo que poseemos'. En éste, se debe presentar una tarjeta ante un lector RFID (proximidad). ¿De qué tipo de sistema se trata?
    A. Sistema de autenticación de un factor (1F)
    B. Sistema de autenticación de doble factor (2F)
    C. Sistema de autenticación de triple factor (3F)
    D. Basado en reto/respuesta