Modelo 2

Las siguientes preguntas solo tienen una respuesta correcta. Cada respuesta correcta suma 1/2, cada incorrecta resta 1/6 de punto y las no contestadas no puntúan.

1. Si Alicia envía un mensaje a Bernardo con el siguiente esquema donde el símbolo $\oplus$ representa la concatenación: $K^B_{priv}(K_S) \oplus K_S[K^A_{pub}(H(m)) \oplus m]$, ¿qué asegura este esquema?
   - A. Autentica el origen del mensaje.
   - B. Asegura confidencialidad del mensaje.
   - **C.** Envía un mensaje inútil.
   - D. Autentica el origen del mensaje, y asegura la integridad y la confidencialidad del mensaje.

2. El handshake de SSL es seguro porque ...
   - A. ... se codifica con una clave simétrica el *mastersecret*, necesario para codificar de forma segura la comunicación.
   - **B.** ... ninguna de las otras.
   - C. ... aporta las claves privadas para el resto de la comunicación.
   - D. ... se intercambian la claves simétricas de forma segura.

3. El uso de un *salt* en el almacenamiento de claves ...
   - A. ... permite el almacenamiento de las claves en los servidores.
   - B. ... ninguna de las otras.
   - C. ... asegura que claves débiles sean seguras.
   - **D.** ... dificulta los ataques contra las claves de usuario.

4. ¿Qué esquema de codificación utilizó César sin pretenderlo?
   - A. RSA
   - B. DES
   - C. CBC
   - **D.** ECB

5. ¿Qué elementos puede contener un certificado?
   - A. La clave privada del usuario certificado.
   - B. La clave pública de la entidad certificadora.
   - **C.** Información personal del usuario.
   - D. La clave privada de la entidad certificadora.

6. Si Alicia envía un mensaje a Bernardo con el siguiente esquema donde el símbolo *oplus* representa la concatenación: $K^B_{pub}(K_S) \oplus K_S(m)$, ¿qué asegura este esquema?
   - A. Autentica el origen del mensaje.
   - **B.** Asegura confidencialidad del mensaje.
   - C. Envía un mensaje inútil.
   - D. Autentica el origen del mensaje, y asegura la integridad y la confidencialidad del mensaje.

7. ¿Cuál de las siguientes afirmaciones es cierta
   - **A.** Ninguna función hash es matemáticamente segura.
   - B. Los algoritmos de SHA son seguros porque no existen colisiones tal y como se demuestra matemáticamente.
   - C. MD5 es suficientemente seguro para almacenar contraseñas en una base de datos.
   - D. SHA256 es insegura por su gran número de colisiones.

8. ¿Para qué sirve una firma digital?
   - A. Asegurar la confidencialidad del mensaje.
   - B. Autenticar al emisor del mensaje.
   - C. Todas las respuestas son ciertas.
   - **D.** Asegurar la integridad de un mensaje.