Modelo 1

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

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

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

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

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

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

7. 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. Envía un mensaje inútil.
   B. Autentica el origen del mensaje, y asegura la integridad y la confidencialidad del mensaje.
   C. Autentica el origen del mensaje.
   D. Asegura confidencialidad del mensaje.

8. 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. Envía un mensaje inútil.
   B. Autentica el origen del mensaje, y asegura la integridad y la confidencialidad del mensaje.
   C. Autentica el origen del mensaje.
   D. Asegura confidencialidad del mensaje.