Modelo 4

Las siguientes preguntas solo tienen una respuesta correcta. Cada respuesta correcta suma 1 punto, cada incorrecta resta 1/4 y las no contestadas no puntúan. El test completo evalúa sobre 3 puntos del total del examen.

1. ¿A qué nivel opera un cifrador de flujo?
   - **A.** A nivel de bit
   - B. A nivel de byte
   - C. Utiliza un tamaño de bloque variable
   - D. Un cifrador de flujo no utiliza claves secretas

2. Imagina un cifrador de bloque que opera a nivel de byte y utiliza un modo de encadenamiento CBC, con IV = 0xAF. Para un texto en claro $m = 0xBC0478$, ¿cuál sería la entrada a la etapa de cifrado del primer bloque?
   - A. 0xAB
   - B. 0xAF
   - **C.** 0x13
   - D. No puede determinarse sin un valor para la clave secreta

3. Considera un criptosistema RSA con parámetros $p = 11$ y $q = 13$. Se sabe también que $e = 7$. ¿Cuál es un valor válido para d en este sistema?
   - A. 101
   - **B.** 103
   - C. 107
   - D. 105

4. Imagina que en una corporación se dispone de un total de 1.500 direcciones IP públicas. En un momento dado, se necesita que al menos 100.000 máquinas puedan acceder simultáneamente a Internet desde la red interna. ¿Qué esquema debería utilizarse?
   - A. VPN
   - **B.** NAT
   - C. VPN o NAT
   - D. VPN y NAT

5. ¿Qué elementos serían necesarios para diseñar un esquema de autenticación de doble factor?
   - A. Una tarjeta de coordenadas
   - B. Un token o teléfono móvil
   - C. Una contraseña
   - **D.** Una contraseña y una tarjeta de coordenadas

6. ¿Cuál es la función del *salt* en un esquema seguro de almacenamiento de contraseñas?
   - **A.** Dificultar los ataques offline
   - B. Dificultar los ataques online
   - C. Dificultar los ataques de diccionario
   - D. No tiene efecto sobre los posibles ataques a esquemas de contraseñas

7. ¿Con qué elemento se firma un certificado digital?
   - A. La clave privada de la Autoridad de Registro
   - **B.** La clave privada de la Autoridad de Certificación
   - C. La clave pública de la Autoridad de Certificación
   - D. La clave pública de la Autoridad de Registro

8. Imagina que auditas un sistema cortafuegos. ¿Qué regla deberías utilizar para implementar una política de *"todo lo que no está explícitamente permitido, está prohibido"*? Los campos de la regla son `ACTION-SOURCE ADDRESS-DESTINATION ADDRESS-PROTOCOL-SOURCE PORT-DESTINATION PORT-FLAG BIT`, respectivamente.

A. `deny all all all all all all`, como primera regla.

B. `deny all all all all all all`, como última regla.

C. `allow all all all all all all`, como primera regla.

D. `allow all all all all all all`, como última regla.

9. Cual de las siguientes secuencias de acciones aseguro la integridad del mensaje y la confidencialidad de este.

   A. Codifico con mi clave privada un mensaje y le concateno el hash del mensaje codificado

   B. Codifico un mensaje con la clave pública del destinatario y le concateno el hash del mensaje.

   C. Concateno el hash del mensaje al mensaje y codifico todo ello con la clave pública del destinatario

   D. Concateno el hash del mensaje al mensaje y codifico todo ello con mi clave privada.

10. Un ataque de denegación de servicio ataca a la implementación de una función de la librería POSIX de sockets. ¿A cuál?

    A. bind

    B. listen

    C. accept

    D. socket

11. Cual de estas afirmaciones es correcta en cuando a las operaciones sobre un certificado:

    A. Descodificando con la clave privada de la entidad certificadora obtengo la clave pública del propietario del certificado.

    B. Descodificando con la clave pública de la entidad certificadora obtengo la clave pública del propietario del certificado.

    C. Descodificando con la clave privada de la entidad certificadora obtengo la clave privada del propietario del certificado.

    D. Descodificando con la clave pública de la entidad certificadora obtengo la clave privada del propietario del certificado.

12. Si utilizo una autenticación de triple factor puedo afirmar:

    A. Que al incluir algo que sé es absolutamente segura.

    B. Que al incluir algo que soy es absolutamente segura.

    C. Que al incluir tres factores distintos es absolutamente segura.

    D. Que se trata del mecanismo de autenticación más seguro existente.