# Modelo 4

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 4 puntos del total del examen.

| Tabla de notación | |
|---|---|
| h | Función hash |
| \| | Concatenación |
| $K^E_{pub}$ | Cifrado con clave pública del emisor |
| $K^E_{prv}$ | Cifrado con clave privada del emisor |
| $K^R_{pub}$ | Cifrado con clave pública del receptor |
| $K^R_{prv}$ | Cifrado con clave privada del receptor |

1. Si se puede hacer una prueba de fuerza bruta contra una password cada 1 ms. ¿Cuánto se tardará como máximo en encontrar la clave si la password está construida con 6 letras minúsculas aleatorias?
   - **A.** Poco más de 4 días
   - B. Poco más de 1 minuto
   - C. Poco más de 11 minutos
   - D. Poco más de 1 h
   - E. Poco más de 11 h
   - F. Poco más de 1 día
   - G. Poco más de 11 días
   - H. Poco más de 1 meses
   - I. Poco más de 4 minutos
   - J. Poco más de 44 minutos
   - K. Poco más de 4 h
   - L. Poco más de 44 h
   - M. Poco más de 44 días
   - N. Poco más de 4 meses

2. En una comunicación codificada con una codificación de bloques hemos conseguido descifrar parte de la comunicación. Sabemos que los bloques son de 3 bits y hemos conseguido saber que el mensaje codificado 110100000010101001111011 como mensaje plano es 111010101???100000110001. ¿Qué se puede afirmar sobre las tres incógnitas?
   - **A.** Que valen 011
   - B. Que valen 000
   - C. Que valen 001
   - D. Que valen 010
   - E. Que valen 100
   - F. Que valen 101
   - G. Que valen 110
   - H. Que valen 111
   - I. Que no podemos saber su valor

3. Queremos transferir un fichero de gran tamaño (F) asegurando la privacidad del envío y su integridad (E=emisor, R=receptor). ¿Cuál de los siguientes esquemas es correcto?
   - **A.** $h(F)|K^E_{pub}(K_S)|K_S(F)$
   - B. $h(F)|K^E_{pub}(h(F))|K_S(F)$
   - C. $h(F)|K^E_{pub}(F)$
   - D. $K^E_{pub}(h(F)|F)$
   - E. $K^E_{pub}(K_S)|K_S(h(F)|F)$
   - F. $h(F)|K^E_{pub}(F)$

G. $K^E_{pub}(F)$

H. $h(F)|K^R_{priv}(h(F))|K_S(F)$

I. $h(F)|K^R_{priv}(F)$

J. $K^R_{priv}(h(F)|F)$

K. $K^R_{priv}(K_S)|K_S(h(F)|F)$

L. $h(F)|K^R_{priv}(F)$

M. $K^R_{priv}(F)$

N. $h(F)|K^R_{priv}(K_S)|K_S(F)$

4. Para enviar un email privado es necesario y suficiente:

   **A.** Codificar la clave simétrica con la clave pública del receptor y concatenarla con el mensaje codificado con la clave simétrica.

   B. Codificar el mensaje con RSA usando la clave pública del receptor

   C. Codificar el mensaje con RSA usando la clave privada del emisor

   D. Hacer el HASH del mensaje, codificarlo con la clave pública del receptor y concatenar con el mensaje.

   E. Codificar la clave simétrica con la clave privada del emisor y concatenarlo con el mensaje codificado con la clave pública del receptor.

   F. Realizar el HASH del mensaje, concatenarlo con el mensaje, cifrarlo todo con la clave simétrica y concatenar la clave simétrica codificada con la clave pública del receptor.

   G. Codificar la clave simétrica con la clave privada del emisor y concatenarla con el mensaje codificado con la clave simétrica.

   H. Codificar la clave simétrica con la clave privada del receptor y concatenarla con el mensaje codificado con la clave simétrica.

   I. Utilizar firmas digitales.

5. Imagina un cifrador en bloque en modo CBC. ¿Cuál es la entrada al bloque de cifrado de la primera etapa si el primer bloque del mensaje en claro es $m_1 = 0110b$ e $IV = 1111b$?

   A. 1000b

   B. 1010b

   **C.** 1001b

   D. No es posible determinar su valor

6. Utilizando la notación que se encuentra en la tabla, ¿cuál es la expresión que determina la firma digital de un mensaje $m$?

   A. $K^E_{pub}(h(m))$

   **B.** $K^E_{prv}(h(m))$

   C. $K^R_{prv}(h(m))$

   D. $h(m)|K^E_{prv}(m)$

7. ¿Qué garantiza la *firma digital* de un documento?

   **A.** La integridad del documento y la autenticación del emisor

   B. La integridad del documento

   C. La autenticación del emisor

   D. Ninguna de las respuestas es correcta (excepto ésta, obviamente)

8. Imagina un criptosistema RSA con claves pública y privada $\{5, 35\}$ y $\{d, 35\}$, respectivamente. ¿Cuál de los siguientes es un valor aceptable para $d$?

   **A.** 5

   B. 7

   C. 11

   D. 4

9. ¿Cuál de las siguientes afirmaciones sobre el uso de 'salt' para almacenar contraseñas es verdadera?
   - **A.** Lo que se guarda en el sistema es el hash calculado sobre la combinación de valor 'salt' y la contraseña: HASH(salt + contraseña).
   - B. El valor 'salt' se calcula en base al hash de cada contraseña.
   - C. El valor 'salt' sólo debe almacenarse hasheado, de otra forma el sistema pierde seguridad.
   - D. Si el 'salt' no es más largo de 8 caracteres, usando tablas Rainbow se puede revertir cualquier contraseña inmediatamente.

10. ¿Cuál de las siguientes afirmaciones sobre los firewalls e IDS es falsa?
   - **A.** La única diferencia entre un IDS y un firewall es que el IDS puede hacer inspección profunda de paquetes.
   - B. Un firewall sólo puede analizar el encabezado de los paquetes TCP/IP.
   - C. Es posible, y tiene sentido, colocar múltiples sensores IDS en una misma red.
   - D. Un firewall puede hacer ciertas comprobaciones de estado para filtrar los paquetes.

11. ¿Cuál de estas afirmaciones sobre los certificados digitales es verdadera?
   - **A.** El objetivo de un certificado digital es que cualquiera pueda obtener, de forma segura, la clave pública de otro usuario.
   - B. El objetivo de un certificado digital es que cualquiera pueda obtener, de forma segura, a la clave privada de la autoridad certificadora.
   - C. El objetivo de un certificado digital es que cualquiera pueda obtener, de forma segura, a la clave privada de otro usuario.
   - D. El objetivo de un certificado digital es que cualquiera pueda obtener, de forma segura, la clave pública de la autoridad certificadora.

12. ¿Cuál de estas afirmaciones sobre el protocolo SSH es falsa?
   - **A.** Se encarga de la autenticación del cliente.
   - B. Se encarga de la autenticación del servidor.
   - C. Se encarga del establecimiento de un canal cifrado para garantizar la confidencialidad de la comunicación.
   - D. Se encarga de la comprobación de la integridad de los mensajes.
   - E. Se encarga de la generación de un identificador único de sesión.