Modelo 2

Las siguientes preguntas solo tienen una respuesta correcta. Cada respuesta correcta suma 1 punto, cada incorrecta resta 1/2 y las no contestadas no puntúan. El test completo evalúa sobre 4 puntos del total del examen.

1. Imagina que s es una clave simétrica compartida entre A y B, m un mensaje cualquiera, + la operación de concatenación y H una función hash. ¿Cuáles de las siguientes construcciones formarían un esquema MAC (o HMAC) válido?

   A. H(m+s)

   B. s+H(m)

   C. m+H(s)

   D. H(m)+H(s)

2. Imagina que A quiere garantizar SOLO la autenticidad de un mensaje m. No es necesario garantizar (de hecho, no se desea) la confidencialidad, porque el mensaje es público. ¿Cuál sería el esquema más adecuado?

   A. A cifra el mensaje con la clave pública de B

   B. A genera una clave de sesión k, cifra m con k, y luego cifra k con la clave pública de B

   C. A genera un hash de m, llamado h, y cifra h con la clave privada de B

   D. A genera una clave de sesión k, cifra m con k, y luego cifra k con la clave privada de A

3. Sea $E(K, P_j)$ una función de cifrado simétrico con clave K que procesa el bloque j-ésimo del texto en claro P, C_j el criptograma correspondiente al bloque anterior y $\oplus$ la función XOR. ¿A qué modos de encadenamiento corresponden las siguientes expresiones?

	Expresión
E_1	$C_j = E(K, P_j),\ j = 1, ..., N$
E_2	$C_1 = E(K, P_1 \oplus IV)$ $C_j = E(K, P_j \oplus C_{j-1}),\ j = 2, ..., N$

   A. E_1 = CBC, E_2 = ECB

   B. E_1 = ECB, E_2 = CBC

   C. E_1 = ECB, E_2 = CTR

   D. E_1 = ECB, la segunda expresión no es correcta

4. En un algoritmo de cifrado simétrico con modo de encadenamiento ECB se produce un error en la transmisión de un bloque cifrado C_i. ¿Cuál de las siguientes afirmaciones es correcta?

   A. Solo afecta al correspondiente texto en claro P_i

   B. Afecta al correspondiente texto en claro P_i, y al siguiente, P_{i+1}

   C. Afecta al correspondiente texto en claro P_i, y a los dos siguientes, P_{i+1} y P_{i+2}

   D. Ninguna de las anteriores

5. En el mismo supuesto que la pregunta anterior, pero utilizando CBC, ¿cuál de las siguientes afirmaciones es correcta?

   A. Solo afecta al correspondiente texto en claro P_i

   B. Afecta al correspondiente texto en claro P_i, y al siguiente, P_{i+1}

   C. Afecta al correspondiente texto en claro P_i, y a los dos siguientes, P_{i+1} y P_{i+2}

   D. Ninguna de las anteriores

6. En el modo de encadenamiento CTR, el proceso de cifrado corresponde a:

   A. A cifra el mensaje con la clave pública de B

   B. A genera una clave de sesión k, cifra m con k, y luego cifra k con la clave pública de B

   C. Una simple función XOR

   D. A genera una clave de sesión k, cifra m con k, y luego cifra k con la clave privada de A

7. En el certificado digital de un usuario, ¿qué elemento cifra la CA correspondiente?

   A. Sólo la clave pública del usuario

B. La clave privada del usuario, junto con su identidad

C. La clave pública del usuario, junto con su identidad

D. Sólo su identidad

8. Para realizar una firma digital, ¿cuáles de los siguientes algoritmos podrías utilizar?

   A. AES y RSA

   B. HMAC y RSA

   C. AES y una función hash

   D. Una función hash y RSA

9. En un sistema RSA, interceptas el texto cifrado $C = 10$ enviado a un usuario cuya clave pública es $e = 5$, $n = 35$. ¿Cuál es el mensaje original?

   A. 5

   B. 7

   C. 3

   D. 21

10. Las tablas Rainbow sirven para montar ataques de tipo...

    A. online

    B. offline

    C. los dos anteriores

    D. diccionario

11. Los esquemas de autenticación de doble factor se basan en...

    A. Algo que sabemos y somos

    B. Algo que tenemos y somos

    C. Algo que sabemos y tenemos

    D. Ninguna de las anteriores

12. Imagina un cortafuegos que protege una red corporativa, llamada `lan`, de Internet, `inet`, y que debe implementar la siguiente política: *No aceptar conexiones entrantes al servidor de correo.* ¿Cuál sería la regla que la implementase?

    `Action | Src. Address | Dst. Address | Protocol | Src. port | Dst. port | Flag bit`

    A. `deny | inet | lan | any | 110 | SYN`

    B. `deny | lan | inet | any | 25 | SYN`

    C. `deny | inet | lan | any | 25 | SYN`

    D. Ninguna de las anteriores