Responde detallada y razonadamente a las siguientes preguntas. Las respuestas no razonadas no serán consideradas como válidas, aunque sean correctas. Recuadra CLARAMENTE tu respuesta a cada apartado. Consigna tu NIA, nombre y apellidos completos en todas las hojas que entregues.

1. Imagina que dispones de un cifrador simétrico, que opera sobre bloques de 4 bits del texto de entrada, y cuya definición es la siguiente: 3

   - $c_3 = 1 \oplus b_3 \,\&\, k_3$
   - $c_2 = b_1 \,\&\, k_2$
   - $c_1 = b_2 \,\&\, k_1$
   - $c_0 = 0 \oplus b_0 \,\&\, k_0$

   donde c_i, b_i y k_i son los bits i-ésimo del bloque cifrado, de entrada y clave de cifrado, respectivamente (b_0 y c_0 son los bits menos significativos de cada bloque). El texto de entrada empieza a procesarse por los bits más significativos. Si es necesario, utiliza un valor $IV = 7h$.

   A. (**1,5 ptos.**) ¿Cuál es el criptograma correspondiente al texto de entrada $b = A93h$, utilizando $k = Bh$ y modo de encadenamiento ECB?

   B. (**1,5 ptos.**) ¿Y para el mismo texto de entrada y clave de cifrado, y modo de encadenamiento CBC?

   Solución:

   A. Como se indica, comenzaremos procesando la entrada desde los bits más significativos, por lo que el primer *nibble* (bloque de 4 bits), que denotaremos b^0, será $Ah = 1010b$. También tenemos $k = Bh = 1011b$. Así, obtendría:

      - $c_3 = 1 \oplus b_3 \,\&\, k_3 = 1 \oplus 1 \,\&\, 1 = 0$
      - $c_2 = b_1 \,\&\, k_2 = 1 \,\&\, 0 = 0$
      - $c_1 = b_2 \,\&\, k_1 = 0 \,\&\, 1 = 0$
      - $c_0 = 0 \oplus b_0 \,\&\, k_0 = 0 \oplus 0 \,\&\, 0 = 0$

      Por el mismo procedimiento, se obtendrían los valores para $c^1 = 0001b$ y $c^2 = 1001b$. Puesto que el modo de encadenamiento es ECB, simplemente debemos concatenar la salida de cada bloque, quedando finalmente $c = 0000\,0001\,1001 = 019h$.

   B. En este caso, el modo de encadenamiento es CBC que, como sabemos, *mezcla* los bloques de entrada, para evitar el ataque semántico, del que adolece ECB. Para ello, comenzamos con el primer bloque:

      1. que se mezcla, con una operación XOR, con el IV, obteniendo un bloque intermedio $B^0 = b^0 \oplus IV = 1010 \oplus 0111 = 1101$. Este bloque pasa ahora por la función de cifrado, obteniendo $c^0 = 0011 = 3h$.
      2. Para el segundo bloque, ésta salida se mezclará de nuevo con el siguiente bloque, $B^1 = c^0 \oplus b^1$. Procediendo de la misma forma para el resto de bloques, obtenemos finalmente que el criptograma resultante es $c = 0011\,0000\,1001 = 309h$.

   NOTA: Más que en ningún otro ejercicio, en éste es especialmente importante explicar con detalle qué se está haciendo en cada momento, de forma que se si comete un error en los cálculos, puedan evaluarse otros aspectos.

2. Responde a las siguientes preguntas 3

   A. (**1 pto.**) Describe con el mayor detalle posible el esquema de firma digital, tanto desde el punto de vista el emisor como del receptor. Incluye, al menos, un diagrama claro y detalla el proceso.

B. (**2 ptos.**) Imagina ahora que dispones de una función *hash* definida como $H(x) = (3x + 2)$ mód 7, y un par clave pública/privada {7,77} y {43,77}, respectivamente. ¿Cuál sería la firma del texto de entrada '56'? ¿Cómo verificaría el receptor la misma?

Solución:

A. Explicado en teoría. Para considerarse una respuesta perfecta, deben tratarse, al menos, de forma clara y precisa los siguientes conceptos:

- ¿Qué es una firma digital?
- ¿Para qué sirve?
- ¿Por qué se utiliza un hash en lugar de cifrar todo el texto de entrada completo?
- Cuál es el proceso detallado, tanto desde el punto de vista del emisor como del receptor
- ¿Qué se consigue con una firma digital?

B. Una firma digital se compone, esencialmente, del cifrado con la clave privada del emisor de un hash del texto de entrada. Para ello, procederemos de la siguiente forma:

1. Calcular el hash del mensaje, $H(56) = 3 \cdot 56 + 2 \mod 7 = 2$.
2. Ahora ciframos con la clave privada del emisor ($\{d = 43, n = 77\}$)el valor anterior, de forma que la firma S quedaría $S = 2^{43} \; mod 77 = 30$. Este valor se concatenaría con el mensaje en claro antes de enviarse al receptor.

Una vez recibido, el receptor (verificador) procedería de la siguiente forma:

1. Recalcularía el hash del mensaje. Suponemos, en este caso, que no ha habido modificación, voluntaria o involutaria (error), en la transmisión del mismo.
2. Descifraría la firma recibida. Para ello, utilizaría el exponente público del emisor, obteniendo $S' = 30^7 \mod 77 = 2$. Como $S = S'$, podemos concluir que, efectivamente, la firma es válida. Así, sabríamos que a) el emisor del mensaje es el adecuado, y b) el mensaje es íntegro y no ha sido modificado en tránsito.