1. Imagina un cifrador simétrico de bloques, $E_k(m)$, con clave k que opera sobre un mensaje m. Para ello, el cifrador trocea el mensaje en bloques de 4 bits que procesa de acuerdo al modo de encadenamiento específico que utilice en cada momento. La operación de cifrado sobre cada bloque es $E_k(b_i) = k \oplus b_i$, donde b_i es el bloque i-ésimo. Por otro lado, dispones de una función hash, $h(x) = \overline{x}$, donde $\overline{x}$ indica el operador de negación o NOT. Si lo necesitas, considera como IV el valor $07h$. [3]

   Contesta a las siguientes cuestiones de forma **razonada**. Aunque sean correctas, no se considerarán válidas respuestas no explicadas claramente. Incluye la respuesta final en el recuadro, y el desarrollo para obtenerla en el espacio en blanco.

   A. (**1 pto.**) Utilizando un modo de encadenamiento ECB, ¿cuál sería el criptograma correspondiente al texto de entrada $m = ABh$, con una clave $k = 0Ch$?. Si necesitas hacer uso de *padding* en algún momento, rellena con ceros por la izquierda con los bits que sean necesarios.

   67h

   Solución: El modo de encadenamiento ECB es el más sencillo, pues no retroalimenta los bloques entre sí, sino que los procesa en paralelo. De esta forma, tendríamos que:
   - $E_k(b_0) = k \oplus b_0 = Ch \oplus Ah = 6h$
   - $E_k(b_1) = k \oplus b_1 = Ch \oplus Bh = 7h$

   El criptograma final es simplemente la concatenación de cada bloque, $E_k(m) = 67h$.

Continúa en la siguiente página

   B. (**1,5 ptos.**) Con el mismo valor de m y k, ¿cuál sería el criptograma correspondiente utilizando un modo de encadenamiento CBC?

   16h

   Solución:

   En este caso, el modo de encadenamiento CBC sí mezcla la salida de cada etapa con la entrada de la siguiente, para evitar los problemas que sufre ECB con regiones de datos muy similares (mismo bloque de entrada produce siempre el mismo bloque de salida). En este caso, tendríamos que:
   - $E_k(b_0) = (IV \oplus b_0) \oplus k = (7h \oplus Ah) \oplus C = 1h$
   - $E_k(b_1) = (E_k(b_0) \oplus b_1)k = (1h \oplus B) \oplus Ch = 6h$

   Por tanto, en este caso el criptograma final quedaría, $E_k(m) = 16h$.

   Solución:

   C. (**0,5 ptos.**) Ante un error de transmisión, ¿qué modo de encadenamiento se comporta mejor (propaga el error en menos bloques)? ¿Por qué?

   Solución:

   Solución:

   Claramente, el modo ECB limita el error al bloque en el que se produce, pues no hay retroalimentación entre bloques. Sin embargo, en CBC el error se propaga desde el bloque en el que se produce, hasta el final del mensaje.

2. Utilizando el algoritmo RSA, con p=3, q=11 y e=9, cifre la palabra "Eloy", considerando que la 'a' se codifica como 1, la 'b' como 2, y así sucesivamente (sin considerar la letra ñ), y que no se distinguen mayúsculas de minúsculas. [3]

A. (**1,5 ptos.**) Carácter por carácter, en caso de ser posible. Si no posible explique por qué.

Solución: Si p=3, q=11, entonces n = 33, z = 20. Si e=9, 9*d mod 20 = 1, luego $d = \frac{k*20+1}{9}$ Con $k = 4$, $e = 9$ luego $K^+ = K^- = (33, 9)$ Entonces para cifrar cada carácter c sería: $codif(c)^9 mod 33$ codif('E') = 5; codif('L') = 12; ...

B. (**1,5 ptos.**) La palabra completa como un mensaje m, en caso de ser posible. Si no es posible explique por qué.

Solución: Si el mensaje a transmitir es m = 512xxx, como $m > n$, no se puede cifrar con el esquema dado.