Nombre: _____ Apellidos: _____ NIA: _____

| Preguntas | blue1Item.1 | blue2Item.8 | blue3Item.15 | Total |
|---|---|---|---|---|
| Puntos | 3 | 3 | 0 | 6 |
| Puntuación | | | | |

1. Imagina un criptosistema simétrico de bloques, $E_k(m)$, con clave $k$ que opera sobre un mensaje $m$, consistente en tu NIA. Para ello, el cifrador trocea el mensaje en bloques de 8 bits que procesa de acuerdo a cada modo de encadenamiento específico. La operación de cifrado sobre cada bloque es $E_k(b_i) = k \oplus b_i$, donde $b_i$ es el bloque i-ésimo. Responde a las siguientes preguntas: [3]
    1. Utilizando un modo de encadenamiento ECB, ¿cuál sería el criptograma correspondiente al texto de entrada de tu ID con clave k=0xA?. Si lo necesitas, considera como IV el valor 0xC. Si tu cadena necesita padding, el bloque correspondiente se rellena con '0' hasta donde sea necesario.
    2. Utilizando un modo de encadenamiento CBC, ¿cuál sería el criptograma correspondiente al texto de entrada de tu ID con clave k=0xA?. Si lo necesitas, considera como IV el valor 0xC.
    3. Ante un error de transmisión, ¿qué modo de encadenamiento se comporta mejor (propaga el error en menos bloques)? ¿Por qué?

| | | Texto en claro | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Clave de cifrado | | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| | 0 | 9 | 1 | 3 | 5 | 4 | 2 | 0 | 5 | 8 | 5 |
| | 1 | 9 | 7 | 9 | 9 | 8 | 8 | 1 | 8 | 0 | 8 |
| | 2 | 4 | 0 | 1 | 1 | 7 | 2 | 4 | 6 | 0 | 2 |
| | 3 | 5 | 3 | 5 | 5 | 3 | 7 | 7 | 9 | 3 | 0 |
| | 4 | 4 | 5 | 8 | 2 | 3 | 1 | 0 | 0 | 0 | 1 |
| | 5 | 6 | 5 | 1 | 0 | 8 | 0 | 6 | 1 | 0 | 6 |
| | 6 | 8 | 1 | 1 | 6 | 7 | 0 | 3 | 8 | 1 | 7 |
| | 7 | 9 | 1 | 7 | 4 | 0 | 8 | 2 | 3 | 6 | 5 |
| | 8 | 0 | 4 | 9 | 6 | 5 | 7 | 2 | 1 | 5 | 6 |
| | 9 | 0 | 0 | 5 | 7 | 9 | 8 | 2 | 4 | 5 | 3 |

Nombre: _____ Apellidos: _____ NIA: _____

2. Imagina que cuentas con los siguientes elementos, que puedes utilizar o no de acuerdo a tu criterio: 3

   - Función de cifrado simétrico por bloques, $E_k(m)$, donde $m$ es el texto en claro y $k$ la clave secreta, definida en la tabla inferior, y que funciona en modo ECB. Para utilizarlo, considera cada dígito del texto en claro un bloque. Así, si el texto en claro es el número '123' y la clave '4', el criptograma correspondiente sería $E_4(1)$, $E_4(2)$, $E_4(3)$ = '582'.
   - Función hash $H(m) = (2m + 7) \mod 11$. La función hash opera sobre todo el mensaje a la vez.
   - Clave pública y privada de Alicia, $K_{pub}A = \{23, 77\}$, $K_{priv}A = \{47, 77\}$.
   - Clave pública y privada de Bernardo, $K_{pub}B = \{5, 65\}$, $K_{priv}B = \{29, 65\}$.
   - Clave simétrica de sesión: 7

   En esta situación, imagina que Alicia desear comunicar su ID de forma segura a Bernardo. Para ello crea un mensaje M, compuesto exclusivamente por su número ID, al que deberá aportar confidencialidad, integridad y autenticación. Considera el mensaje como un número (tu NIA), y no como una cadena o representación ASCII de la misma. Además, considera que, aunque en este caso el mensaje sea muy, éste podría ser de longitud arbitrariamente grande, y utiliza el esquema criptográfico más adecuado para ese caso.

   En este escenario, responde a las siguientes preguntas:

   1. ¿Cuál sería el valor de la firma digital del mensaje M? Solo la firma, sin incluir el propio mensaje. Para los pasos siguientes, la firma del mensaje que obtengas aquí se concatena al final del mismo.
   2. ¿Cuál sería el valor del mensaje firmado y cifrado? De entre los elementos proporcionados en el enunciado, utiliza los que consideres necesarios.
   3. Finalmente, ¿cuál sería el valor del sobre digital para el mensaje? Solo el del sobre, sin incluir el propio mensaje.

3. Has interceptado un mensaje **m** = '333456' enviado por Alicia a Bernardo, del que sabes que ha sido cifrado símbolo a símbolo con RSA. Dispones, asimismo, de la clave pública de Bernardo, $K_{pub}B = \{e = 29, n = 91\}$.

   ¿Podrías criptoanalizar el mensaje y obtener el correspondiente texto en claro?