1. Imagina que Alicia quiere cifrar un mensaje m, para posteriormente enviarlo a Bernardo. Para ello, Alicia dispone de un cifrador simétrico $E_k(m)$ que trabaja sobre bloques de 4 bits, con la estructura de la figura. En ella, $\oplus$ representa la operación XOR, m_i el bit i-ésimo de la representación ASCII del mensaje, k_i el bit i-ésimo de la clave simétrica (también de 4 bits de longitud total) y c_i el bit i-ésimo del criptograma resultante. [4]

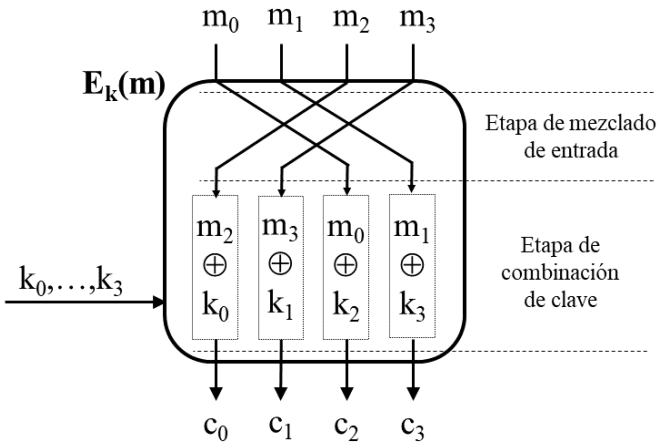

Figura 1: Algoritmo de cifrado simétrico, $E_k(m)$

Con estos elementos, responde a las siguientes cuestiones:

1. ¿Cuál sería el valor hexadecimal del criptograma resultante de cifrar con $E_k(m)$ el mensaje m='HO' con modo de encadenamiento ECB y clave k=0xC? Ten en cuenta que el código ASCII de la letra 'H' es 0x48 y el de 'O', 0x4F. **Solución**: 0xDED3

Solución:
Este modo de encadenamiento procesa los bloque de forma paralela, sin encadenamiento entre ellos. Por tanto, solo hay que trocear la entrada en bloques de 4 bits, y procesarlos a través del cifrador:

0x4	0x8	0x4	0xF	
0100	1000	0100	1111	
0001	0010	0001	1111	- Tras etapa de mezclado
1101	1110	1101	0011	- Tras etapa de combinación de clave
D	E	D	3	= 0xDED3

2. ¿Y el criptograma para el mismo mensaje y clave con modo CBC y vector de inicialización IV = 0xA? **Solución**: 0x7317

Solución:
Este modo de encadenamiento procesa los bloque encadenando las salidas previas con las entradas salvo para el primer bloque para el que se utiliza el vector de inicialización. Por tanto, solo hay que trocear la entrada en bloques de 4 bits, y procesarlos a través del cifrador:

0x4	0x8	0x4	0xF	
0100	1000	0100	1111	
1010	0111	0011	0001	De la etapa anterior (IV en el primer caso)
1110	1111	0111	1110	XOR con etapa anterior
1011	1111	1101	1011	- Tras etapa de mezclado
0111	0011	0001	0111	- Tras etapa de combinación de clave
7	3	1	7	= 0x7317

Alicia debe enviar ahora el mensaje cifrado anterior a Bernardo. Para ello dispone de una implementación del algoritmo RSA, junto con la clave pública de Bernardo, $K_{pub} = \{19, 119\}$, que ha obtenido

previamente. Aunque por brevedad se ha pedido cifrar solo dos caracteres del mensaje, éste es, en realidad, de varios gigabytes de longitud.

3. Explica de forma detallada y concisa cómo debería proceder Alicia para enviar el mensaje del apartado 2 a Bernardo. Como suponemos habitualmente, el medio de transmisión es hostil, y los atacantes puede interceptar y modificar los mensajes enviados.

   Solución:
   Aunque en el apartado 2 se nos ha pedido codificar dos caracteres en realidad el mensaje es de varios gigabytes de longitud y, dados los elementos de los que disponemos, el mensaje debe ser de la forma $IV|K_{pub}(k)|E_k(m)$

4. ¿Cuál sería un formato posible del mensaje final que debería enviar Alicia? (Explica el formato que has realizado)
   Solución: 0xA607317

   Solución:
   Tenemos todos los datos para enviar el formato y sólo queda calcular $K_{pub}(k)$. Como k = 0xC = 12, entonces $K_{pub}(k) = 12^{19}$ mód 119.
   Como 12^{19} mód 119 = (12^{16} mód 119 · 12^2 mód 119 · 12^2 mód 119) mód 119
   Por otro lado:
   12^2 mód 119 = 25 mód 119 = 25
   $(12^2)^2$ mód 119 = 25^2 mód 119 = 30 mód 119 = 30
   $(12^4)^2$ mód 119 = 30^2 mód 119 = 67 mód 119 = 67
   $(12^8)^2$ mód 119 = 67^2 mód 119 = 67 mód 119 = 86

   Entonces 12^{19} mód 119 = $(86 \cdot 25 \cdot 12)$ mód 119 = 96 = $0x60$

2. El concepto central de los esquemas de autenticación es el de *firma digital*. Responde razonadamente a las siguientes cuestiones: 2

   - Describe con un esquema, y unas breves explicaciones, cómo un emisor A generaría la firma de un mensaje m, y cómo un receptor B la verificaría.

     Solución:

     [Esquema de firma digital de teoría]
     La firma digital no es más que el cifrado con la clave privada del emisor del hash de un mensaje, $K^A_{priv}(h(m))$. Finalmente, dicho emisor enviaría el mensaje m en claro, junto con esta firma, quedando: $m|K_{priv}(h(m))$. El receptor, al recibir este criptograma, procede de la siguiente forma:
     1. Calcula de nuevo el hash del mensaje recibido, $h(m) = H'$.
     2. Deshace el cifrado del hash del emisor con la clave pública de A, obteniendo $H = h(m)$.
     3. Si H' y H son idénticos, el receptor puede estar seguro de que A generó la firma (puesto que sólo A tiene acceso a su clave privada), y de que el mensaje no ha sido modificado (puesto que los hashes son iguales).

   - ¿Cuáles de las propiedades básicas que garantizan la seguridad de un mensaje (confidencialidad, autenticación e integridad), proporciona una firma digital?
     Solución: Autenticación e integridad
   - Cuando se desea firmar y cifrar simultáneamente un mensaje, ¿qué operación debe hacerse primero? ¿Por qué?

     Solución:
     En este caso, *siempre se debe firmar primero*. La razón es sencilla: si firmamos un texto ya cifrado, no podemos ver lo que estamos firmando, y podríamos ser fácilmente engañados.