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?

    Solución:

    Imaginemos que el NIA del estudiante es '123456'. Como el enunciado indica que el tamaño de bloque es 8 bits, es más cómodo convertir el número a binario ('11110001—00100000—0') y trabajar directamente así. Vemos que la longitud de su representación binaria no es múltiplo de 8, por lo que necesitaremos padding en el último bloque.

    En todo esquema criptográfico de cifrado por bloques, el padding se incluye a la derecha, puesto que el fichero se procesa bloque a bloque por el principio. En este caso, es necesario incluir 7 bits de padding (que simplemente se desecharían en el descifrado), por lo que el último bloque queda '0**0000000**'.

    En este punto:

    1. El modo ECB simplemente procesa los bloques de uno en uno, sin encadenamiento:

    $$E_k(b_0) = 00001010 \oplus 11110001 = 11111001 = FBh$$
    $$E_k(b_1) = 00001010 \oplus 00100000 = 00101000 = 2Ah$$
    $$E_k(b_2) = 00001010 \oplus 00000000 = 00001000 = 0Ah$$

    Por tanto, el criptograma final es: $E_k(m) = FB2A0Ah$
    2. El modo CBC sí añade realimentación al sistema, para evitar los problemas clásicos del modo ECB. En este caso, cada bloque se encadena con el posterior: $E_k(b_i) = (E_k(b_{i-1}) \oplus b_i) \oplus k$. Para el bloque b_0 se utiliza el IV. Por tanto, quedaría:

    $$E_k(b_0) = (IV \oplus b_0) \oplus k = (00001100 \oplus 11110001) \oplus 00001010 = F7h$$
    $$E_k(b_1) = (E_k(b_0) \oplus b_1) \oplus k = (11110111 \oplus 00100000) \oplus 00001010 = 11011101 = DDh$$
    $$E_k(b_2) = (E_k(b_1) \oplus b_2) \oplus k = (11011101 \oplus 00000000) \oplus 00001010 = 11010111 = D7h$$

    Por tanto, el criptograma final es: $E_k(m) = F7DDD7h$
    3. El modo más resistente a los fallos de transmisión es ECB, que no propaga el error más allá de su bloque. CBC lo sufre en el bloque del error y en el siguiente.

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, $K_{pub}A = \{23, 77\}$, $K_{priv}A = \{47, 77\}$.

	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

- 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.

Solución:

Puesto que se nos dice que el mensaje puede ser arbitrariamente grande, y que se debe proveer confidencialidad, autenticación e integridad, el esquema más adecuado en este caso es uno híbrido, que combina lo mejor de los esquemas simétricos y asimétricos.

Supondremos que el ID es '123456', utilizaremos RSA como criptosistema asimétrico, y denotaremos como $E_{pubA}(m)$ el cifrado con la clave pública de A sobre un mensaje m. De esta forma:

1. La firma digital de A sobre un mensaje m es: $S(m) = E_{privA}(H(m))$. Solo hay que calcular los valores adecuados:
   - $H(m) = (2m + 7) \mod 11 = (2 \cdot 123456 + 7) \mod 11 = 2$
   - El valor de la firma queda entonces $S(m) = m^d \mod n$, donde n es el módulo del par de claves del firmante: $S(m) = 2^{47} \mod 77 = 18$.
   - Se nos dice que la firma se concatena al final, por lo que el mensaje firmado quedaría 12345618.
2. Ahora es necesario cifrar el mensaje. Para ello se utiliza una clave simétrica de sesión, que se desecha tras el descifrado. La clave que se proporciona es $ks = 7$. Realizando el cifrado en la tabla (buscando el texto en claro en columnas y el valor de la clave en filas), obtenemos que el criptograma para el mensaje firmado anterior es $E_{ks}(m) = 43536515$.
3. Solo queda ya calcular el valor del sobre digital, que no es más que la protección (cifrado) de esta clave de sesión con la clave pública del destinatario, de forma que solo él pueda descifrarla:

$$E_{pubB}(7) = 7^5 \mod 65 = 37$$

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?

Solución:

Con un módulo tan reducido, el ataque más sencillo es, simplemente, factorizarlo. Enseguida se observa que $91 = 7 \cdot 13$, por lo que $p = 7$ y $q = 13$. A partir de aquí, solo resta reproducir los pasos necesarios para generar las claves RSA:

1. Calculamos $\phi(n) = (p-1)(q-1) = 6 \cdot 12 = 72$
2. Conocemos el exponente público, e, luego solo nos resta encontrar uno privado adecuado, de forma que $ed \equiv 1 \mod \phi(n) = 29d \equiv 1 \mod 72$. Como sabemos, hay diversas formas de encontrar el inverso multiplicativo de **e**, que se resumen muy bien aquí [1], pero con número tan pequeños la prueba y error suele ser lo más sencillo. Para ello, simplemente reescribimos la expresión anterior como:

   $$ed \equiv 1 \mod \phi(n) \rightarrow ed = 1 + k\phi(n) \rightarrow d = \frac{1 + k\phi(n)}{d}$$

   para algún k, que hace d entero.
   Rápidamente, para k = 2, obtenemos d = 5.
3. En este punto, ya podemos descifrar el mensaje. Así, para el primer símbolo del texto en claro, c_1:

   $$c_1 = (m_1)^d \mod n = 3^5 \mod 91 = 61$$

   El resto del mensaje se recupera de la misma forma.