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. **PROBLEMA 1** 3

Imagina que recibes el siguiente mensaje, cifrado con un esquema híbrido estándar, 5174215—42, donde el símbolo '—' separa dos elementos importantes del esquema.

A continuación, recrea con el máximo detalle posible todo el proceso de descifrado y verificación del mensaje, recuadrando CLARAMENTE los resultados intermedios y finales. Para ello dispones de:

- Un cifrador simétrico, cuya función de descifrado $D(x,k)$ (p. ej.: $D(4,3)=6$) se define en la tabla inferior para una clave $k=3$. Esta función opera dígito a dígito sobre el criptograma (es decir, $D(abcd) = D(a)\|D(b)\|D(c)\|D(d)$), donde $\|$ indica concatenación).
- Una función hash $H(x) = (2x+5) \mod 9$. La firma de un mensaje ocupa tres dígitos decimales (p. ej.: 23 se codificaría como 023, o 7 como 007), y se añade al final del mismo.
- Tu par de clave público/privada es {7,143} y {103,143}, respectivamente. La clave pública del emisor es {29, 221}.

Función $D(x,3)=y$

| x | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|---|---|
| y | 4 | 3 | 0 | 5 | 6 | 2 | 7 | 1 | 9 | 8 |

Si lo consideras necesario, puedes utilizar las siguientes expresiones:

- $(42^{50}) \mod 143 = 100$
- $(42^{3}) \mod 143 = 14$
- $(14 \cdot 10^{4}) \mod 143 = 3$
- $(32^{20}) \mod 221 = 16$
- $(32^{9}) \mod 221 = 83$

**Solución:**

Puesto que el mensaje ha sido cifrado con un esquema híbrido, el mismo estará compuesto por un sobre digital (42). El proceso completo quedaría:

1. Comenzaremos *'deshaciendo'* el sobre, descifrándolo con la clave privada del receptor. De esta forma, obtendremos la clave de sesión $k_s$:

$$k_s = 42^{103} \mod 143 = 42^{50} \cdot 42^{50} \cdot 42^{3} \mod 143 = 100 \cdot 100 \cdot 3 \mod 143 = 3$$

2. Ahora, utilizamos $k_s$ para descifrar el resto del mensaje. Para ello utilizamos la tabla que se proporciona, obteniendo $D(5174215) = 2316032$. Se nos dice que la firma ocupa tres dígitos decimales, por lo que el mensaje original es $m = 2316$ y la firma $s = 032$.
3. Para verificarla, recalculamos primero H(m), obteniendo:

$$h = H(2316) = 2 \cdot 2316 + 5 \mod 9 = 2$$

Ahora desciframos el valor de $s$ con la clave pública del emisor, de forma que:

$$h' = 32^{29} \mod 221 = 32^{20} \cdot 32^{9} \mod 221 = 16 \cdot 83 \mod 221 = 2$$

Puesto que $h = h'$, podemos considerar verificada la firma, y estar seguros de que el mensaje es íntegro y auténtico. Finalmente, el mensaje descifrado es $m = 2316$.

2. **PROBLEMA 2** 3

Responde razonadamente, y con el mayor detalle posible, a las siguientes preguntas:

1. **(1,5 ptos)** ¿Qué es un certificado digital? ¿Cuáles son los principales campos que contiene? ¿Cómo se genera?
2. **(1,5 ptos)** ¿Cuáles son los elementos que componen una PKI estándar? ¿Cuál es la función de cada uno de ellos? Haz un diagrama claro que represente todos estos conceptos.

**Solución:** Teoría