Las respuestas no razonadas, o no que utilicen estrictamente la notación indicada, 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** $\boxed{4}$

Imagina que un usuario A desea comunicarse de forma segura con otro usuario B, enviando un mensaje m y garantizando todas las propiedades necesarias del mismo.

Para ello, A cuenta con los siguientes elementos:

- Un cifrador simétrico $E_k(x) = x^k \oplus 245$, que utiliza una clave secreta k. El símbolo $\oplus$ representa la función XOR.
- Una operación de descifrado simétrico, $D_k(x) = (x \oplus 245)^{-k}$.
- Una función hash $h(x) = 5x + 1 \mod 9$.
- A y B disponen de un par de claves pública y privada cada uno, $K^A_{pub} = \{29, 35\}$, $K^A_{priv} = \{5, 35\}$ y $K^B_{pub} = \{7, 91\}$, $K^B_{priv} = \{31, 91\}$, respectivamente. Si es necesario, A utilizaría una clave de sesión $ks_A = 3h$.

Para concatenar elementos, utiliza el símbolo '|'. Responde a las siguientes cuestiones:

1. ¿Cuál sería el valor de la firma digital de un mensaje $m = 37$ que A envía a B?
   Solución: $\boxed{6}$

   Solución:

   Para calcular esta firma, basta con cifrar con la clave privada del emisor el hash del mensaje. Para ello:

   $$h(m) = h(37) = 5 \cdot 37 + 1 \mod 9 = 6$$

   Ahora ciframos dicho valor, para obtener la firma S:

   $$S = 6^5 \mod 35 = 6$$

2. ¿Y el valor del criptograma final para un mensaje $m = 17$ que A envie a B?. El esquema utilizado debe garantizar la confidencialidad, integridad y autenticación del mensaje.
   Solución: $\boxed{5000211149 \mid 3}$

   Solución:

   En este caso, es necesario utilizar el esquema híbrido, que combina de forma segura primitivas simétricas para la confidencialidad y asimétricas para la autenticación e integridad. Primero calcularemos la firma del mensaje:

   $$h = h(17) = ((5 \cdot 17 + 1) \mod 9) = 5$$
   $$S = 5^5 \mod 35 = 10$$

   Ahora, concatenamos la firma al mensaje original (obteniendo 17 | 7) y ciframos el conjunto con el cifrador simétrico y la clave de sesión:

   $$E(177) = 1710^3 \oplus 245 = 5000211000 \oplus 245 = 12A092A38h \oplus f5h = 12A092ACDh = 5000211149$$

   Solo falta cifrar la clave de sesión con la clave pública del destinatario, para formar el sobre digital, SD:

$$SD = 3^7 \mod 91 = 3$$

El resultado final es, por tanto, 5000211149 | 3.

3. Por último, imagina que A recibe de B un mensaje $m_B = 341123632 \mid 20$, cifrado y firmado. En este mensaje, la firma del mismo ocupa dos cifras decimales. ¿Cuál sería el valor del mensaje en claro? ¿Se verifica su firma?

   Mensaje en claro: $\boxed{\text{-}}$ **¿Se verifica la firma?**: $\boxed{\text{No}}$

   Solución:
   En este caso, sólo hay que deshacer las operaciones hechas por B. Para ello, comenzamos deshaciendo el sobre digital ('20'), para obtener la clave de sesión utilizada:

   $$ks_B = 20^7 \mod 91 = 6$$

   Una vez recuperada, ya podemos descifrar el mensaje original:

   $$D(177) = (341123632 \oplus 245)^{-20} = \frac{341123632 \oplus 245}{10^{20}}$$

   Esta expresión, claramente, no va producir un número entero, sino un número fraccionario muy cercano a cero. Por tanto, como toda la aritmética RSA es entera, claramente la firma del mensaje no se va verificar.
   En cualquier caso, algunas calculadoras pueden resolver la expresión a 0 por falta de precisión. Incluso en ese caso, tendríamos que $m = 0$ y la firma del mismo $S = 0$ también.
   El hash del mismo sería: $h(0) = 1$ que es distinto de S, luego, de nuevo, concluimos que la firma no se verifica.

2. **PROBLEMA 2** $\boxed{2}$

   El algoritmo de Diffie-Hellman (DH) permite a dos entidades Alicia y Bernardo generar una clave simétrica compartida, incluso ante la presencia de un atacante que tenga acceso a todos los mensajes intercambiados. Para ello hace uso de dos números primos p, y g, con $g < p$, que se hacen públicos. Luego, tanto A como B eligen independientemente dos secretos aleatorios, S_A y S_B, respectivamente. A partir de aquí:

   1. Alicia calcula su clave pública T_A, elevando g a S_A módulo p. Bernardo, hace lo mismo con S_B, obteniendo T_B.
   2. Alicia y Bernardo intercambian ahora sus claves públicas por Internet.
   3. Alicia calcula entonces su clave simétrica S elevando T_B a S_A módulo p. Bernardo, por su parte, y de forma independiente, calcula otra clave simétrica S' con las mismas operaciones, es decir, elevando T_A a S_B módulo p.

      A. Demuestra que, en general, Alicia y Bernardo obtienen la misma clave simétrica, es decir, que $S = S'$

      Solución:
      $S = (T_B^{S_A}) \mod p = ((g^{S_B} \mod p)^{S_A}\, modp = (g^{S_B \times S_A}) \mod p = (g^{S_A} \mod p)^{S_B} \mod p = (T_A^{S_B}) \mod p = S'$

      B. Con $p = 23$ y $g = 5$, supón que Alicia y Bernardo eligen como secretos $S_A = 4$ y $S_B = 3$, respectivamente. Calcula entonces las claves públicas T_A y T_B.

      Solución:
      Solo hay que operar:
      $T_A = g^{S_A} \mod p = (5^4 \mod 23) = 4$
      Por otro lado:

$T_B = g^{S_B} \mod p = (5^3 \mod 23) = 10$

C. De acuerdo al resultado del apartado anterior, calcula ahora la clave simétrica compartida S.

Solución:
Sabemos que, tal y como hemos demostrado anteriormente, S = S' y, por tanto, cualquiera de las dos partes pueden calcular S. Por ejemplo, para Alice:
$S = {T_B}^{S_A} \mod p = (10^4 \mod 23) = 18$
Comprobamos que, efectivamente, Bob obtiene el mismo valor:
$S' = {T_A}^{S_B} \mod p = (4^3 \mod 23) = 18$