1. Imagina que Alice desea enviar un correo, M, a Bob. Bob dispone de un par de clave pública y privada, (K_B^+, K_B^-), y Alice del certificado de Bob. Sin embargo, Alice no tiene ningún par de clave pública/privada. Alice y Bob, y el resto del mundo, comparten una misma función hash, $H(x)$, y un algoritmo de cifrado simétrico, $E(clave, mensaje)$, que pueden utilizar, si es necesario. En este escenario, sin modificarlo o añadir nuevos elementos, 1

   A. ¿Es posible diseñar un esquema de proporcione autenticación al mensaje? Si la respuesta es afirmativa, utilizando la nomenclatura anterior, indica cómo.

   Solución:
   No, sin un par de claves pública/privada, o un secreto compartido, Bob no puede verificar que Alice creó el mensaje de ninguna forma.

   B. ¿Es posible diseñar un esquema de proporcione confidencialidad al mensaje de Alice? Si la respuesta es afirmativa, utilizando la nomenclatura anterior, indica cómo.

   Solución:
   Sí, basta que Alice cifre el mensaje con la clave pública de Bob, $C = E\{K_B^+, M\}$

2. El algoritmo de Diffie-Hellman (DH) permite a dos entidades 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 primos p, y g, con $g < p$, que se hacen públicos. Luego, tanto Alice como Bob eligen independientemente dos secretos aleatorios, S_A y S_B, respectivamente. A partir de aquí: 2

   1. Alice calcula su clave pública T_A, elevando g a S_A módulo p. Bob, hace lo mismo con S_B, obteniendo T_B.
   2. Alice y Bob intercambian ahora sus claves públicas por Internet.
   3. Alice calcula entonces su clave simétrica S elevando T_B a S_A módulo p. Bob, 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, Alice y Bob 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 $p = 11$ y $g = 2$, supón que Alice y Bob como secretos $S_A = 5$ y $S_B = 12$, respectivamente. Calcula entonces las claves públicas de Alice y Bob, T_A y T_B.

   Solución: Solo hay que operar:
   $T_A = g^{S_A} \mod p = (2^5 \mod 11) = 10$
   Por otro lado:
   $T_B = g^{S_B} \mod p = (2^{12} \mod 11) = 4$

   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:
   $S = {T_B}^{S_A} \mod p = (4^5 \mod 11) = 1$
   Comprobamos que, efectivamente, Bob obtiene el mismo valor:
   $S' = {T_A}^{S_B} \mod p = (10^{12} \mod 11) = 1$

3. El esquema de sobre digital es la manera adecuada de proporcionar confidencialidad, autenticación e integridad a las comunicaciones entre dos partes, Alice y Bob, con claves, (K_A^+, K_A^-) y (K_B^+, K_B^-), respectivamente. $\boxed{3}$

   Recrea a continuación todo el esquema completo de forma clara y concisa, enumerando cada uno de los pasos en los que consiste. NO es necesario explicar con texto cada paso, si éstos son suficientemente claros.