Ejercicio 4. *(25%)* Alice quiere enviar un mensaje junto con su firma digital a Bob. Dado que comunican a través de un canal inseguro, debe cifrar el mensaje para evitar que un espía lo obtenga. Alice y Bob deciden usar el criptosistema de ElGamal para cifrar el mensaje y el sistema de firma digital basado en ElGamal. Para ambos sistemas, escogen trabajar módulo $p = 11$ con $g = 2$ como elemento generador del grupo multiplicativo (no hace falta demostrar que p es primo o que g es un generadordel grupo multiplicativo). El mensaje, que es un entero módulo p, que Alice quiere enviar a Bob, junto con su firma digital, es $M = 7$.
Para mayor seguridad, deciden usar una función hash h para la firma digital, dicha función es pública. Para resolver este ejercicio no es necesario especificar la función hash h, es suficiente con saber que $h(M) = 4$.
Alice escoge azar 4 como clave privada para firmar el mensaje. Bob escoge al azar 5 como clave privada para que Alice le envíe el mensaje el cifrado.

(a) Explica con un esquema cual es el proceso de firma digital y de cifrado del mensaje. En particular, menciona que datos son públicos y que datos son privados (para Alice y para Bob). También menciona que datos son enviados por Alice a Bob y como descifra Bob el mensaje y comprueba la veracidad de la firma.

(b) Calcula la firma del mensaje $M = 7$ usando la clave privada de Alice.

(c) Calcula el cifrado del mensaje $M = 7$ usando la clave pública de Bob.

(d) ¿Qué envía Alice a Bob a través del canal inseguro de comunicación?

(e) Calcula como Bob descifra el mensaje y comprueba la veracidad de la firma.

(f) ¿Qué beneficio tiene usar una función hash en la firma digital?, o dicho de otra forma, ¿Qué tipo de ataque de un criptoanalista evitan al usar una función hash?

Nota: El esquema de la pregunta (a), si se desea, se puede hacer en varias partes según se va contestando a las siguientes preguntas.

Nota: la respuesta de este ejercicio no es única porque Alice debe escoger un número al azar (que lo escogéis vosotros) para el cifrado y otro para la firma digital.

$p=11$, $g=2$, $M=7$, $h(M)=4$, - Alice escoge $a=4$ - Bob escoge $b=5$

↑ El rol está cambiado =

(b) Alice: $A = g^a \bmod p = 2^4 \bmod 11 = 5$

→ Clave pública: $(p, g, A) = (11, 2, 5)$

→ Clave privada: $(a) = (5)$

- Alice firma el mensaje con $h(M)=4$ y escoge $\boxed{k=3}$ ↑

$r = g^k \bmod p = 2^3 \bmod 11 = 8$

$s = k^{-1}(h(M) - a \cdot r) \Rightarrow 7(4 - 4 \cdot 8) \bmod p-1 = -196 \bmod 10 = \boxed{4}$

•Calculamos $k^{-1} \bmod p-1 = 3^{-1} \bmod 10 = 7$

La firma es $(r, s) = (8, 4)$

Alice ofta usando la clave púb de Bob.

(c) Alice calcula A: $g^a \bmod p = 5$

~~Bob calcula B y cifra el mensaje:~~

$B = g^b \bmod p = 2^5 \bmod 11 = 10$

$C = A^b \cdot M \bmod p = 5^5 \cdot 7 \bmod 11 = 7$

(d) Alice envía $(B, C) = (10, 7)$

(e) - Descifrado:

$B^{p-1-a} \cdot C \bmod p = 10^{11-1-4} \cdot 7 \bmod 11 = 10^6 \cdot 7 \bmod 11 = \boxed{7} = M$

- Comprobación firma:

$A^r \cdot r^s \bmod p = 5^8 \cdot 8^4 \bmod 11 = 4 \cdot 4 \bmod 11 = 16 \bmod 11 = \boxed{5}$

$g^{h(m)} \bmod p = 2^4 \bmod 11 = \boxed{5}$

iguales =

(a) Cifrado M: Alice -> CP: $(P, g, A) = (11, 2, 5)$ C.Priva = (a)

Bob -> C. púb: (B, C) , Clave Pri: (b)

Firma Digital: Alice ->

Bob →

① Ataques de algoritmo discreto //