PRÁCTICA: CIFRADO ELGAMAL ELÍPTICO

Objetivo: Implementar el cifrado de clave pública ElGamal en su versión basada en curvas elípticas.

Desarrollo:

1. Implementa el cifrado ElGamal elíptico para curvas del tipo $y^2= x^3+ ax+ b$, según el diagrama que se incluye a continuación

Dado un número primo p, una curva elíptica E $y^2= x^3+ ax+ b$, y un punto base P de dicha curva

- Clave privada de B: entero aleatorio $d_B \in Z_p$
- Clave pública de B: punto d_BP
- Mensaje original: punto $Q_m \in E$
- Mensaje cifrado de A a B:
  dos puntos $\{Q_m+a_A(d_BP), a_AP\} \in E$
  siendo $a_A \in Z_p$ un entero aleatorio

Para esta implementación se hace necesario:

- Calcular todos los puntos (x,y) de la curva E: obtenidos desechando aquellos enteros x en [0,p-1] que producen valores $x^3+ ax+ b \pmod p$ que no se pueden obtener a partir de $y^2 \pmod p$ para ningún entero y en [0,p-1]
- Opcional: Codificar un mensaje m mediante un punto (x,y) de la curva, donde el mensaje m es un a ristra binaria luego M es una potencia de 2 tq $0<m<M$, obteniendo la constante $h<p/M$, y el menor valor de j (j=0,1,2,…,h-1) para el que $x=mh+j \pmod p$ es coordenada x de un punto de la curva.
- Sumar puntos $P= (x_1,y_1)$ y $Q= (x_2,y_2)$, obteniendo $P+Q = (x_3,y_3)$, donde $x_3= \lambda^2 - x_1 - x_2$, $y_3= \lambda(x_1 - x_3) - y_1$, con

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1}, & \text{si } P \neq Q \\ \dfrac{3x_1^2 + a}{2y_1}, & \text{si } P = Q \end{cases}$$

Nota: Programarlo para a_A y d_B que sean potencias de 2

Ejemplo:

- A partir de las entradas:

p= 13
a= 5
b= 3
P= (9,6)
d_B=2
Mensaje original=(7,2)
Opcional: Mensaje original=m=10=2
M=4
a_A=4

Se producen las salidas:

Puntos de la curva: (0,4),(0,9),(1,3),(1,10),(4,3),(4,10),(5,6),(5,7), (7,2),(7,11),(8,3),(8,10),(9,6),(9,7), (10,0), (12,6),(12,7),
Clave pública de B: punto d_BP=(9,7)
h=3<13/4
Opcional: Mensaje original codificado como punto Q_m =(2*3+1,2)=(7,2)
Primer punto del Mensaje cifrado $Q_m+a_A(d_BP)$=(0,9)
Segundo punto del Mensaje cifrado a_AP=(9,6)