PRÁCTICA: ALGORITMOS DIFFIE-HELLMAN y ELGAMAL ELÍPTICOS

Objetivo: Implementar el algoritmo de Diffie-Hellman y el cifrado de ElGamal en sus versiones basadas en curvas elípticas.

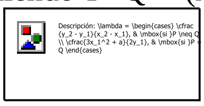
Desarrollo:

1. Implementa ambos esquemas para curvas del tipo $y^2= x^3+ ax+ b$, según elo siguiente.

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

- Clave privada de B: entero aleatorio $d_B \in Z_p$
- Clave privada de A: entero aleatorio $d_A \in Z_p$
- Clave pública de B: punto d_BG
- Clave pública de A: punto d_AG
- Clave secreta compartida calculada por A: $d_A*(d_BG)$
- Clave secreta compartida calculada por B: $d_B*(d_AG)$
- Mensaje original: m codificado como entero
- Mensaje original codificado como punto: $Q_m \in E$
- Mensaje cifrado y clave pública enviados de A a B:
  dos puntos $\{Q_m+d_{A*}(d_BG), d_AG\} \in E$

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 $x^3+ ax+ b$ (mod p) que no se pueden obtener a partir de y^2(mod p) para ningún entero y en [0,p-1]
- Considerar el mensaje m en decimal codificado como una ristra binaria tq 0<m<M, luego M es una potencia de 2 y dicho mensaje m se codifica mediante un punto (x,y) de la curva, obteniendo la constante h<p/M, y el menor valor de j (j=0,1,2,…,h-1) para el que x=mh+j (mod p) es coordenada x de un punto de la curva E.
- Sumar puntos P= (x_1,y_1) y Q= (x_2,y_2), obteniendo P+Q = (x_3,y_3), donde, en módulo p, se tiene que $x_3= \lambda^2 - x_1 - x_2$, $y_3= \lambda(x_1 - x_3) - y_1$, con 

Ejemplo:

- Entradas:

p= 11
a= 1
b= 1
G= (3,8)
d_A=3
d_B=2
Mensaje original=3

- Salidas:

Puntos de la curva: (0,1),(0,10),(1,5),(1,6),(2,0),(3,3),(3,8),(4,5),(4,6),(6,5),(6,6),(8,2),(8,9)
Clave pública de B: punto d_BG=2(3,8)=(6,6)
Clave pública de A: punto d_AG=3(3,8)=(0,1)
4(3,8)=(0,10). 5(3,8)=(6,5)
Clave secreta compartida calculada por A: 3*(6,6)=(3,3)
Clave secreta compartida calculada por B: 2*(0,1)=(3,3)
M=4
h=2<11/4
Mensaje original codificado como punto Q_m =(3*2,5)=(6,5)
Mensaje cifrado y clave pública enviados de A a B: $\{Q_m+d_{A*}(d_BG), d_AG\}$ = {(6,5)+(3,3),(0,1)}={(0,10),(0,1)}