Tarea 3: Curvas Elípticas.

1. Sea la curva elíptica $E := 0 = y^2 - x^3 - x - 9$ definida sobre $\mathbb{Z}_{17}$

   i) Calcula y muestra todos los puntos de E.

   ii) Alicia desea enviar el siguiente mensaje $C = (a, b) = ((12, 7), (11, 12))$ a Bob, los parámetros públicos de Bob son $\alpha = (0, 3) \in E$ una raíz primitiva y $\beta = (13, 3)$, donde $\beta = s\alpha$ y s su llave privada. Usa cualquier algoritmo mencionado en la sección 5.2 del libro **"Elliptic Curves Number Theory and Cryptography de Lawrence C. Washington"** Para resolver el PLD.

   iii) A partir de la información encontrada en *ii*) descifra el mensaje enviado a Bob.

2. Sea $E := y^2 + 20x = x^3 + 21 \ (mod\ 35)$ y sea $P = (15, -4) \in E$.

   i) Factoriza 35 tratando de calcular $3P$.

   ii) Factoriza 35 tratando de calcular $4P$ duplicándolo.

   iii) Calcula ambos $3P$ y $4P$ sobre $E \ (mod\ 5)$ y sobre $E \ (mod\ 7)$ explica por que el factor 5 se obtiene calculando $3P$ y el factor 7 se obtiene calculando $4P$.

3. Alicia quiere firmar un mensaje utilizando el esquema ElGamal elíptico con los siguientes parámetros: $p = 314159$, $a = 217$, $b = 2006$, $P = (123456, 43989)$, $n = 314423$.
   Su clave privada es $d = 223344$ y su clave pública es $Q = (216438, 187612)$.

   i) Si el mensaje que quiere firmar es $m = 6500$ (cantidad de pesos que quiere retirar de su cuenta mediante una transferencia bancaria), ¿cuál es la firma digital de m? (supongamos que el entero aleatorio k tal que $1 \leq k \leq n - 1$ que se tiene que escoger es igual a 666).

   ii) ¿Qué cómputos tiene que hacer el banco para verificar la firma de Alicia?

4. Sea $\mathbb{E} : y^2 = x^3 + 333x + 2$ sobre $\mathbb{F}_{347}$ y sea $P = (110, 136)$

   (a) Si sabemos que $|\mathbb{E}| = 358$. ¿podemos decir que $\mathbb{E}$ es criptográficamente útil?, ¿Cuál es el orden de P? ¿Entre que valores se puede escoger la clave privada?

   (b) Si tu clave privada es $d = 101$ y algún conocido te ha enviado el mensaje cifrado $(C_1 = (232, 278), C_2 = (135, 214))$ ¿Cuál era el mensaje original?

5. Sea $\mathbb{E} : y^2 = x^3 + 2x + 7$ sobre $\mathbb{Z}_{31}$ con $\#\mathbb{E} = 39$ y $P = (2, 9)$ es un punto de orden 39 sobre $\mathbb{E}$, el ECIES simplicado definido sobre $\mathbb{E}$ tiene $\mathbb{Z}_{31}^*$ como espacio de texto plano, supongamos que la clave privada es $m = 8$

   (a) Calcula $Q = mP$

   (b) Descifra la siguiente cadena de texto cifrado
   $((18, 1), 21), ((3, 1), 18)), ((17, 0), 19), ((28, 0), 8)$

   (c) Supongamos que cada texto plano representa un caracter alfabético, convierte el texto plano en una palabra en ingles. usa la asociación $(A \longrightarrow 1, \ldots, Z \longrightarrow 26)$ en este caso 0 no es considerado como un texto plano o un par ordenado[1].

[1] **Nota**: La tarea es en parejas con personas diferentes a las que hicieron las tareas 1 y 2, se entrega el viernes 24 de mayo antes de las 11:59 p.m, solo formato pdf, enviarla a `dolphinperruno@gmail.com, c.c.p. mandiaz@ciencias.unam.mx`, tareas recibidas después de esta hora se calificara sobre 6, no mandar captura de código para justificar procedimientos.