Tarea 3: Criptografía y seguridad- 2020-2, Curvas Elípticas.

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

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

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

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

2. Sea E la curva elíptica $y^2 = x^3 + x + 28$ definida sobre $\mathbb{Z}_{71}$.

   i) Calcula y muestra el número de puntos de E

   ii) Muestra que E no es un grupo cíclico.

   iii) ¿Cuál es el máximo orden de un elemento en E?, encuentra un elemento que tenga este orden.

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

   (a) ¿Es Q=(81,-176) un punto de E?

   ii) 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?

   iii) Si tu clave privada es $k = 101$ y algún conocido te ha enviado el mensaje cifrado $(M_1 = (232, 278), M_2 = (135, 214))$ ¿Cuál era el mensaje original?

4. Sea $\mathbb{E} : F(x, y) = y^2 - x^3 - 2x - 7$ 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 $m = 8$

   i) Calcula $Q = mP$

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

   iii) 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.