Facultad de Ciencias, UNAM
Criptografía y Seguridad
Tarea 3

Altamirano Vázquez Jesús Fernando
Rubí Rojas Tania Michelle

9 de junio de 2020

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

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

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

   c) Calcula $3Q$ y $4Q$ sobre $\mathbb{E}$ (mód 5) y sobre $\mathbb{E}$ (mód 7). Explica por qué el factor 5 se obtiene calculando $3Q$ y por qué el factor 7 se obtiene calculando $4Q$.

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

   a) Calcula y muestra el número de puntos de $\mathbb{E}$.

   b) Muestra que $\mathbb{E}$ no es un grupo cíclico.

   c) ¿Cuál es el máximo órden de un elemento en $\mathbb{E}$? Encuentra un elemento que tenga este órden.

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 $\mathbb{E}$?

   b) Si sabemos que $|\mathbb{E}| = 358$. ¿Podemos decir que $\mathbb{E}$ es criptográficamente útil? ¿Cuál es el órden de P? ¿Entre qué valores se puede escoger la clave privada?

   c) 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 órden 39 sobre $\mathbb{E}$, el ECIES simplificado 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 carácter alfabético, convierte el texto plano en una palabra en Inglés. Usa la asociación $(A \to 1, ..., Z \to 26)$.