Ejercicio 3

David García Curbelo

Sea $\mathbb{F}_{32} = \mathbb{F}_2[\xi]_{\xi^5+\xi^2+1}$. *Cada uno de vosotros, de acuerdo a su número de* $DNI = 45352581$ *o similar, dispone de una curva elíptica sobre* $\mathbb{F}_{32}$ *con una raíz* x *y un punto base dados en el Cuadro 6.1.*

Ejercicio 1. *Calcula, mediante el algoritmo de Shank o mediante el Algoritmo 9,* $\log_Q \mathcal{O}$.

Ejercicio 2. *Para tu curva y tu punto base, genera un par de claves pública/privada para el protocolo ECDH.*

Ejercicio 3. *Cifra el mensaje* $(\xi^3 + \xi^2 + 1, \xi^4 + \xi^2)$ *mediante el criptosistema de Menezes-Vanstone.*

Ejercicio 4. *Descifra el mensaje anterior.*