Ejercicio Tema 5

Ana Buendía Ruiz-Azuaga

May 23, 2022

1 Ejercicio Tema 5

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

2 Apartado 1

Calcula, mediante el algoritmo de Shank o mediante el Algoritmo 9, $\log_Q O$

Res

3 Apartado 2

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

Res

4 Apartado 3

Cifra el mensaje $(\xi^3+\xi^2+1, \xi^4+\xi^2) \in \mathbb{F}_{32}^2$ mediante el criptosistema de Menezes-Vanstone

Res

5 Apartado 4

Descifra el mensaje anterior.

Res