Ejercicio 3

David García Curbelo

Los parámetros de un criptosistema de ElGamal son $p = 211$ *y* $g = 3$*, es decir, el criptosistema está diseñado en el cuerpo* $\mathbb{F}_{211} = \mathbb{Z}_{211}$ *y tomamos como generador de* $\mathbb{F}_{211}^*$*,* $g = 3$*. La clave pública empleada es* $3^a = 109 \pmod{211}$*. Descifra el criptograma* $(154, dni \pmod{211})$*, donde dni es el número de tu DNI. Para calcular los logaritmos discretos necesarios emplea dos de los métodos descritos en la teoría.*