

Ejercicio 2

David García Curbelo

Consideremos el cifrado por bloques miniAES descrito en el ejercicio 2.1.

Apartado I. *Calcula $E_{dni}(0x01234567)$ usando el modo CBC e $IV = 0x0001$.*