Ejercicio 1

David García Curbelo

Consideremos el cifrado por bloques miniAES descrito en el ejercicio 2.1.
Apartado I. ***Calcula*** $\boldsymbol{E_{dni}}(0x01234567)$ ***usando el modo*** CBC ***e*** $IV = 0x0001$***.***

Apartado I. ***Calcula*** $\boldsymbol{E_{dni}}(0x01234567)$ ***usando el modo*** CFB***,*** $r = 11$***, y vector de inicialización*** $IV = 0x0001$***.***