Ejercicios de repaso Módulos I y II

1. El LFSR con polinomio de realimentación 1+ x +x2 + x4 y semilla 0001 genera el primer periodo

3. Obtén el último elemento de la 1ª columna del estado salida de la operación MixColumn del cifrado AES para el estado de entrada S:

d4	e0	b8	1e
bf	b4	41	27
5d	52	11	98
30	ae	f1	e5