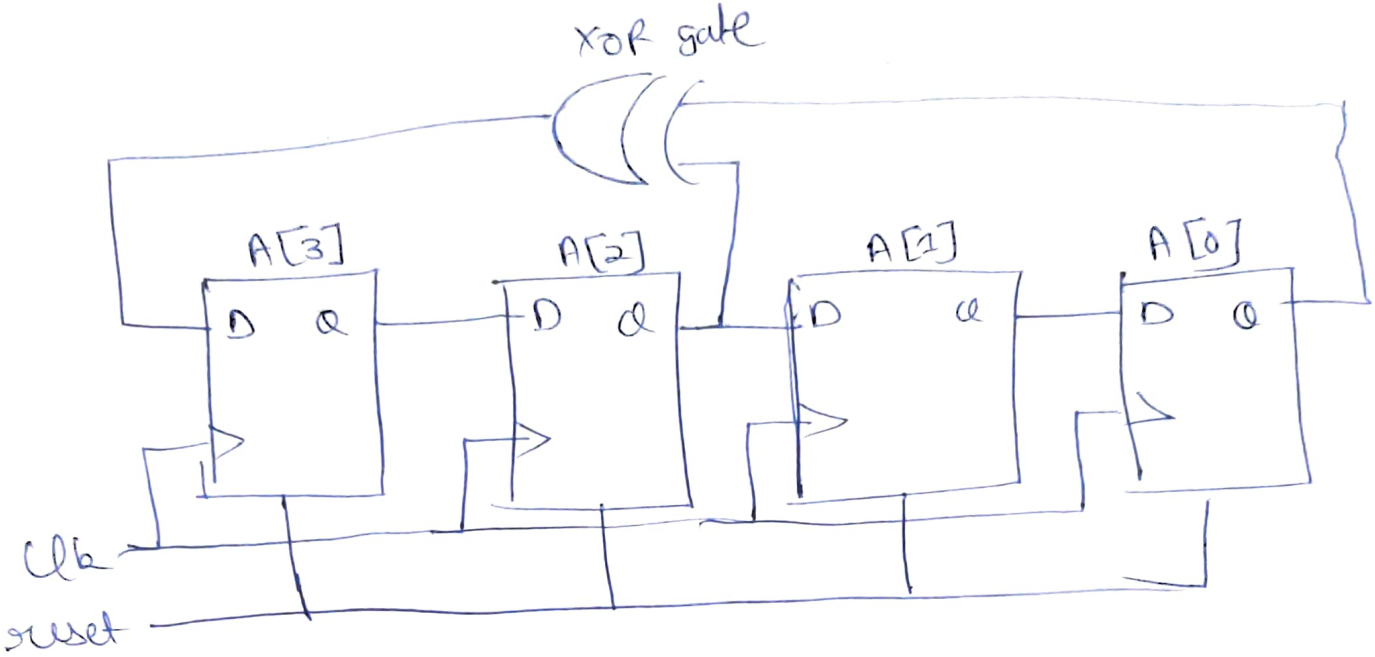
Q1]



Q3]

a) Input = [redacted] 10100111

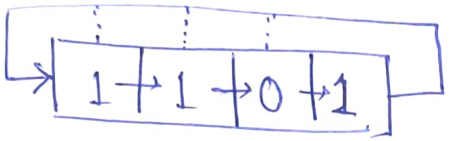
Output = 0001010 1

key = Input ⊕ output = 10110010

b). Key generated : 1 0 1 1 . . . . . .

to get the first 4 key outputs as 1 0 1 1, initial state needs to be: A[3] = 1, A[2] = 1 A[1] = 0 A[0] = 1

c) We know, Initial State of Shift Register



(we don't know which bit out of A[1], A[2], A[3] is being used to XOR)

↳ To figure out the XOR BIT we look at the next BITS of Key generated.

Current State	Next Keybit to generate	XOR OPtions
1101	0	A[3] or A[2]
0110	0	Only A[3]

Key

10110010

↳ This means XORing the A[3] with A[0] gives our new A[3] and we may not check any further.