۱۰ آذر
چهارشنبه
۲۵ ربیع الثانی ۱۴۴۳
1 Dec.2021

در الگوریتم رمزنگاری AES یک مدار شیفت به راست چرخشی نیاز داریم. در این مدار بر حسب انتخاب مقادیر S_0 و S_1 ورودی ۴ بیتی $W[3:0]$ به شکل جدول زیر شیفت می یابد. مدار معادل را فقط با ماشین پلکسرها پیاده سازی کنیم.

S_1	S_0	y_3	y_2	y_1	y_0
0	0	w_3	w_2	w_1	w_0
0	1	w_0	w_3	w_2	w_1
1	0	w_1	w_0	w_3	w_2
1	1	w_2	w_1	w_0	w_3

-20