

در الگوریتم رمزنگاری AES یک مدار شیفت به راست چرخشی نیاز داریم. در این مدار برحسب انتخاب‌های s_0 و s_1 ورودی ۴ بیتی $w[3:0]$ به شرح جدول درستی زیر شیفت می‌یابد. مدار معادل را فقط با مالتی پلکسرها پیاده‌سازی کنید.

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

