【例4-15】设当前的State为

$$\begin{bmatrix} D1 & 85 & 1A & F9 \\ 93 & 1B & F7 & 10 \\ CA & A8 & B6 & 45 \\ 40 & 8F & F5 & 20 \end{bmatrix}$$

计算MixColumn (State) 列混合

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} D1 & 85 & 1A & F9 \\ 93 & 1B & F7 & 10 \\ CA & A8 & B6 & 45 \\ 40 & 8F & F5 & 20 \end{bmatrix} = \begin{bmatrix} 9D & 1B & 75 & BC \\ E9 & DF & DB & 36 \\ 0D & 5F & 9E & 03 \\ B1 & 22 & 9E & 05 \end{bmatrix}$$

代码中叫做state1，

87	F2	4D	97
6E	4C	90	EC
46	E7	4A	C3
A6	8C	D8	95

State → 列混合后

47	40	A3	4C
37	**D4**	70	9F
94	E4	**3A**	42
ED	A5	A6	**BC**

代码中交state2