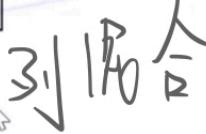


【例4-15】设当前的State为

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

计算MixColumn (State) 

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

代码中叫做state1,

87 <sub>16</sub>	F2 <sub>16</sub>	4D <sub>16</sub>	97 <sub>16</sub>
6E <sub>16</sub>	4C <sub>16</sub>	90 <sub>16</sub>	EC <sub>16</sub>
46 <sub>16</sub>	E7 <sub>16</sub>	4A <sub>16</sub>	C3 <sub>16</sub>
A6 <sub>16</sub>	8C <sub>16</sub>	D8 <sub>16</sub>	95 <sub>16</sub>

State

47 <sub>16</sub>	40 <sub>16</sub>	A3 <sub>16</sub>	4C <sub>16</sub>
37 <sub>16</sub>	D4 <sub>16</sub>	70 <sub>16</sub>	9F <sub>16</sub>
94 <sub>16</sub>	E4 <sub>16</sub>	3A <sub>16</sub>	42 <sub>16</sub>
ED <sub>16</sub>	A5 <sub>16</sub>	A6 <sub>16</sub>	BC <sub>16</sub>

→ 列混合后

代码中交state2