

PLAIN/CIPHER TEXT (ARRAY OF 16 BYTES)

$b_0, b_1, b_2, b_3, b_4, b_5, \dots, b_{15}$

STATE MATRIX (4×4 MATRIX OF BYTES)

ROW ₀	$S_{0,0}=b_0$	b_4	b_8	b_{12}
ROW ₁	b_1	b_5	b_9	b_{13}
ROW ₂	b_2	b_6	b_{10}	b_{14}
ROW ₃	b_3	b_7	b_{11}	$S_{3,3}=b_{15}$
	COL ₀	COL ₁	COL ₂	COL ₃

Figure 1

The main encryption process first moves the plain text to a 4×4 -byte matrix called the "state."