

state = plaintext

add\_roundkey (state, round 0)

i = 0

sbox (state)

linear\_matrix\_multiply (state, round i)

add\_roundconst (state, round i)

add\_roundkey (state, round i+1)

repeat while  
i < n\_rounds

i = i + 1

ciphertext = state

