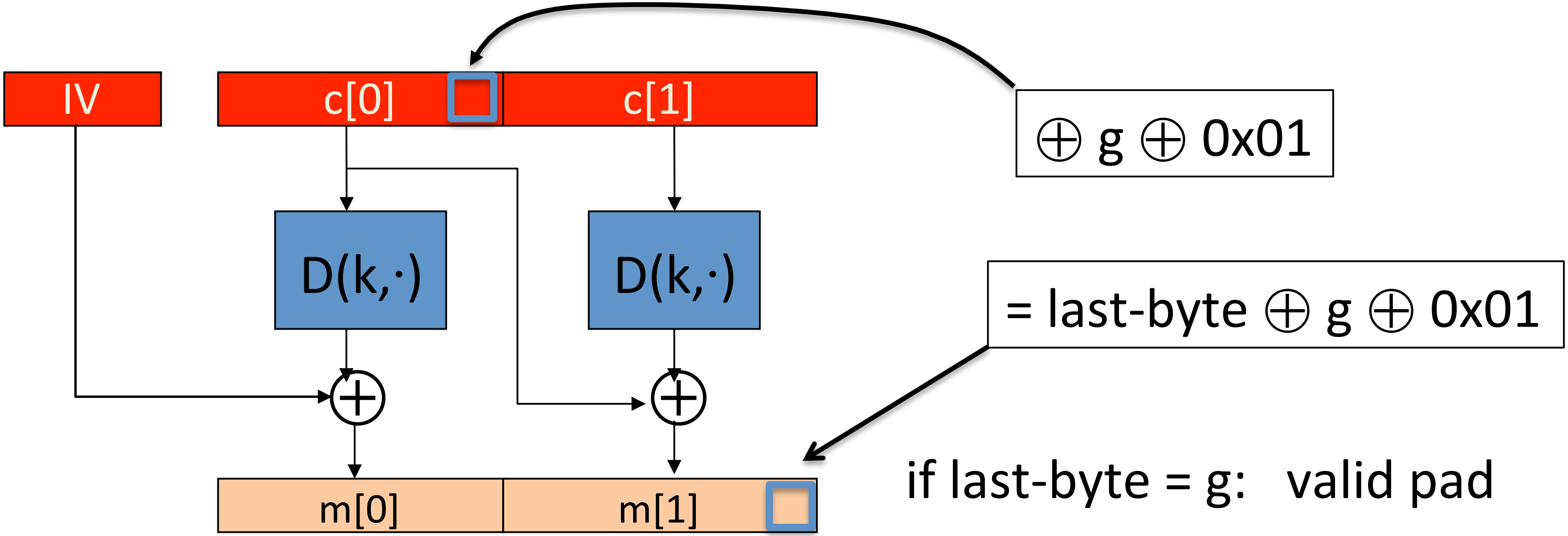
step 1: let **g** be a guess for the last byte of m[1]



$\oplus$ g $\oplus$ 0x01

= last-byte $\oplus$ g $\oplus$ 0x01

if last-byte = g: valid pad

otherwise: invalid pad