# Tema 8 - Cripto

$m = X = 23$

$K_c = (31, 3, 19)$

$K = 3$

$p = 31$

$g = 3$

$\alpha = 19$

$u = g^K \pmod p$

$v = m \, x^K \pmod p$

$u = 3^3 \pmod{31} \equiv 27 \bmod 31$

$v = 23 \cdot 19^3 \pmod{31} \equiv 23 \cdot 19 \cdot 19^2 \bmod 31 \equiv 23 \cdot 19 \cdot 361 \equiv$

$\equiv 23 \cdot 19 \cdot 20 \equiv 23 \cdot 380 \equiv 28 \cdot 8 \equiv 184 \bmod 31 \equiv 29 \bmod 31$

$(u, v) = (27, 29) \qquad (?, \circ)$