

Tema 8 - Crip

$$\begin{aligned} m &= X = 23 \\ K_e &= (31, 3, 19) \\ K &= 3 \\ p &= 31 \\ g &= 3 \\ \alpha &= 19 \end{aligned}$$

$$\begin{aligned} u &= g^K \pmod{p} \\ v &= m \cdot X^K \pmod{p} \end{aligned}$$

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

$$\begin{aligned} V &= \cancel{23} \cdot 19^3 \pmod{31} \equiv 23 \cdot 19 \cdot 19^2 \pmod{31} \equiv 23 \cdot 19 \cdot 361 \equiv \\ &\equiv 23 \cdot 19 \cdot 20 \equiv 23 \cdot 380 \equiv 28 \cdot 8 \equiv 184 \pmod{31} \equiv 29 \pmod{31} \end{aligned}$$

$$(u, v) = (27, 29) \quad (?, 0)$$