Tomás Higuera Viso e359327

EJERCICIO 3

(2) $c = 359327$

(3) $K_{PUB} = \{e=29, 91\}$

$\boxed{\begin{matrix} n=91 \\ e=29 \end{matrix}} \rightarrow n = p \cdot q$

$\boxed{n = 7 \cdot 13 = 91} \rightarrow \boxed{\begin{matrix} p = 7 \\ q = 13 \end{matrix}}$

(4) $Z = (7-1)\cdot(13-1) = \boxed{72}$

(5) $e \cdot d \bmod Z = 1$

$29 \cdot d = 1 \bmod(\phi(n))$

$d = \frac{72k+1}{29} = \frac{72\cdot 2+1}{29} = \boxed{5}$

k tiene que ser entero al igual que d.

(6) $c = 359327$

$K_{PRIV} = \{91, 5\}$

$m_0 = 3^5 \bmod 91 = 61$

$m_1 = 5^5 \bmod 91 = 31$

$m_2 = 9^5 \bmod 91 = 81$

$m_3 = 3^5 \bmod 91 = 61$

$m_4 = 2^5 \bmod 91 = 32$

$m_5 = 7^5 \bmod 91 = 63$

$\rightarrow \boxed{m = 61-31-81-61-32-63}$

Escaneado con CamScanner