ELGAMAL

P = 2579, a = 765, α = 2, t = 1, k = 853, m = 1299

Cifrado :

para la llave β = powermod(2, 765, 2579) = 949 y publico (2576, 2, 949) y privado (765).

y1 = powermod(2, 853, 2579) = 435

δ1 = (powermod (949, 853, 2579))\*1299 mod (2579) = (2424\* 1299) mod (2579) = 2396

c1 =(y1, δ1) = (435, 2396)

Descifrado:

p’ = p – 1 – 765 = 1813

m’ = powermod(435, 1813, 2579) = 1980

m = (1980\*2396) mod (2579) = 1299

**c1 =(y1, δ1) = (435, 2396)**

**llave publica (α, p, β) = (2, 2579, 949)**

**llave privada (a = 765)**