

# [PAN] Cifrado Homomórfico (Resumen)

Se utiliza cuando se quieren realizar computaciones en una entidad que no es de confianza. Se realiza el uso de grupos de homomorfismos:  $D_K(x+y) = D_k(x) \{ o \} D_k(y)$

- Cifrado:  $Cx = E(X) = X^e \text{ mod}(n)$ ;  $Cy = E(y) = y^e \text{ mod}(n)$
- Descifrado:  $X = D(Cx) = c_x^d \text{ mod}(n)$ ;  $Y = D(Cy) = c_y^d \text{ mod}(n)$
- Multiplicación:  $Cx * Cy = (x^e \text{ mod}(n)) * (y^e \text{ mod}(n)) = X^e * y^e \text{ mod}(n) = (x*y)^e \text{ mod}(n) = E(x*y)$
- Por lo tanto  $D(C_x * C_y) = x*y$

From:

<http://knoppia.net/> - Knoppia

Permanent link:

[http://knoppia.net/doku.php?id=pan:res\\_cifrado\\_homomorfico&rev=1736276849](http://knoppia.net/doku.php?id=pan:res_cifrado_homomorfico&rev=1736276849)

Last update: **2025/01/07 19:07**

