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