Cifrado Homomorfico

Cuando un tercero tiene que operar con nuestros datos y no queremos que los vea, se aplica cifrado homomorfico, que permite realizar operaciones sobre datos cifrados.

A la hora de operar con cifrado homomorfico se usan los siguientes componentes:

- **n** → Tamaño de los vectores
- **q** → Valor del módulo (módulo q)
  - Trabajamos con módulos en potencias de 2 (2^x)
- **e** → Error
  - Dsitribución normal N(0,γ*q) → r = γ*q
    - Media 0
    - Valor relacionado con q
    - El valor debe estar redondeado
    - Valor entre 0 y q
- **a** → Vector de soporte
  - Vector de tamaño n con valores entre 0 y q-1
- **S** → Secreto o clave privada
  - Solo la conoce el dueño de los datos a operar
  - Valores aleatorios del conjunto {-1,0,1}

Sabiendo esto, sabemos que la clave pública (a,b) del cifrado homomorfico es:

$(a,b) = S^T*a+e MOD (q)$