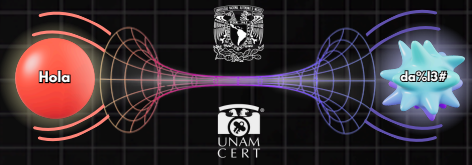
Mecanismos de Cifrado

El cifrado es un proceso que transforma la **información legible (texto plano)** en un **formato ilegible (texto cifrado)** mediante el uso de algoritmos y claves criptográficas.



Hay dos principales tipos de cifrado que se usan de forma frecuente:

Cifrado simétrico: Usa una sola clave para cifrar y descifrar.

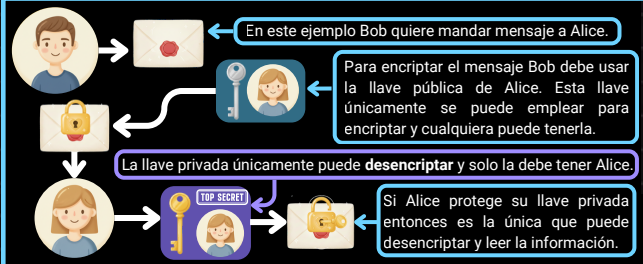
Es fundamental buscar un medio seguro para compartir la llave, ya que si se filtra, cualquiera puede acceder a la información.

Algunos de los algoritmos más populares para este tipo de cifrado son:

AES (Advanced Encryption Standard) · **Blowfish / Twofish** · **DES / 3DES**

Son muy utilizados en el cifrado local de datos y VPN's.

Cifrado simétrico: Usa dos claves diferentes pero relacionadas, una pública para cifrar y una privada para descifrar.



Este tipo de cifrado es considerablemente más seguro dado que la clave privada nunca se comparte.

Algunos de los algoritmos más populares para este tipo de cifrado son:

RSA (Rivest–Shamir–Adleman) · **ECC (Elliptic Curve Cryptography)**

Son muy utilizados en el cifrado HTTPS y certificados SSL/TLS, firmas digitales, correos electrónicos y autenticación.

Bibliografía

Ciampa, M. (2022). CompTIA Security+: Guide to network security fundamentals (7th ed.). Cengage Learning.