

Cifrado

# Cifrado

- En el punto de origen:
  - Se dispone de los datos originales
  - Se dispone de una clave o algoritmo de cifrado
  - Se cifran los datos originales usando la clave o algoritmo
  - Un atacante no puede descifrar los datos si no conoce la clave

# Descifrado

- En el punto de destino
  - Se recibe el mensaje cifrado
  - Se tiene la clave o el algoritmo de cifrado
  - Se aplica de manera inversa
  - Se obtiene el mensaje original

# Cifrado en un sistema

- Ayuda a que la información viaje protegida
- La clave de cifrado debe ser guardada en secreto
- La clave de cifrado debe tener una fuerza suficiente
- El propio acto de cifrado requiere recursos del sistema
  - En ocasiones el cifrado va en contra de la eficiencia

# Ejemplo