# Encriptación

# Encriptación sin retorno

- También conocida como hashing
  - Se dispone de los datos originales
  - Se dispone de un algoritmo de hash
  - Se cifran los datos originales usando el algoritmo
  - ¡Obtenemos una cadena indescifrable!

# No se desencripta

- En el punto de destino
  - Se recibe el mensaje encriptado
  - Se obtiene un valor a comparar
  - Se encripta dicho valor
  - Se comparan las dos cadenas
  - Si hay coincidencia, es que la cadena original es la misma

# Uso típico del cifrado

- Codificar información como contraseñas
- Se compara el hash de la contraseña
- Motivo por el cual ninguna web actual te da tu contraseña si la has olvidado
  - ¡Ellos tampoco la tienen!

# Peligro del hashing

- Se pueden generar bibliotecas
- Existen estas bibliotecas de fuerza bruta de hashes en internet
- Ocupan varios gigas
- Para un hash, ofrecer cientos de cadenas coincidentes
- Facilitan el proceso de ataque

# Ejemplo