

# Lección 2: Sistemas de Cifra con Clave Secreta

---



**intypedia**  
INFORMATION SECURITY ENCYCLOPEDIA

**Fausto Montoya Vitini**

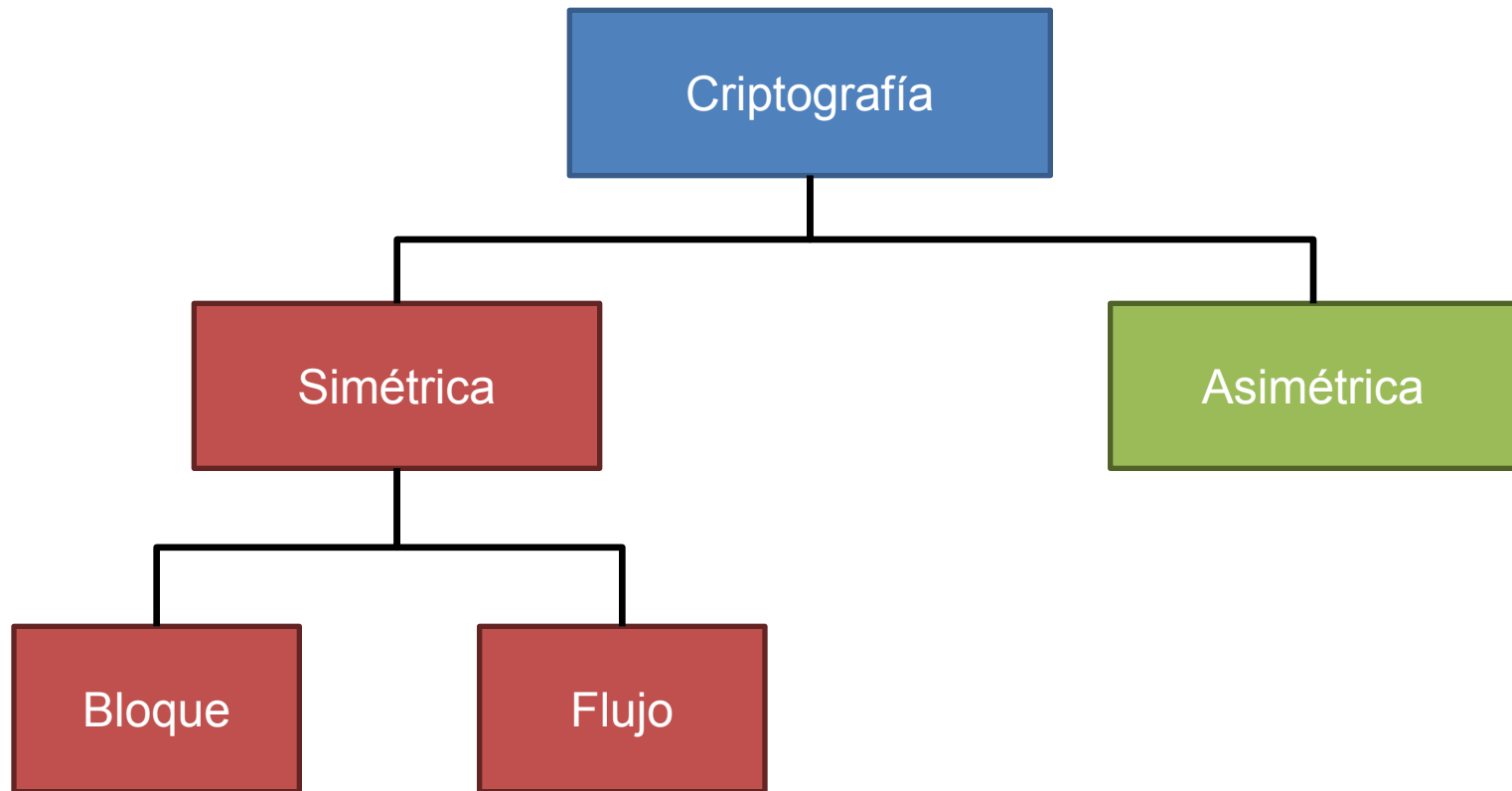
fausto@iec.csic.es

**Consejo Superior de Investigaciones Científicas**

Profesor de Investigación

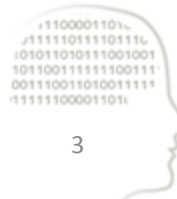
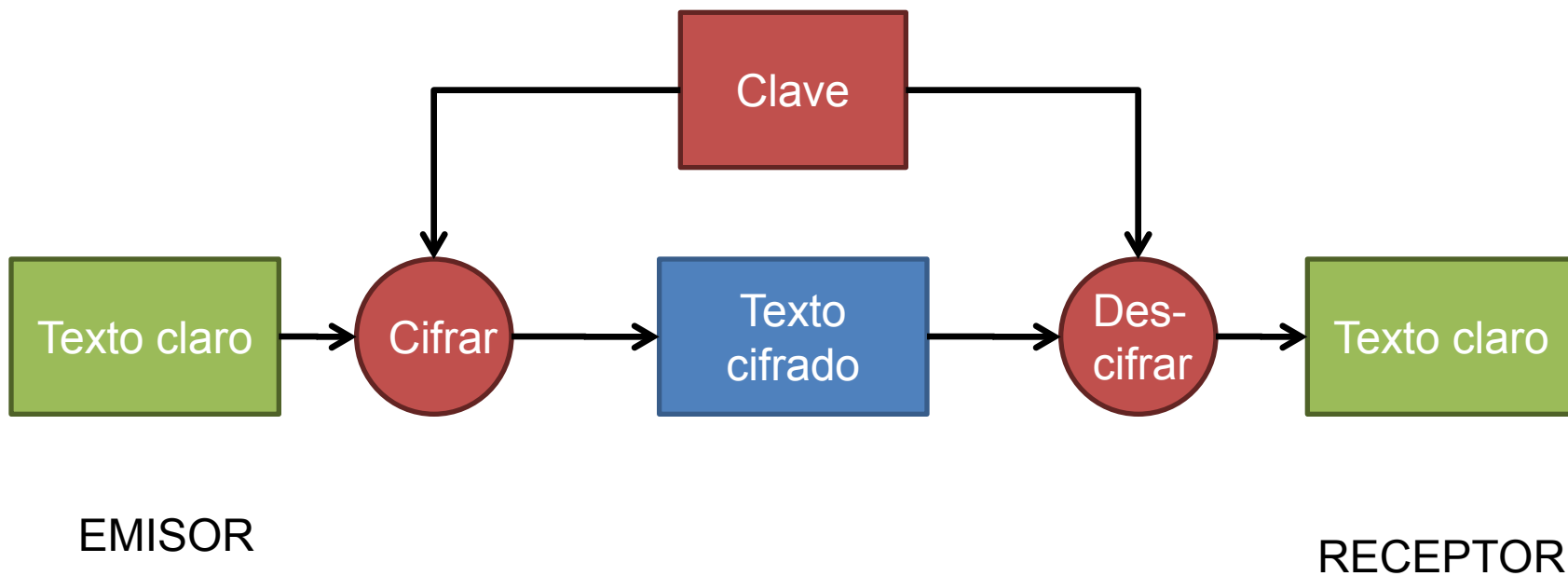
# Los tipos de criptografía

---



# Funcionamiento del cifrado simétrico

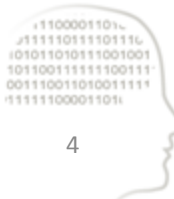
- Se utiliza la misma clave para cifrar y descifrar



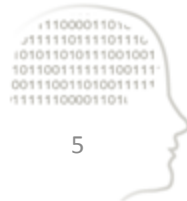
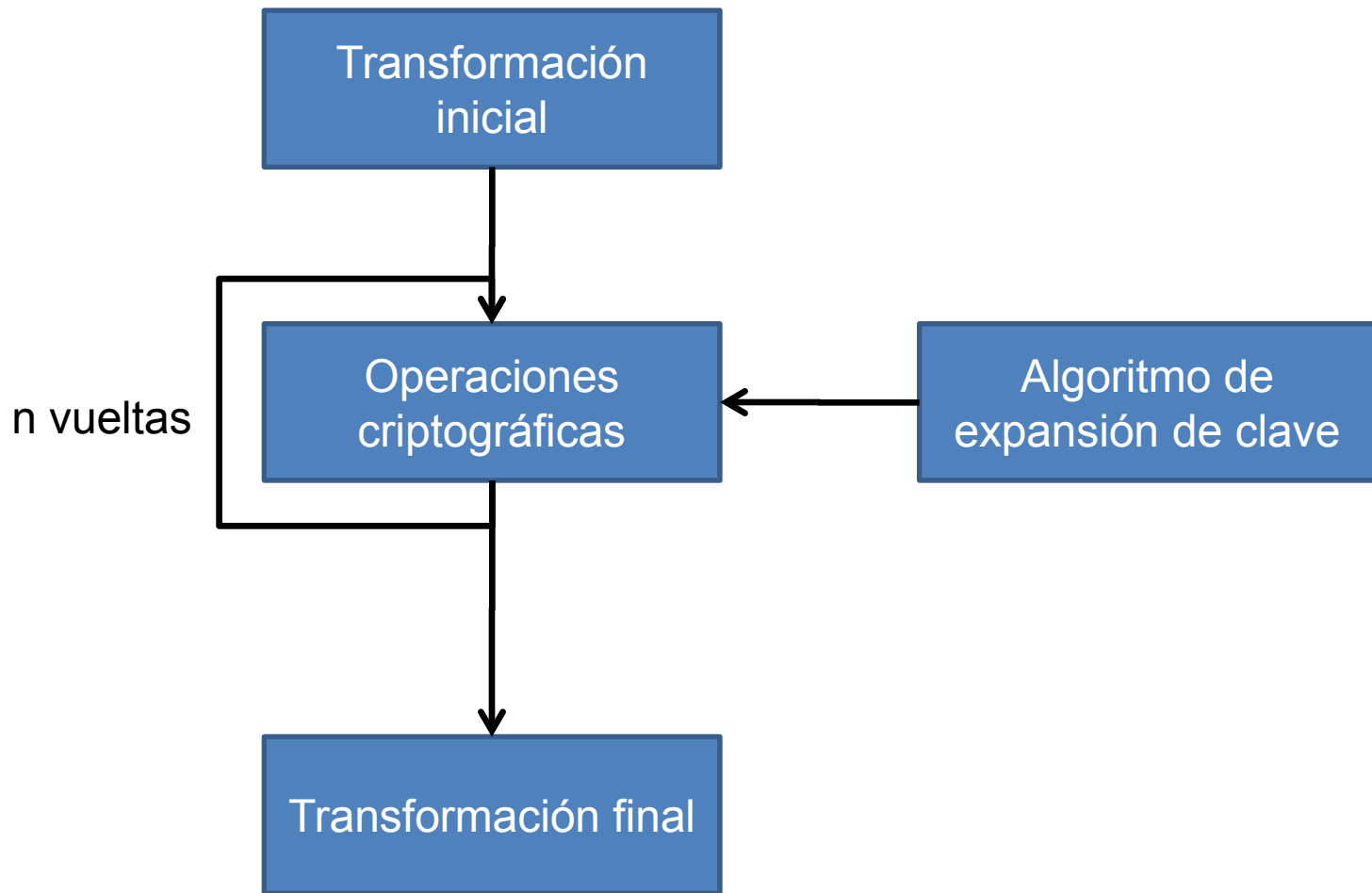
# Cifrado en bloque I

---

- El texto en claro se cifra en secuencias de bits o bloques de tamaño fijo
- El tamaño de bloque suele oscilar entre 64 y 256 bits.
- Nunca deben cifrarse los bloques individual e independientemente, sino encadenados, de manera que el cifrado de cada bloque dependa de todos los bloques que lo preceden.



# Cifrado en bloque II



# Cifrado en bloque III

---

- Transformación inicial
  - Aleatoriza los datos de entrada y puede añadir complejidad a los datos.
- Vueltas de cifrado
  - Función no lineal complicada de los datos y la clave.
  - Puede consistir en una sola operación muy compleja o en la sucesión de varias transformaciones simples.



# Cifrado en bloque IV

---

- Transformación final
  - Sirve para que las operaciones de cifrado y descifrado sean simétricas.
- Algoritmo de expansión de clave
  - Convierte la clave de usuario en un conjunto de subclaves que pueden estar constituidas por varios cientos de bits en total.
  - Conviene que sea unidireccional.
  - Conocer una subclave no debe permitir deducir las demás.



# Propiedades necesarias para un buen algoritmo de cifrado en bloque

---

- Confusión
  - Un pequeño cambio en la clave debería producir un cambio del 50% del texto cifrado resultante.
  - Un atacante haciendo una búsqueda exhaustiva de claves no recibirá ninguna señal de que está acercándose a la clave correcta.
- Difusión
  - Un pequeño cambio en el texto en claro debería producir un cambio del 50% del texto cifrado resultante.
  - Oculta las relaciones estadísticas entre el texto claro y el texto cifrado.
- Completitud
  - Cada bit del texto cifrado dependerá de cada bit de la clave.
  - El atacante no podrá obtener partes válidas de la clave mediante ataques de “divide y vencerás”.



# Cifrado en flujo I

---

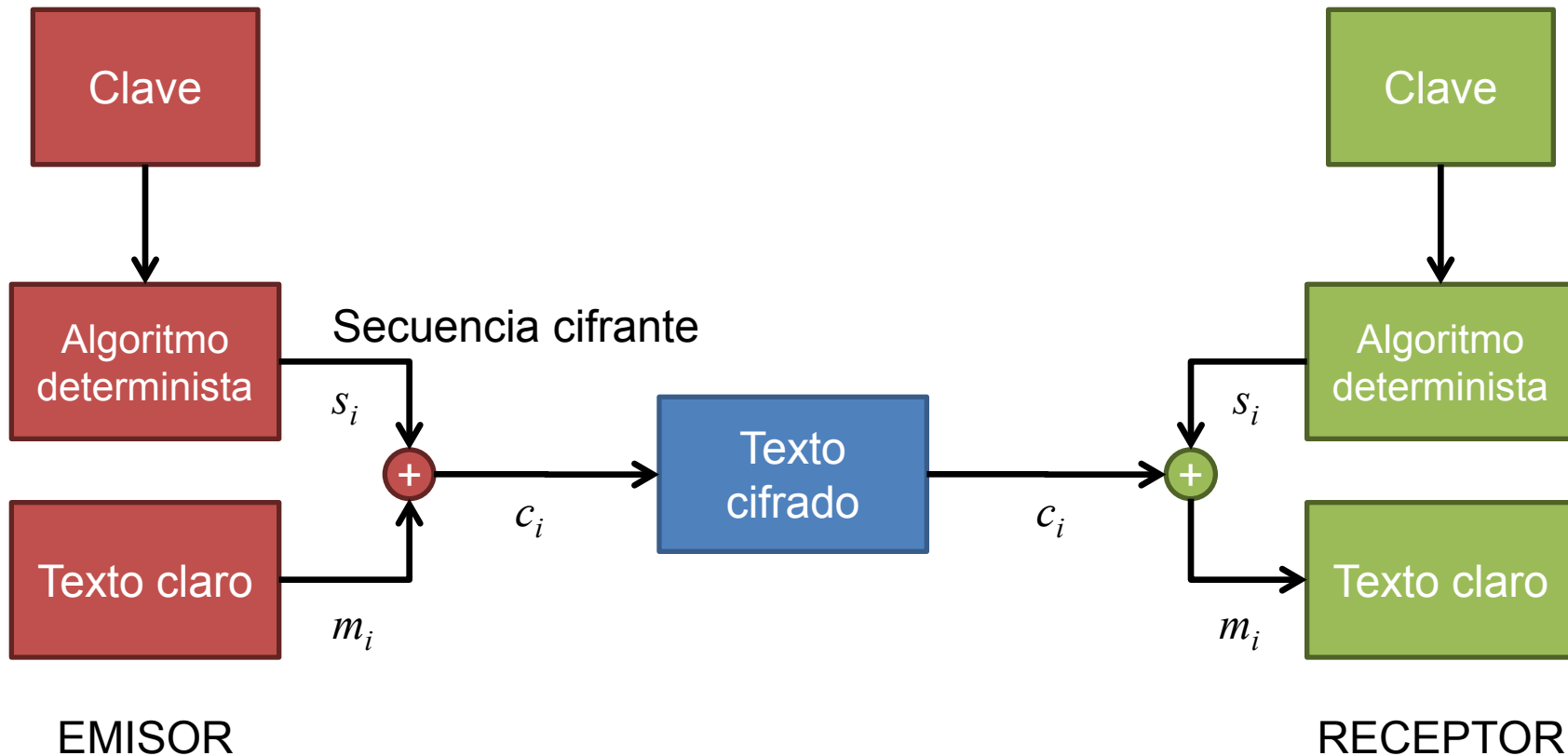
- El texto en claro se cifra bit a bit.
- Se utiliza una secuencia cifrante ( $s_i$ ) para determinar si cada bit del texto claro ( $m_i$ ) se cambia o se deja sin cambiar.

Cifrado:  $c_i = m_i + s_i$       Descifrado:  $m_i = c_i + s_i$

- La secuencia cifrante se crea mediante un algoritmo determinista de generación de números pseudoaleatorios a partir de una semilla, que constituye la clave secreta.



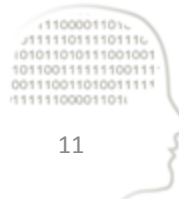
# Cifrado en flujo II



# Ataque de fuerza bruta (o búsqueda exhaustiva de claves)

---

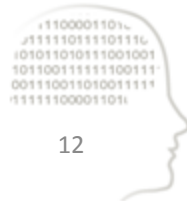
- Un algoritmo está bien diseñado si la forma más simple de ataque es la búsqueda exhaustiva de claves.
- Los ataques de fuerza bruta o de búsqueda exhaustiva de claves consisten en probar una a una todas las posibles combinaciones de la clave.
- Para una clave de  $n$  bits, el número total de claves posibles (o el tamaño del espacio de claves) es igual a  $2^n$ .
- En promedio, habrá que probar la mitad de claves hasta dar con la correcta.
- Hoy para que el ataque sea computacionalmente irrealizable se recomienda una longitud mínima de 128 bits de clave.



# Comparación entre el cifrado en bloque y cifrado en flujo

---

- Ambos tipos de algoritmos son muy rápidos, adecuados por tanto para cifrar grandes volúmenes de datos, pero los de flujo son incluso más veloces.
- Los algoritmos de flujo pueden cifrar datos producidos a ráfagas sin esperar a que estén los bloques completos.
- En los cifrados de flujo nunca se debe reutilizar la misma clave para cifrar dos textos.
- Las longitudes de clave oscilan entre los 32 y 256 bits.
- Ambos presentan el problema de distribución de la clave: ¿cómo hacer que el emisor y receptor acuerden una misma clave secreta de cifrado?





# intypedia

INFORMATION SECURITY ENCYCLOPEDIA