SEGURIDAD DE LA INFORMACIÓN

TEMA 2 – PARTE 3

TÉCNICAS CRIPTOGRÁFICAS BÁSICAS

(Y SERVICIOS DE SEGURIDAD ASOCIADOS)

- Recomendaciones generales:
  - En general, la **longitud mínima de clave** para un cifrado simétrico en bloque debería ser **128 bits**
  - **El tamaño mínimo de los bloques de datos** dependerá de la aplicación específica en la que se use el algoritmo, pero en la mayoría de ocasiones el mínimo **debería ser 128 bits**
  - La **cantidad máxima de información a cifrar con una misma clave debería limitarse a $2^{n/2}$**, donde *n* es el tamaño del bloque de datos

CLAVES: >= 128 bits	Bloques: >= 128 bits	Rekeying: cada $2^{n/2}$

Otros algoritmos simétricos relevantes

- Blowfish
  - Requiere una **clave de entre 32 y 448 bits** (pero sólo **se recomienda** su uso con **más de 80 bits**)
  - Se utiliza en algunas configuraciones de IPSEC
  - La longitud de cada **bloque de datos** es **de 64 bits**, demasiado pequeño para algunas aplicaciones
    - Por ese motivo, sólo se recomienda en uso heredado (*legacy use*)
- Kasumi
  - Requiere una **clave de 128 bits** de longitud, y la longitud de los **bloque de datos** es **de 64 bits**
  - Se usa en UMTS (con el nombre UIA1) y en GSM (con el nombre A5/3)
  - Presenta una serie de problemas que no afectan a su uso práctico en esas aplicaciones
    - sin embargo, no se recomienda para aplicaciones futuras
- Camellia
  - Requiere una **clave de 128 bits**, pero también da soporte a claves **de 192 y 256 bits**
    - Las versiones con 192 o 256 bits de clave son un 33% más lentas que la de 128 bits
  - Se utiliza como **uno de los posibles cifrados en TLS**
  - Por el momento no se han encontrado ataques efectivos a este algoritmo

- Continuando con las recomendaciones…

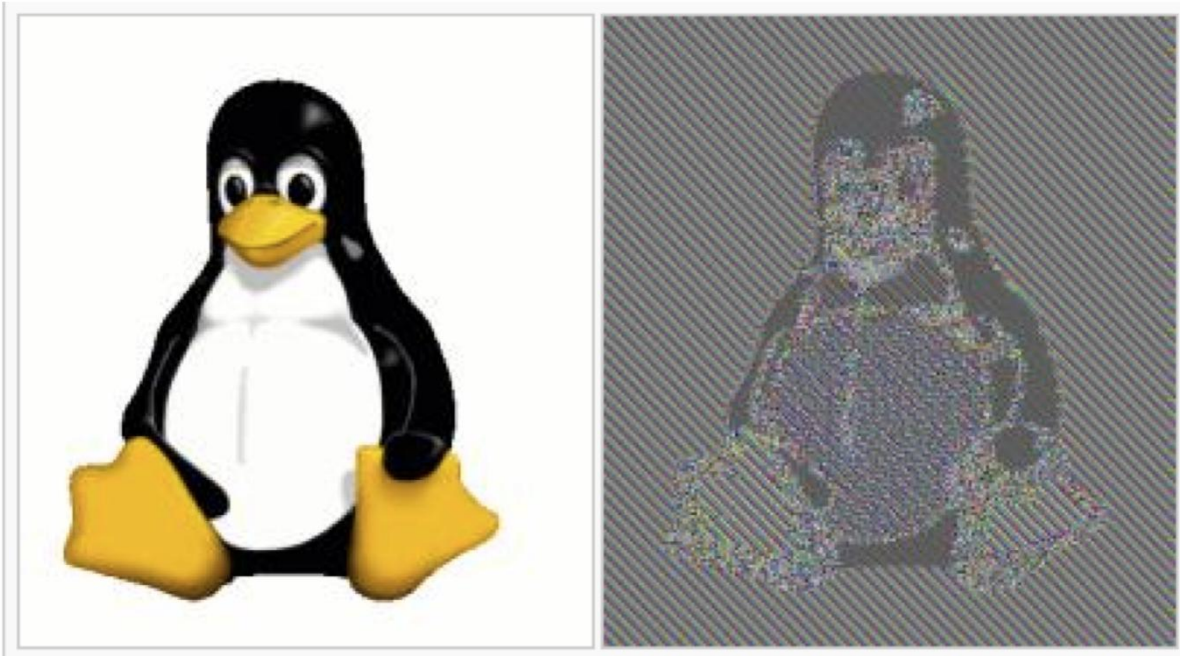
Primitive	Recommendation	
	Legacy	Future
AES	✓	✓
Camellia	✓	✓
Three-Key-3DES	✓	✗
Two-Key-3DES	✓	✗
Kasumi	✓	✗
Blowfish$^{\geq 80\text{-bit keys}}$	✓	✗
DES	✗	✗

La verdadera fortaleza de las claves de 256 bits

$\sim 4{,}4 * 10^{21}$	Todos los datos del mundo en 2013
$\sim 7 * 10^{22}$	Estrellas en el universo
$4{,}37 * 10^{29}$	Longitud en mm del Universo observable
$1{,}4615 * 10^{48}$	2^{160}
$1{,}1579 * 10^{77}$	2^{256}
$\sim 7{,}1 * 10^{79}$	Átomos del Universo
$\sim 10^{85}$	Átomos del Universo + Átomos Materia oscura

Modos de operación para algoritmos simétricos

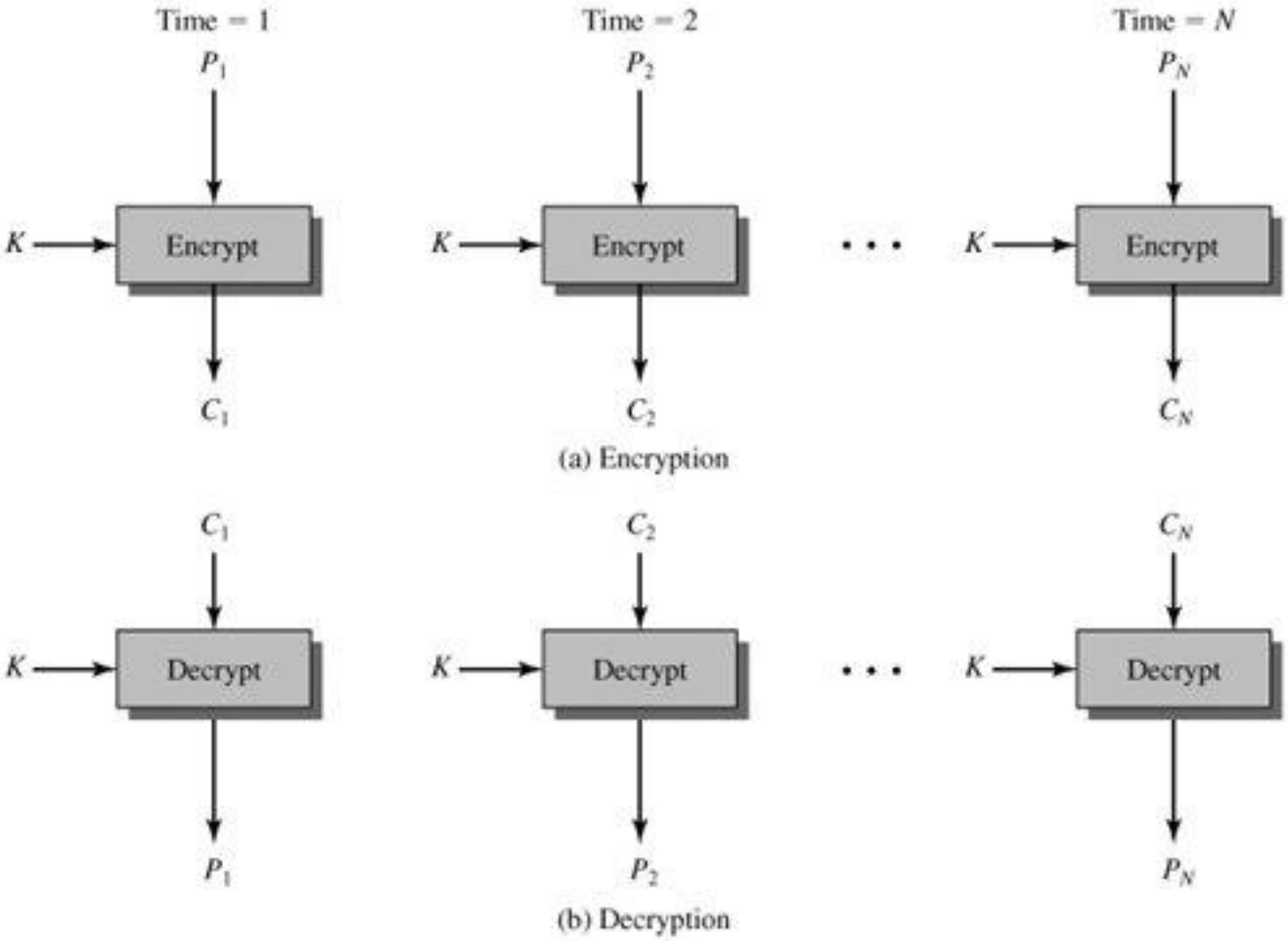
- Un modo de operación es una técnica para mejorar el efecto final de un algoritmo criptográfico
  - También se usa para adaptar el algoritmo a un tipo de aplicación concreta
- En ningún caso supone la modificación del algoritmo de cifrado en sí, sino de la forma en que se opera con los bloques de datos

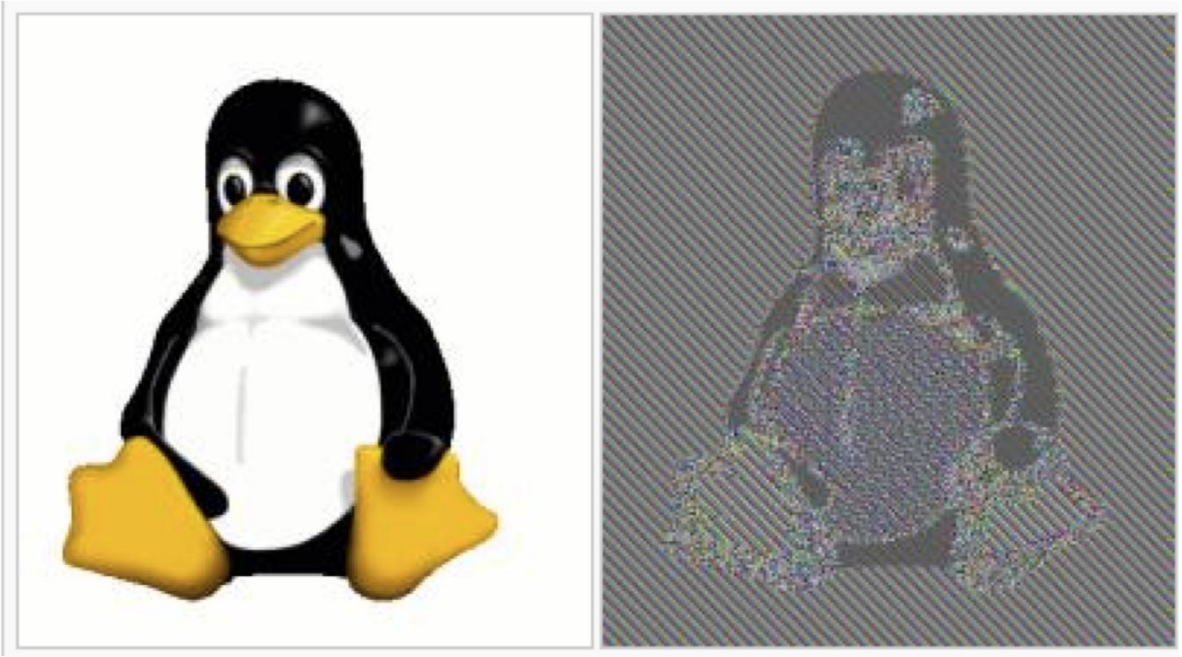


Modos de operación para algoritmos simétricos

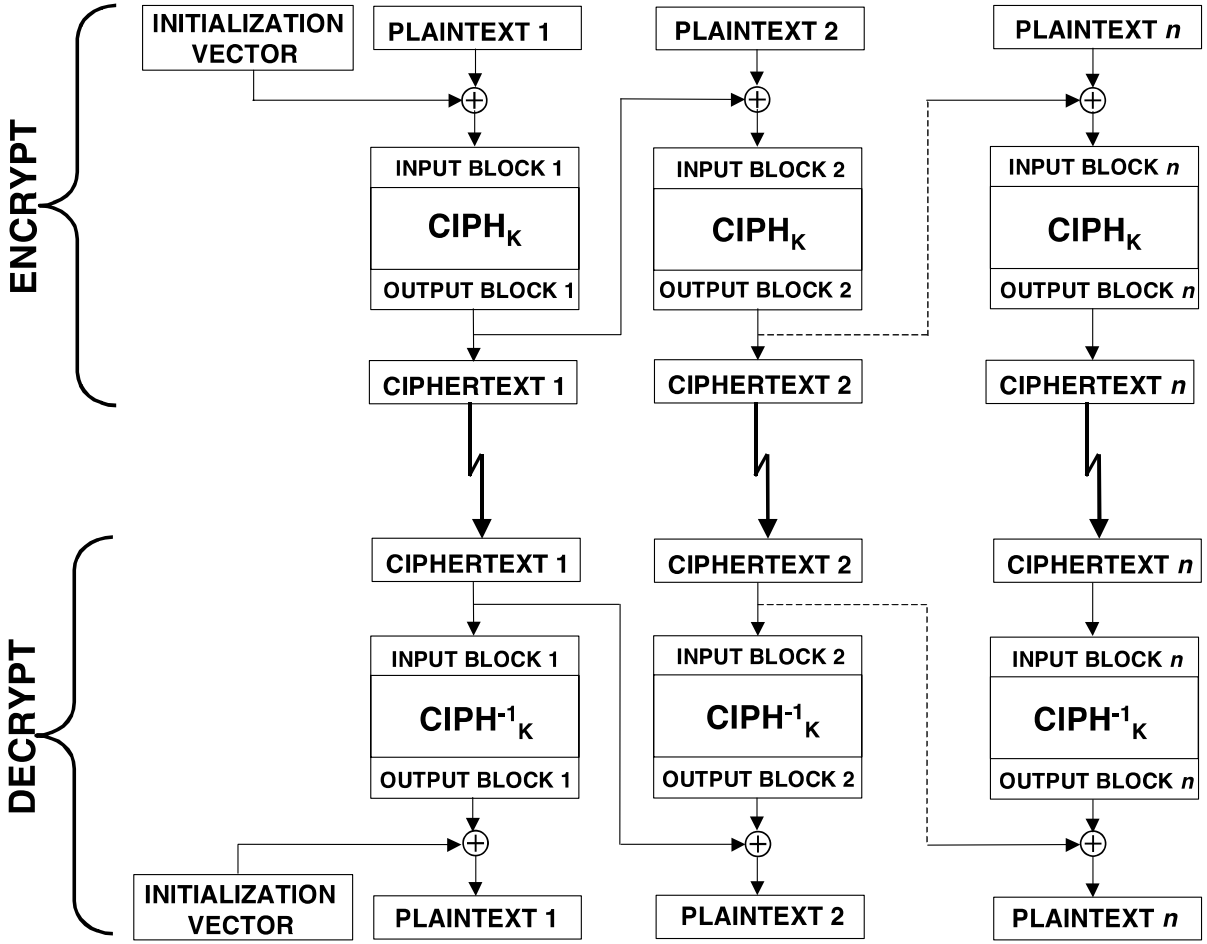
- Hay diferentes modos de operación, o lo que es lo mismo, diferentes formas de aplicar un mensaje *M* a un algoritmo de cifrado en bloque
  - cada una de ellas con sus ventajas y desventajas
- *NIST* ha definido cinco modos de operación, y cualquiera de ellos se puede utilizar con cualquier algoritmo simétrico (*DES*, *3DES*, *AES*, …)
  - Electronic Codebook (ECB)
  - Cipher Block Chaining (CBC)
  - Cipher Feedback (CFB)
  - Output Feedback (OFB)
  - Counter (CTR)
  - Galois-CTR (GCM)

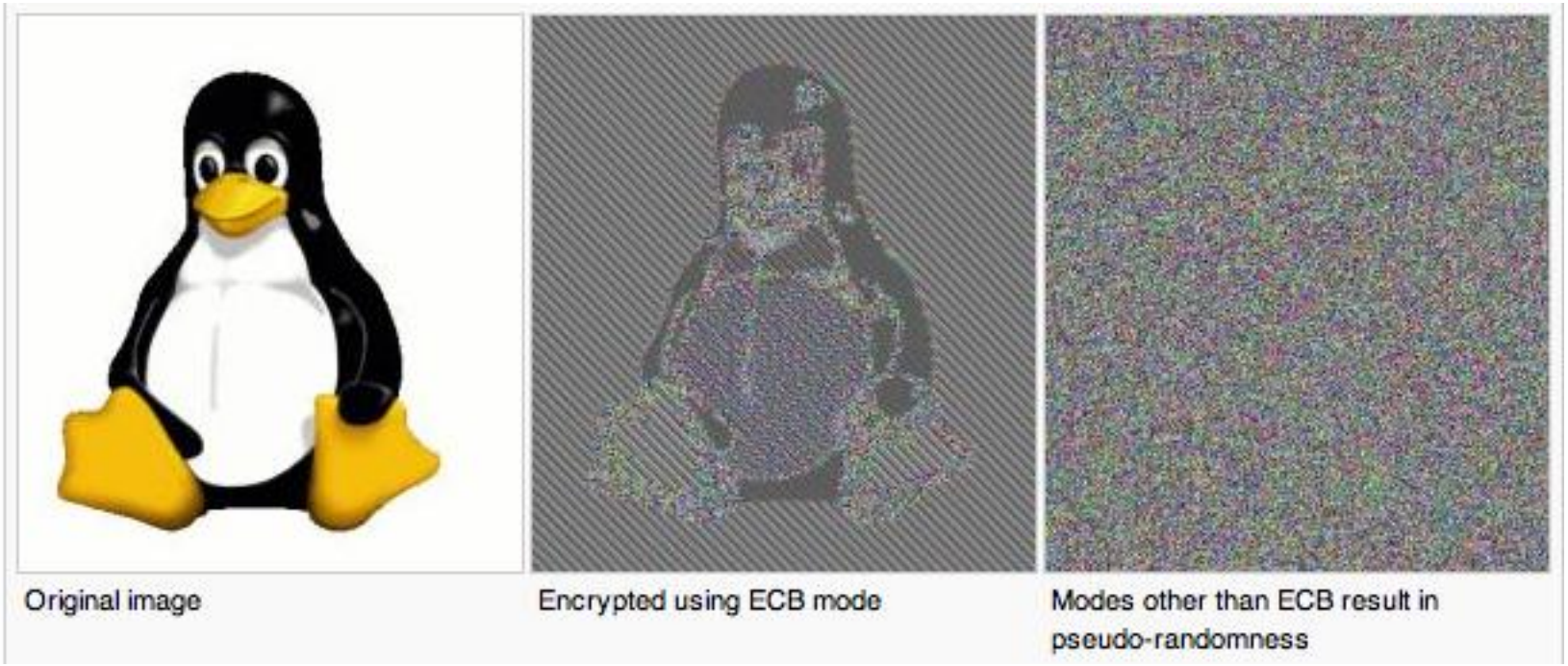
- Electronic Codebook (ECB)





- Cipher Block Chaining (CBC)



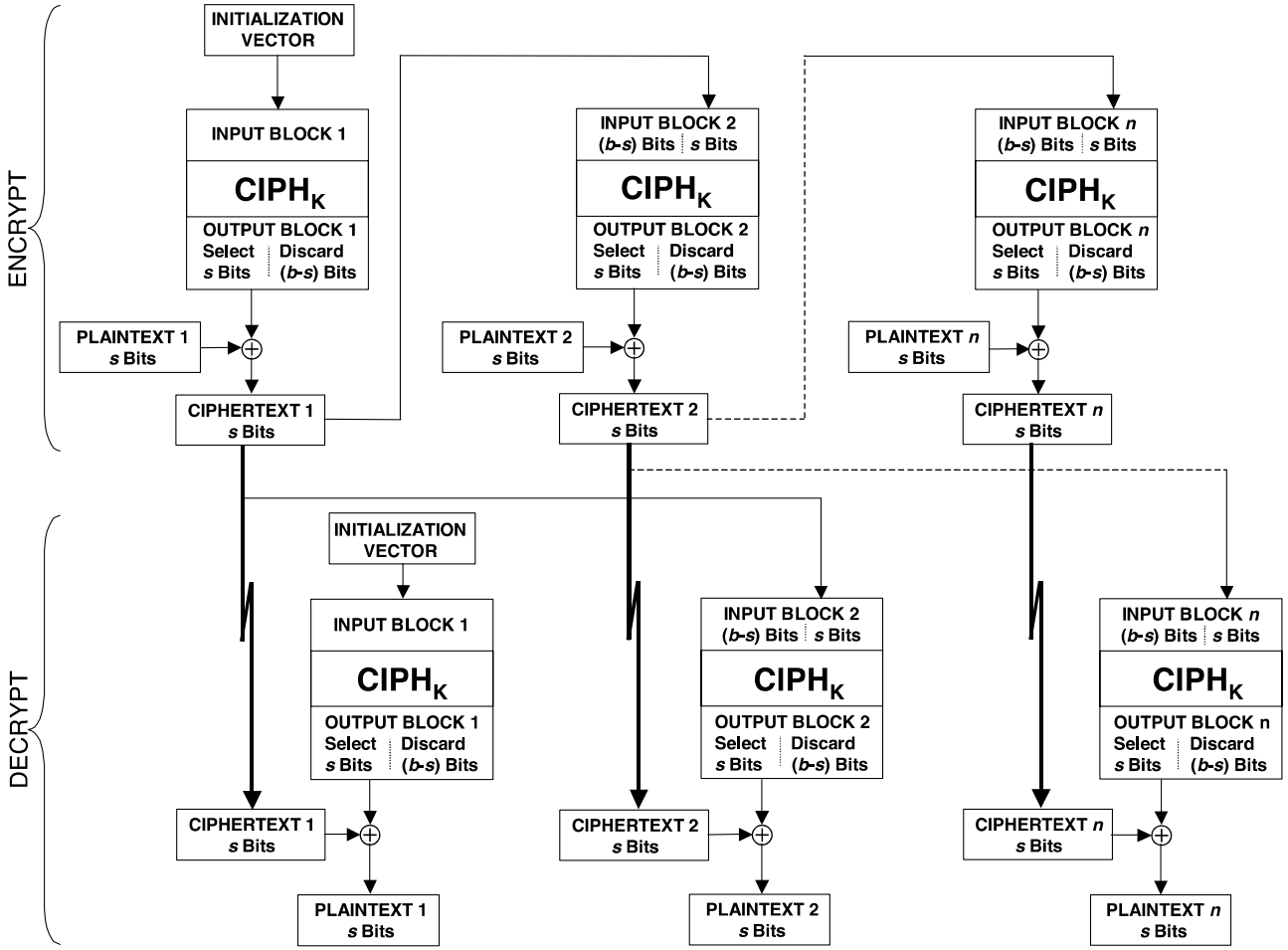


Original image

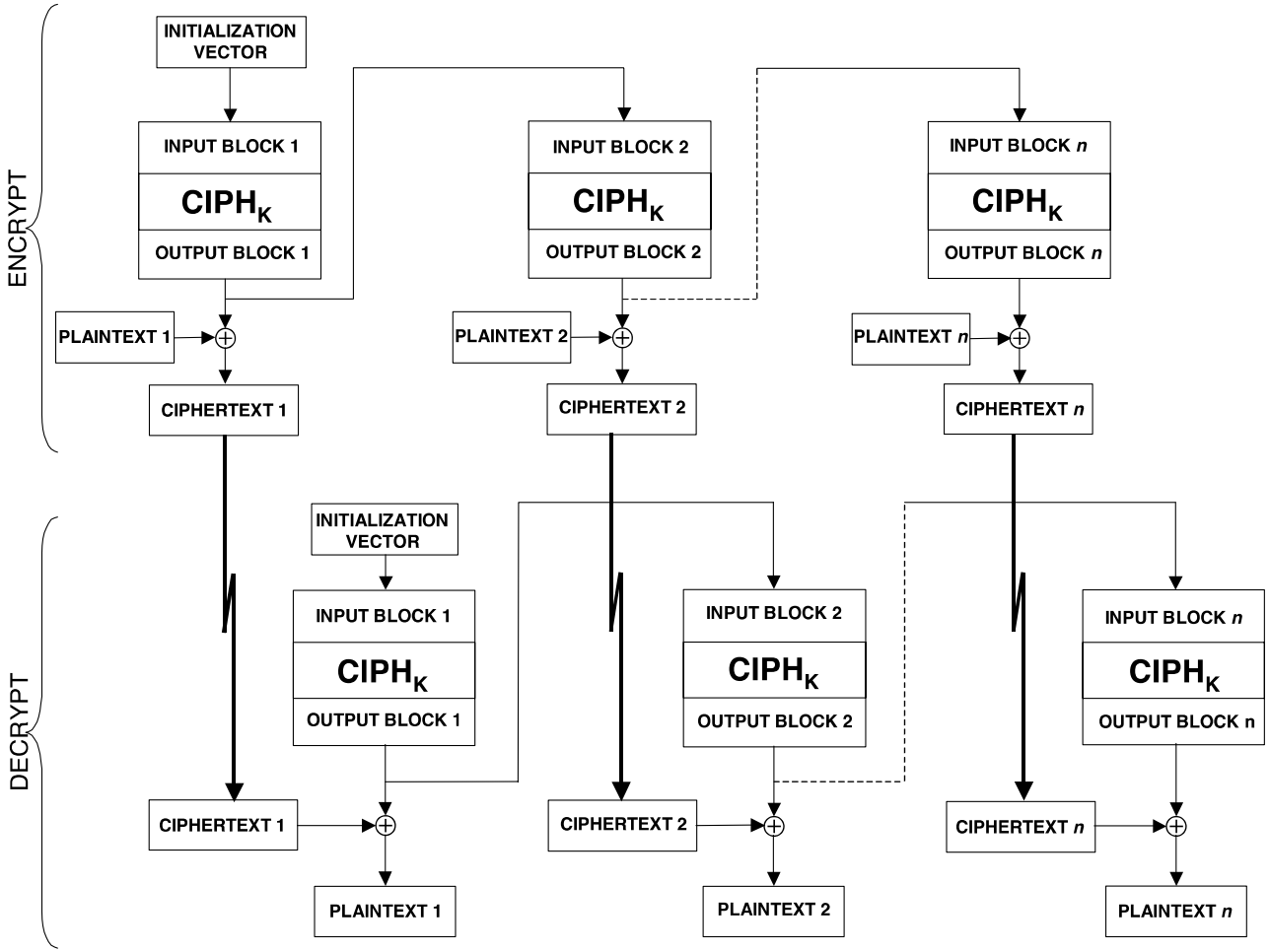
Encrypted using ECB mode

Modes other than ECB result in pseudo-randomness

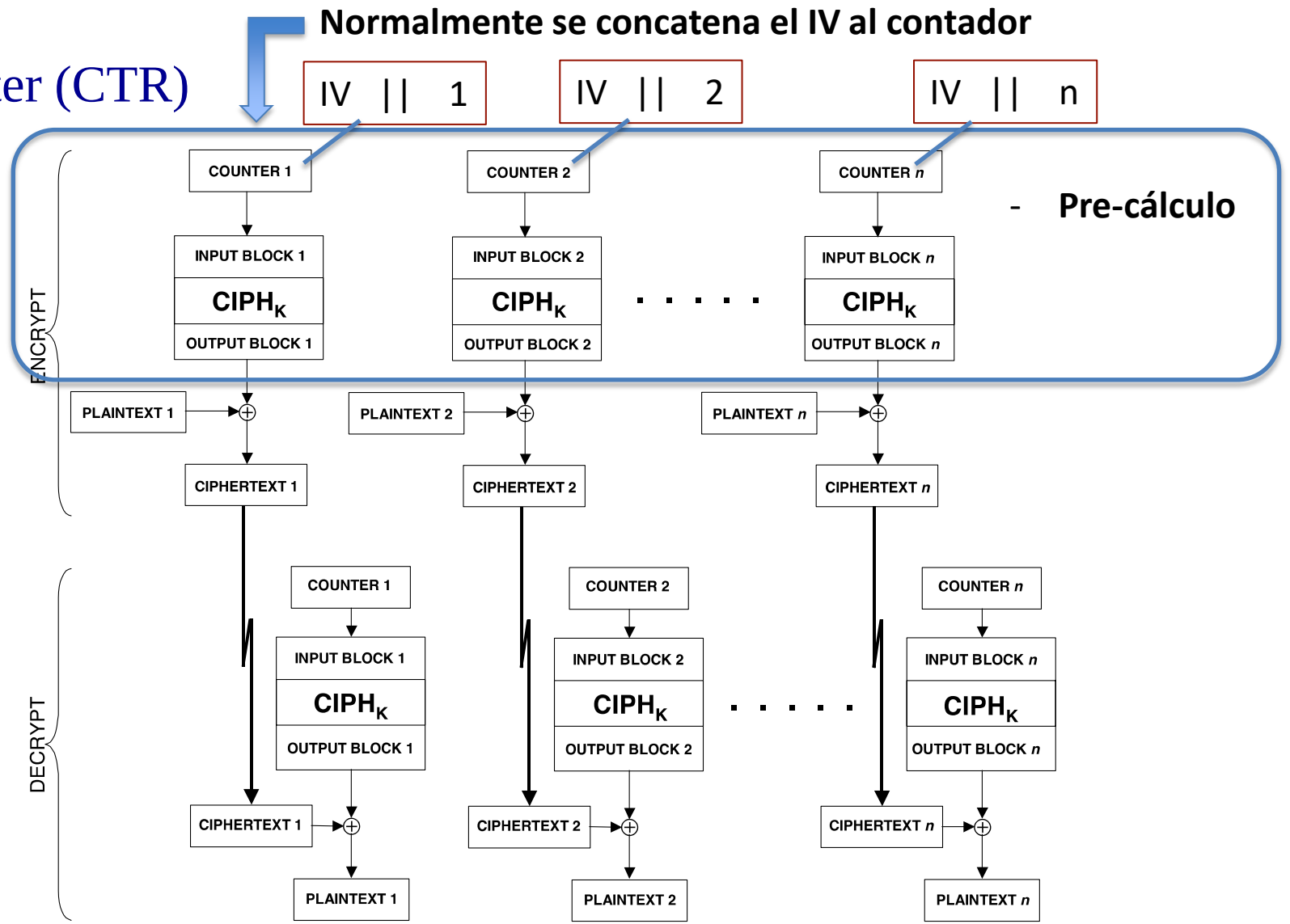
- Cipher Feedback (CFB)



- Output Feedback (OFB)



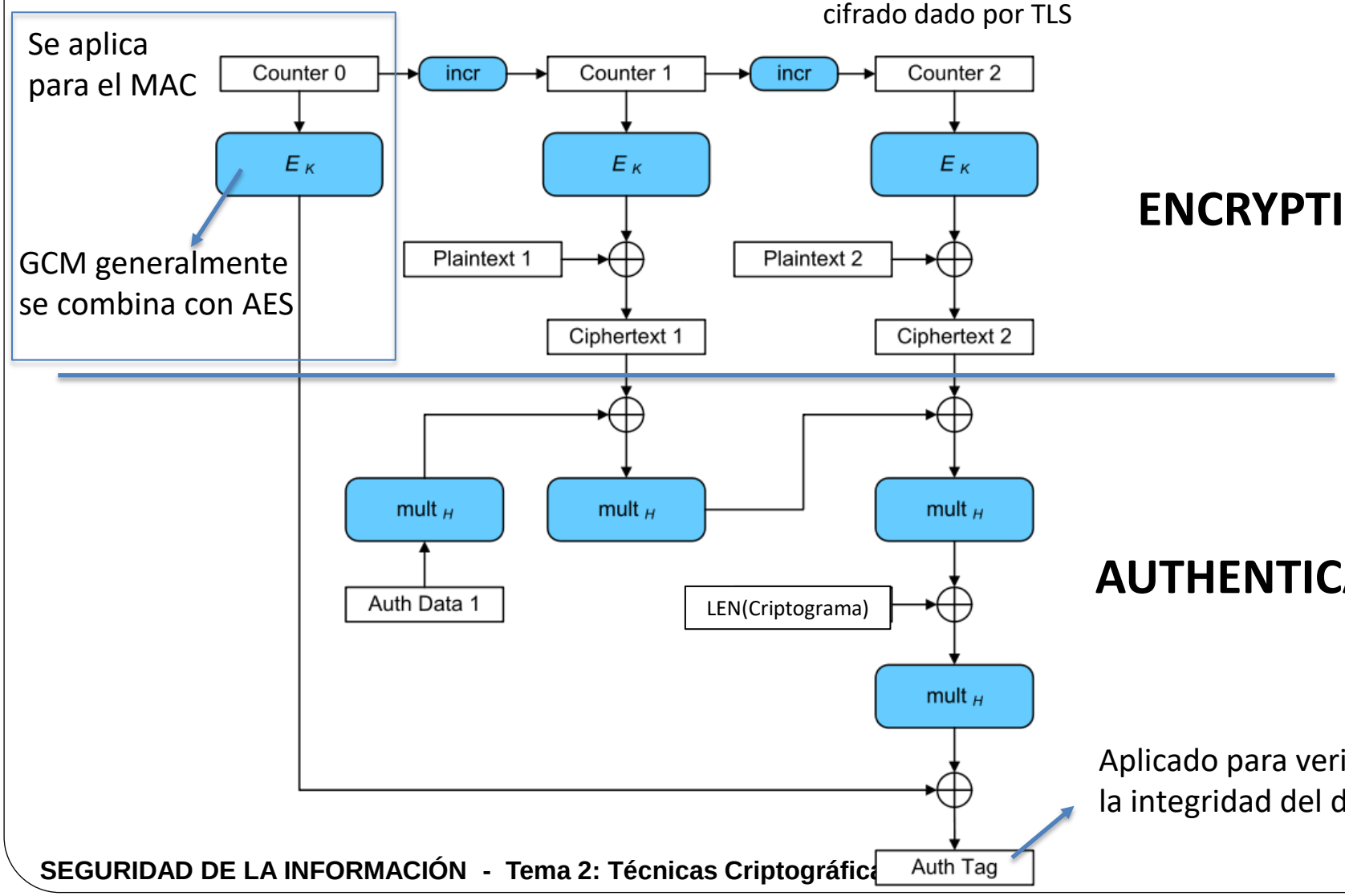
- Counter (CTR)


Normalmente se concatena el IV al contador
IV || 1
IV || 2
IV || n
COUNTER 1
COUNTER 2
COUNTER n
- Pre-cálculo
INPUT BLOCK 1
CIPH$_K$
OUTPUT BLOCK 1
INPUT BLOCK 2
CIPH$_K$
OUTPUT BLOCK 2
INPUT BLOCK n
CIPH$_K$
OUTPUT BLOCK n
ENCRYPT
PLAINTEXT 1
PLAINTEXT 2
PLAINTEXT n
CIPHERTEXT 1
CIPHERTEXT 2
CIPHERTEXT n
DECRYPT
COUNTER 1
COUNTER 2
COUNTER n
INPUT BLOCK 1
CIPH$_K$
OUTPUT BLOCK 1
INPUT BLOCK 2
CIPH$_K$
OUTPUT BLOCK 2
INPUT BLOCK n
CIPH$_K$
OUTPUT BLOCK n
CIPHERTEXT 1
CIPHERTEXT 2
CIPHERTEXT n
PLAINTEXT 1
PLAINTEXT 2
PLAINTEXT n

Extra: Modos de operación con integridad

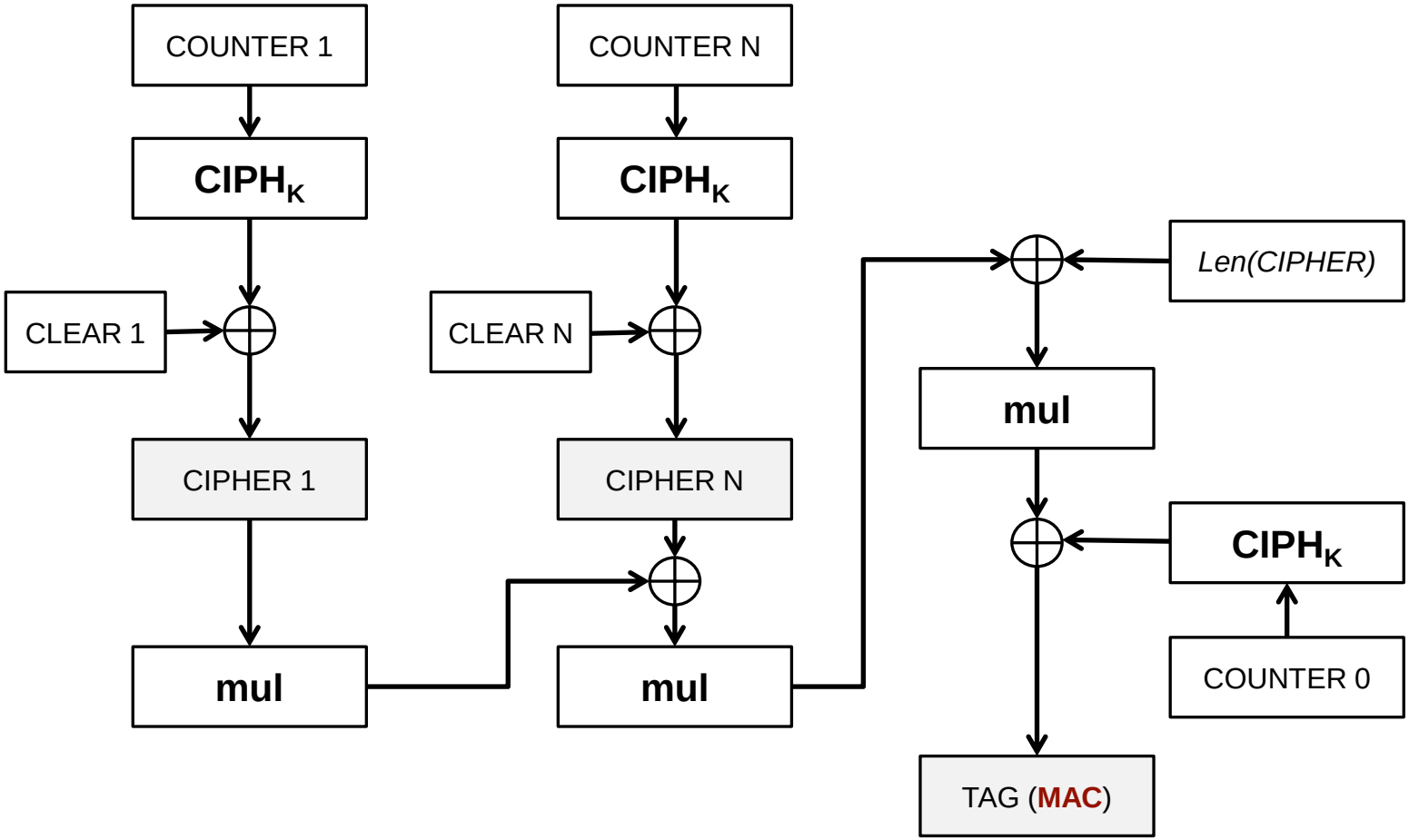
- Galois-CTR (GCM)

- Funciona de forma similar que el modo CRT pero usa Carter-Wegman **MAC** en un campo de Galois
- Es rápido y eficiente, y está soportado por el suite de cifrado dado por TLS



Extra: Modos de operación con integridad

- Galois-CTR (GCM)

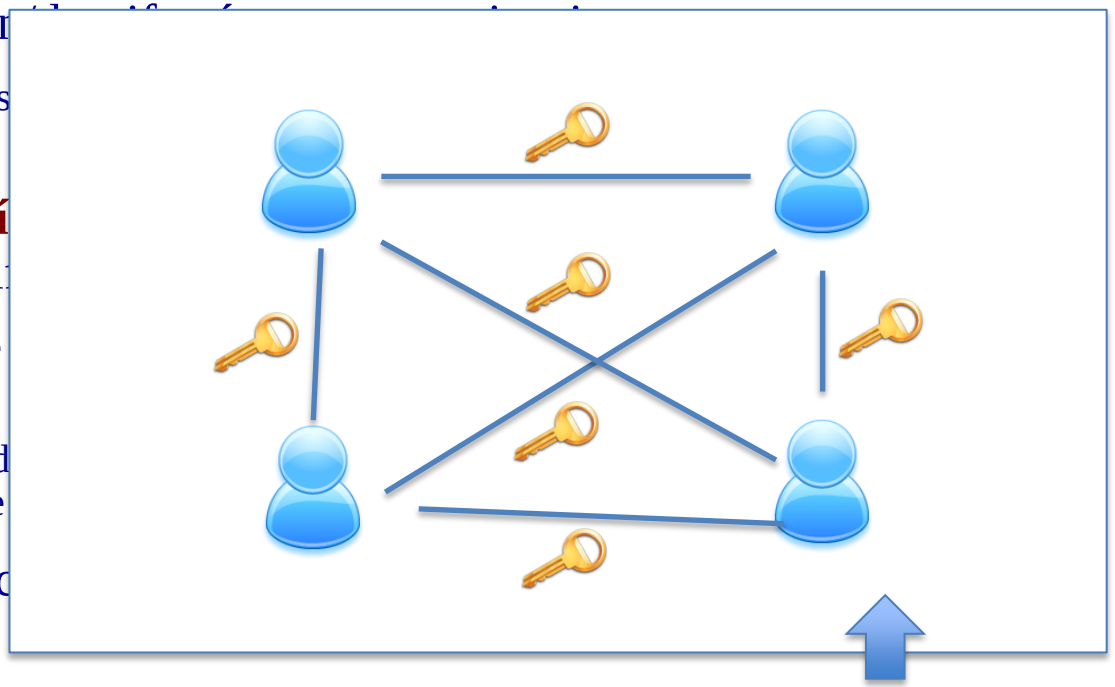


Ventajas y desventajas de los algoritmos simétricos

- **Ventajas**:
  - Los algoritmos simétricos se pueden diseñar para alcanzar un **alto rendimiento** (alto caudal de información cifrada)
    - En HW se pueden alcanzar del orden de cientos de Mbytes/sec
    - En SW se pueden alcanzar del orden Mbytes/sec
  - Se pueden **componer** para producir cifrados más fuertes
  - Se pueden utilizar como base para **construir otros mecanismos** criptográficos, como **funciones hash y generadores pseudoaletorios de números**
  - Los algoritmos simétricos necesitan **claves *K* relativamente cortas**

- **Desventajas**:
  - En una comunicación entre dos usuarios, estos han de **acordar, a priori, la clave K** con la que cifrarán/descifrarán sus comunicaciones
    - la clave ha de permanecer estrictamente en secreto, por lo que sólo la han conocer esos dos usuarios que se comunican
  - Si los dos usuarios están **físicamente lejanos** entre sí, acordar la clave puede convertirse en una tarea difícil
    - ¿qué medio suficientemente seguro habrán de utilizar si no es posible una reunión presencial entre ambos?
    - además, a efectos de seguridad, es recomendable que la clave *K* entre dos usuarios se cambie con cierta frecuencia, lo que complica el problema
  - En una red grande (de muchos usuarios) habrá demasiadas claves que administrar
    - Para una comunidad de *n* usuarios, el número de claves en el sistema será de ***(n * (n-1)) / 2***
      - Ej: 100 usuarios ➔ 4950 claves
    - Probablemente hará falta una **tercera parte confiable** para ayudar a los usuarios en las tareas de administración de claves

- Desventajas:
  - En una comunicación entre dos usuarios, estos han de **acordar, a priori, la clave K** con la que cifrará
    - la clave ha de permanecer es
      usuarios que se comunican
  - Si los dos usuarios están **fí**
    convertirse en una tarea di
    - ¿qué medio suficientemente
      entre ambos?
    - además, a efectos de segurid
      con cierta frecuencia, lo que
  - En una red grande (de muc
    administrar



    - Para una comunidad de *n* usuarios, el número de claves en el sistema será de ***(n * (n-1)) / 2***
      - Ej: 100 usuarios ➔ 4950 claves
    - Probablemente hará falta una **tercera parte confiable** para ayudar a los usuarios en las tareas de administración de claves