

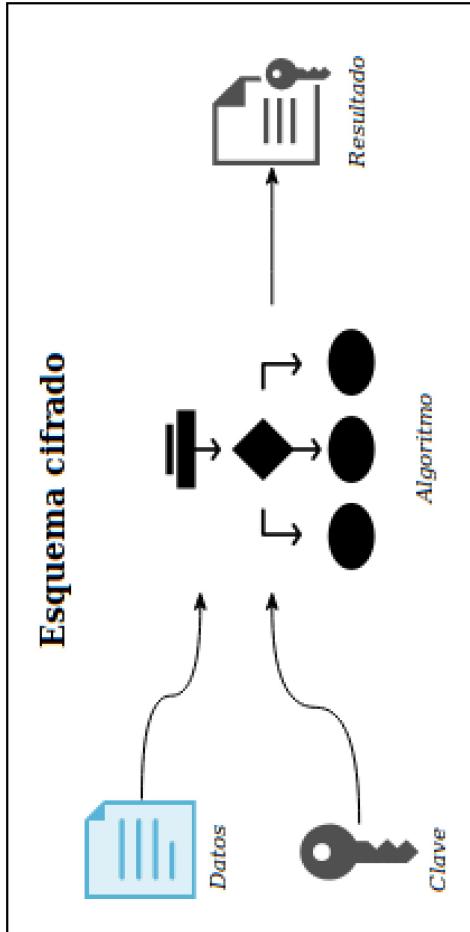
ÍNDICE

1. Introducción a la criptografía
2. Cifrado de clave simétrica
3. Cifrado de clave asimétrica
4. Algoritmo de cifrado hash
5. Sistemas híbridos



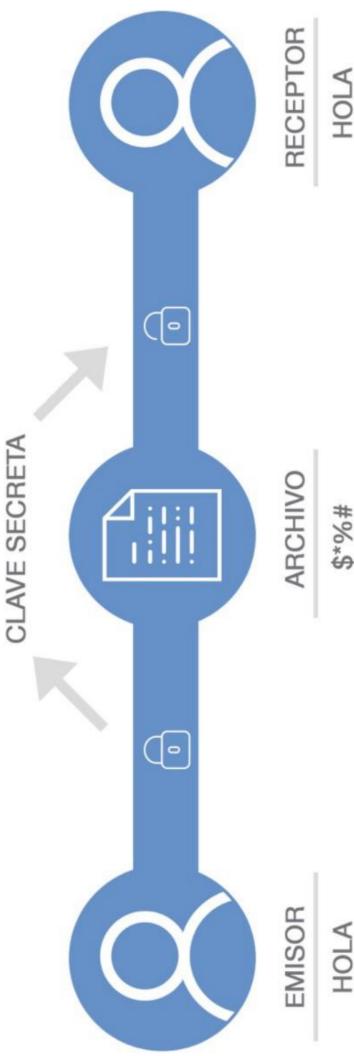
1. INTRODUCCIÓN A LA CRIPTOGRAFÍA

- Una medida que a tomar respecto a la consistencia de los datos es que estos sean indescifrables por personas que accedan a ellos indebidamente.
- **Cifrar:** transcribir, utilizando una clave, un mensaje cuyo contenido se quiere ocultar.
- **Clave:** conjunto de signos utilizados para la transmisión de un mensaje privado cuyo contenido se quiere ocultar.



1. INTRODUCCIÓN A LA CRIPTOGRAFÍA

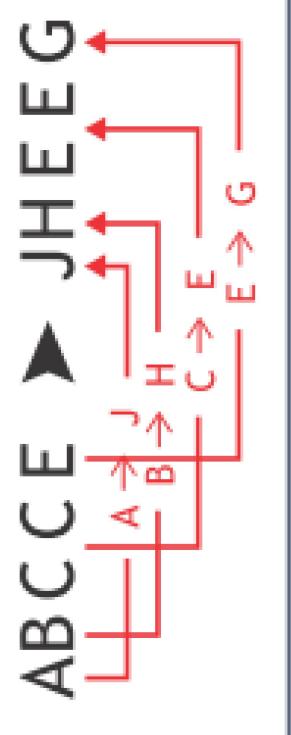
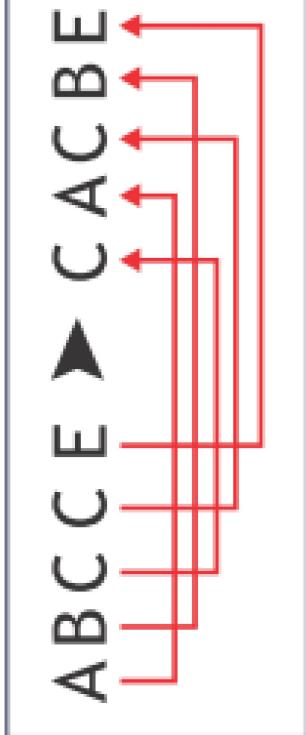
- La **criptografía** está integrada por las técnicas utilizadas para, utilizando una **clave**, convertir un mensaje inteligible (llamado **texto nativo**) en otro (**texto cifrado**), cuyo contenido solo puede ser comprendido por quienes **conozcan la clave**. Los **algoritmos de cifrado** son el método utilizado para ocultar el contenido del mensaje y el **criptosistema** es el conjunto de equipos y claves usados para cifrarlo.



1. INTRODUCCIÓN A LA CRIPTOGRAFÍA

Los sistemas criptográficos se basan en dos técnicas:

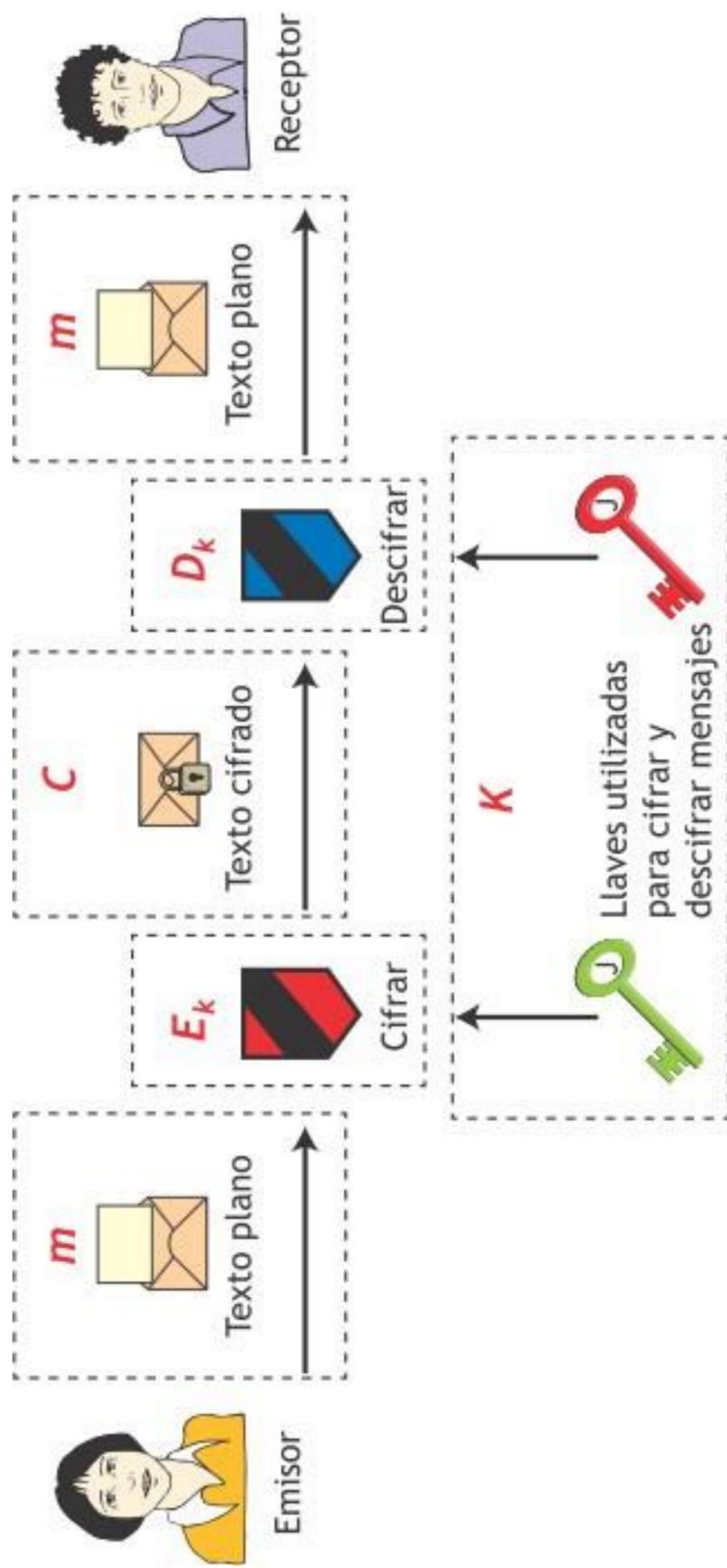
- **Transposición:** los signos o símbolos del mensaje original se cambian de posición.



1. INTRODUCCIÓN A LA CRIPTOGRAFÍA

- **Criptosistema:** según el Centro Criptológico Nacional (CCN), es el conjunto de claves y equipos de cifra que, utilizados coordinadamente, ofrecen un medio para cifrar y descifrar.
- **Los elementos de un criptosistema:**
 - **Mensajes sin cifrar,** texto plano o texto nativo (m): son los documentos originales sin haber sido cifrados.
 - **Mensajes cifrados (C)** o criptogramas.
 - **Conjunto de claves (K):** son los datos o llaves que permiten cifrar los mensajes.
- **Transformaciones de cifrado (E).**
- **Transformaciones de descifrado (D).**

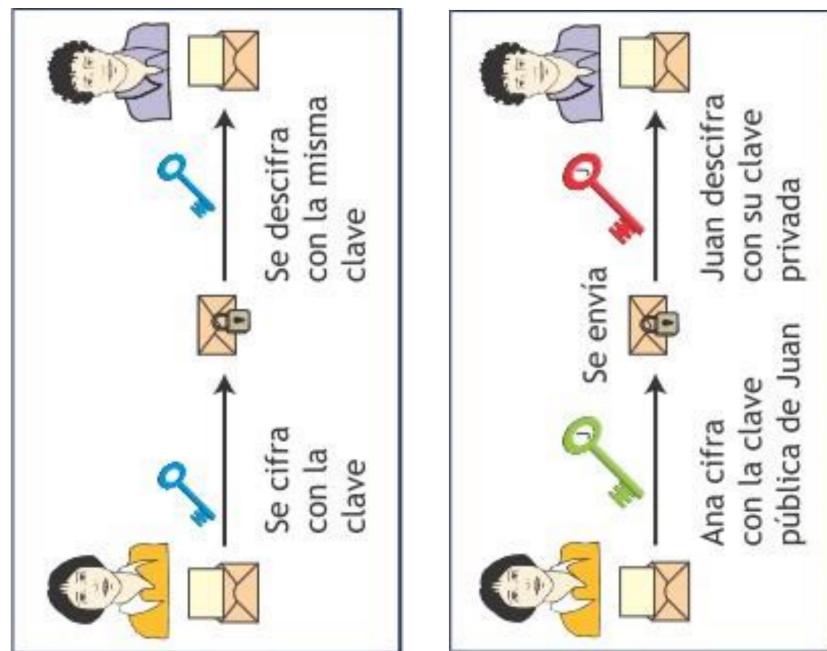
1. INTRODUCCIÓN A LA CRIPTOGRAFÍA



1. INTRODUCCIÓN A LA CRIPTOGRAFÍA

Tipos de sistemas de cifrado:

- **Criptosistemas simétricos o de clave secreta.** En estos sistemas existe una única clave secreta que conocen y comparten emisor y receptor y que es utilizada para cifrar y descifrar el mensaje. La seguridad de este tipo de sistemas consiste en mantener dicha clave en secreto.



- **Criptosistemas asimétricos o de clave pública.** En este tipo de sistemas cada usuario crea un par de claves inversas: una privada y otra pública. Lo que el emisor cifra con una clave, el receptor lo descifra con la clave inversa. La seguridad de este tipo de sistemas radica en la dificultad de averiguar la clave privada a partir de la pública.

2. CIFRADO DE CLAVE SIMÉTRICA

Estos sistemas son mucho más rápidos y sencillos de implementar que los de clave asimétrica y resultan apropiados para el **cifrado de grandes volúmenes de datos**. Hay dos grandes grupos de algoritmos de cifrado:

- **Cifradores de flujo:** cifran bit a bit.
- **Cifradores de bloque:** cifran un bloque de bits (habitualmente, cada bloque es de 64 bits) como una unidad.

Uno de los inconvenientes de este tipo de cifrado es que **la clave debe ser conocida por el emisor y el receptor**, quienes deben encontrar un modo seguro de comunicarla entre ambos.

2. CIFRADO DE CLAVE SIMÉTRICA

Se necesita una clave por cada par de usuarios, lo que hace crecer exponencialmente el número de claves según se van incrementando los usuarios. Existen dos fórmulas:

$$C_m^n = \frac{m!}{n!(m-n)!}$$

Para 5 usuarios sería:

$$\frac{5(5-1)}{2} = 10$$

$$C_5^2 = \frac{5!}{2!(5-2)!} = 10$$

$$\frac{n(n-1)}{2}$$

2. CIFRADO DE CLAVE SIMÉTRICA

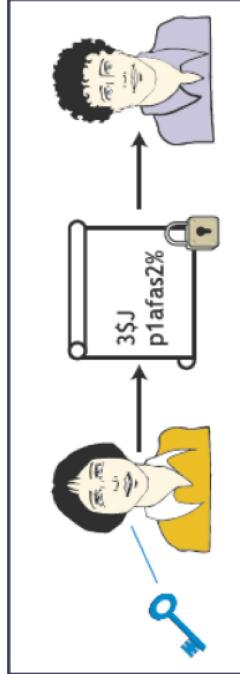
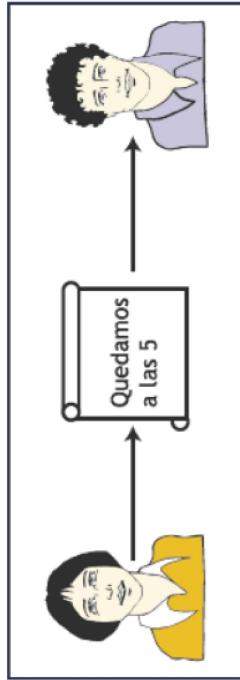
Hay dos sistemas para atacar un cifrado simétrico:

- **Criptoanálisis.** Se analiza el texto cifrado para intentar ser descifrado. En este tipo de ataque se aprovechan las características del algoritmo para intentar averiguar el texto originario o bien la clave secreta que se está utilizando. El peor resultado sería que el atacante descubriera la clave.
- **Método de fuerza bruta.** Consiste en probar todas y cada una de las posibles claves empleadas para cifrar el texto. Una vez que se haya encontrado la clave adecuada, ya se podrá descifrar el mensaje. La fortaleza del cifrado en casos de ataques por fuerza bruta depende de la complejidad de la clave.

2. CIFRADO DE CLAVE SIMÉTRICA

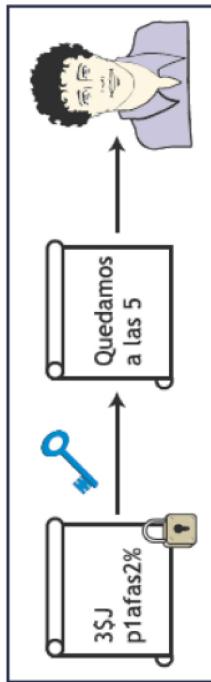
Utilización de clave simétrica:

Vamos a ver en un ejemplo el funcionamiento de la clave simétrica. Ana quiere enviar un mensaje a Juan y, como pretende que su contenido sea secreto, lo cifra utilizando una clave simétrica. Esta clave debe ser conocida tanto por Ana como por Juan.



Una vez que Ana ha utilizado la clave, el mensaje será indescifrable para todo el mundo excepto para Juan, que conoce la clave. ¿Qué pasa si una tercera persona intercepta el mensaje?

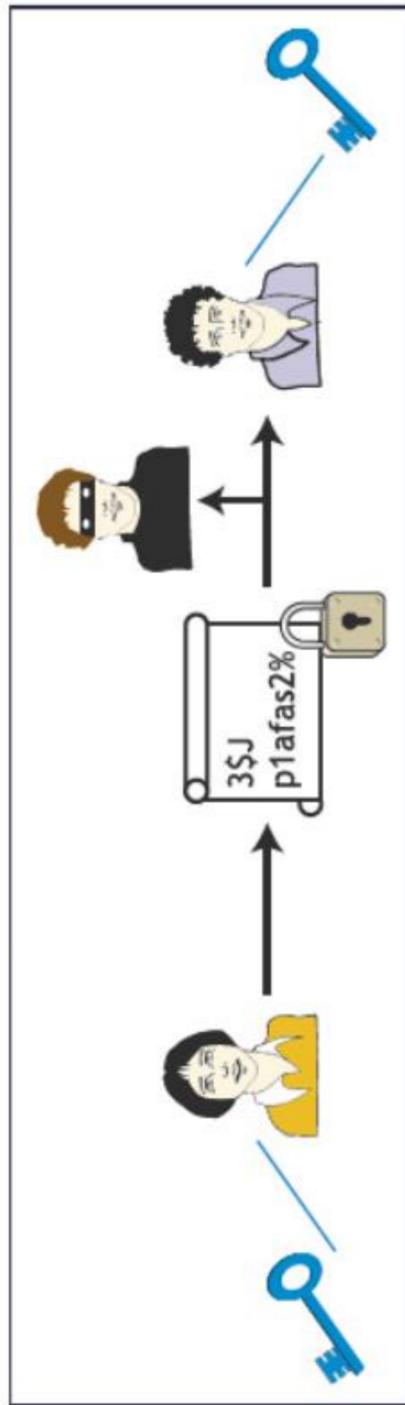
El mensaje solo puede descifrarse si se conoce la clave. En este caso, solo lo puede descifrar Juan, que es quien conoce la clave.



2. CIFRADO DE CLAVE SIMÉTRICA

Utilización de clave simétrica:

Si un intruso interceptase el mensaje, solo podría descifrarlo si conociera la clave compartida por Ana y Juan. Eso podría suceder si Ana o Juan no la guardaran adecuadamente o si hubieran fijado una clave no muy compleja, fácil de ser averiguada por ataques de fuerza bruta.



2. CIFRADO DE CLAVE SIMÉTRICA

Ventajas del cifrado por clave simétrica:

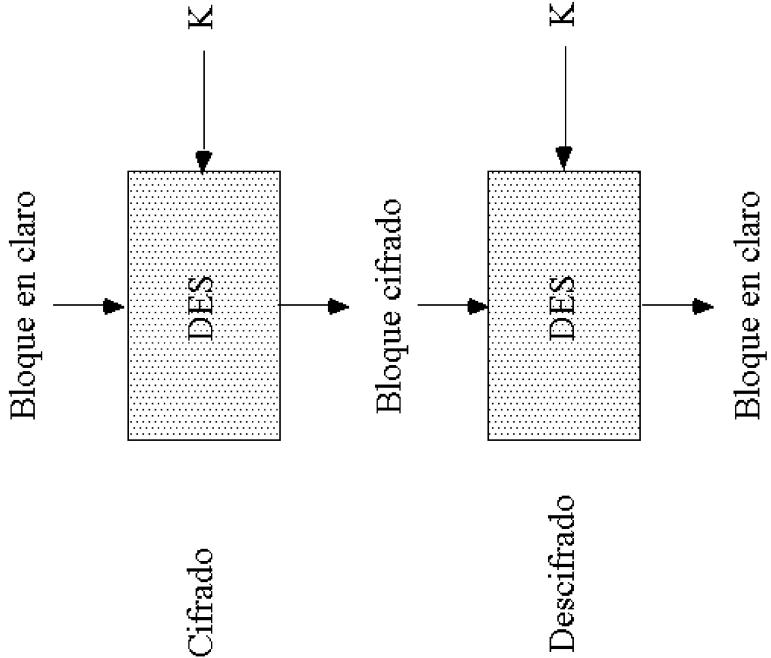
- Son rápidos y eficientes.
- Resultan apropiados para el cifrado de grandes volúmenes de datos.

Inconveniente del cifrado por clave simétrica:

- Exigen una clave diferente por cada pareja de interlocutores (el espacio de claves se incrementa enormemente conforme aumentan los interlocutores).
- Requiere un control estricto sobre el intercambio seguro de la clave entre el emisor y el receptor.
- Son vulnerables a ataques por fuerza bruta, por lo que la fortaleza de la clave es fundamental.

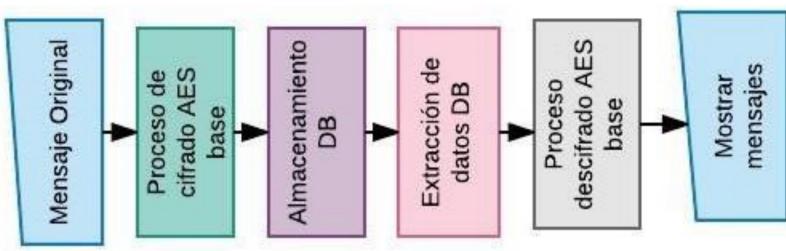
2. CIFRADO DE CLAVE SIMÉTRICA: ALGORITMOS DE CIFRADO

- **DES (Data Encryption Standard).** Utiliza cifrado por bloques de 64 bits, toma un texto plano de esa longitud y lo transforma, mediante una serie de operaciones, en texto cifrado de la misma longitud. De los 64 sólo se utilizan 56 bits, el resto para otras operaciones. Inseguro.



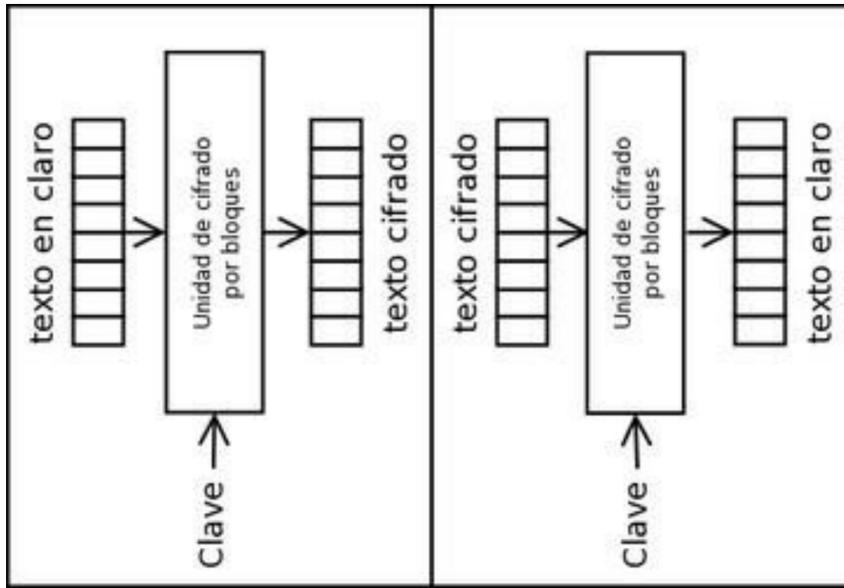
2. CIFRADO DE CLAVE SIMÉTRICA: ALGORITMOS DE CIFRADO

- **AES (Advanced Encryption Standard):** Es rápido y eficiente y proporciona una encriptación segura utilizando un **cifrado por bloques de 128 bits y claves de 128, 192 o 256 bits**. Se utiliza fundamentalmente en aplicaciones bancarias por Internet, comunicaciones inalámbricas, protección de datos en discos duros, etc.



2. CIFRADO DE CLAVE SIMÉTRICA: ALGORITMOS DE CIFRADO

- **RC5 (Rivest Cipher):** Se trata de un algoritmo que opera con un tamaño variable de bloques (32, 64 y 128 bits) y un número variable de claves (entre 0 y 2040 bits). Tiene las características de consumir poca memoria y de poder adaptarse a microprocesadores con distintos tamaños de palabra.



2. CIFRADO DE CLAVE SIMÉTRICA: ALGORITMOS DE CIFRADO

- IDEA (International Data Encryption Algorithm): Fue creado para remplazar al DES, este algoritmo trabaja en bloques de **64 bits** y utiliza **una clave de 128 bits**, lo que la hace inmune al criptoanálisis, e imposible de descifrar mediante fuerza bruta.

