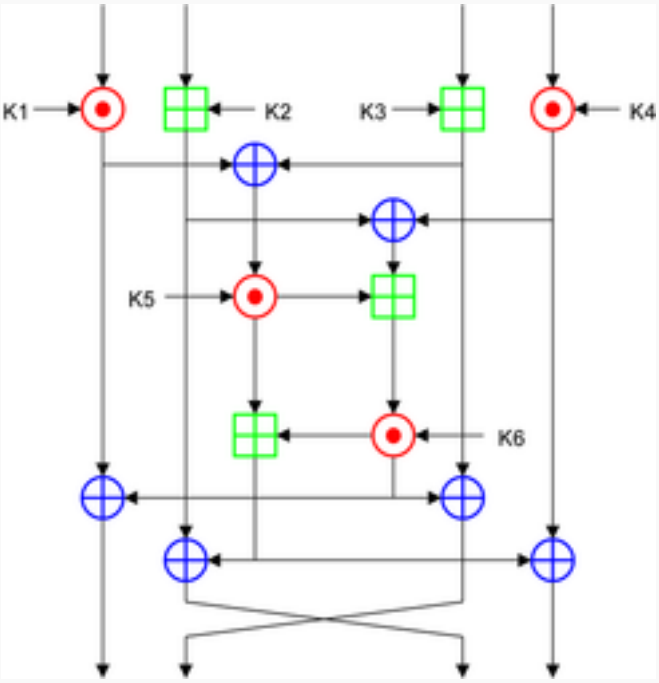
# International Data Encryption Algorithm

Ir a la navegaciónIr a la búsqueda

**IDEA**




Una ronda de cifrado de IDEA

| General | |
|---|---|
| **Diseñador(es)** | Xuejia Lai, James Massey |
| **1ª publicación** | 1991 |
| **Antecesor** | PES |
| **Sucesor** | MESH, Akelarre (cifrado), IDEA NXT (FOX) |
| **Detalle de cifrado** | |

| | |
|---|---|
| **Longitud de la clave** | 128 bits |
| **Longitud de bloque** | 64 bits |
| **Estructura** | Red de sustitución-permutación |
| **Mejor criptoanálisis público** | |
| La clave se puede recuperar con una complejidad computacional de $2^{126.1}$ utilizando Meet-in-the-middle con estructuras de grafos bipartitos completos. Este ataque es computacionalmente más rápido que un ataque de fuerza bruta completo, aunque no es factible computacionalmente.[1] | |
| [editar datos en Wikidata] | |

En criptografía, **International Data Encryption Algorithm** o **IDEA** (del inglés, *algoritmo internacional de cifrado de datos*) es un cifrador por bloques diseñado por Xuejia Lai y James L. Massey de la Escuela Politécnica Federal de Zúrich y descrito por primera vez en 1991. Fue un algoritmo propuesto como reemplazo del DES (Data Encryption Standard). IDEA fue una revisión menor de **PES** (Proposed Encryption Standard, del inglés *Estándar de Cifrado Propuesto*), un algoritmo de cifrado anterior. Originalmente IDEA había sido llamado **IPES** (Improved PES, del inglés *PES Mejorado*).

IDEA fue diseñado en contrato con la Fundación Hasler, la cual se hizo parte de Ascom-Tech AG. IDEA es libre para uso no comercial, aunque fue patentado y sus patentes vencieron en 2010 y 2011. El nombre "IDEA" es una marca registrada y está licenciado mundialmente por MediaCrypt.

IDEA fue utilizado como el cifrador simétrico en las primeras versiones de PGP (PGP v2.0) y se incorporó luego de que el cifrador original usado en la v1.0 ("Bass-O-Matic") se demostrara inseguro. Es un algoritmo opcional en OpenPGP.

Índice

## Funcionamiento[editar]

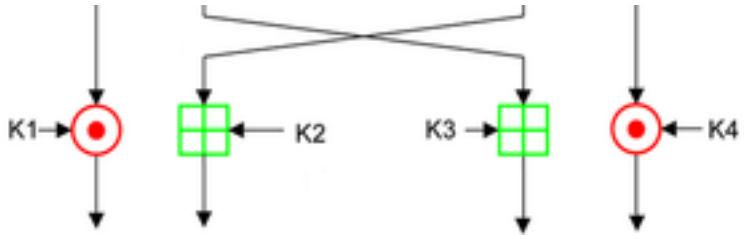
IDEA opera con bloques de 64 bits usando una clave de 128 bits y consiste de ocho transformaciones idénticas (cada una llamada un *ronda*) y una transformación de salida (llamada *media ronda*). El proceso para cifrar y descifrar es similar. Gran parte de la seguridad de IDEA deriva del intercalado de operaciones de distintos grupos — adición y multiplicación modular y O-exclusivo (XOR) bit a bit — que son algebraicamente "incompatibles" en cierta forma.

IDEA utiliza tres operaciones en su proceso con las cuales logra la confusión, se realizan con grupos de 16 bits y son:

- Operación O-exclusiva (XOR) bit a bit (indicada con un círculo plus azul⊕)
- Suma módulo $2^{16}$ (indicada con un caja plus verde⊞)
- Multiplicación módulo $2^{16}+1$, donde la palabra nula (0x0000) se interpreta como $2^{16}$ (indicada con un círculo punteado rojo⊙)

($2^{16} = 65536$; $2^{16}+1 = 65537$, que es primo)

Después de realizar 8 rondas completas viene una 'media ronda' y cuyo resultado es este:




Este algoritmo presenta, a primera vista, diferencias notables con el DES, que lo hacen más atractivo:

- El espacio de claves es mucho más grande: $2^{128} \approx 3.4 \times 10^{38}$
- Todas las operaciones son algebraicas
- Es más eficiente que los algoritmos de tipo Feistel, porque a cada vuelta se modifican todos los bits de bloque y no solamente la mitad.
- Se pueden utilizar todos los modos de operación definidos para el DES

## Seguridad[editar]

En primer lugar, el ataque por fuerza bruta resulta impracticable, ya que sería necesario probar $10^{38}$ claves, cantidad imposible de manejar con los medios informáticos actuales.

Los diseñadores analizaron IDEA para medir su fortaleza frente al criptoanálisis diferencial y concluyeron que es inmune bajo ciertos supuestos. No se han informado de debilidades frente al criptoanálisis lineal o algebraico. Se han encontrado algunas claves débiles, las cuales en la práctica son poco usadas siendo necesario evitarlas explícitamente.

En 2011, el IDEA de 8,5 rondas se rompió mediante un ataque Meet-in-the-middle. Independientemente, en 2012 se rompió utilizando otra variante de Meet-in-the-middle, usando una estructura de grafo bipartitos completos, con una reducción de la fuerza criptográfica de aproximadamente 2 bits; sin embargo, este ataque no amenaza, en la práctica, la seguridad de IDEA.[1]