*Marco Ramirez*

*[Company Name] | [Company Address]*

*[Document Title]*

*[Document Subtitle]*

Table of Contents

**No table of contents entries found.**

# Algoritmo Data Encription Standard (DES)

Es un algoritmo de cifrado histórico que jugó un papel crucial en la seguridad de la información. Aunque ya no se considera seguro para muchos estándares actuales, su estudio proporciona una comprensión de los principios básicos de la criptografía simétrica. Se desglosará visualmente cómo DES transforma texto plano en texto cifrado a través de una serie de operaciones estructuradas.

DES es un cifrador de bloque que utiliza una clave de 56 bits para cifrar y descifrar datos en bloques de 64 bits. A pesar de que la clave inicial es de 64 bits, se descartan 8 bits para obtener la clave de cifrado de 56 bits. Este proceso utiliza dos principios fundamentales de la criptografía: la sustitución y la transposición, ejecutados a través de 16 rondas.

## Fases del cifrado DES

### Permutación Inicial (IP)

Al principio, el bloque de texto plano de 64 bits se somete a una permutación inicial. Esta etapa reorganiza los bits del texto plano según un patrón predefinido, dividiendo el resultado en dos mitades de 32 bits cada una, conocidas como Texto Plano Izquierdo (LPT) y Texto Plano Derecho (RPT).

#### Rondas de cifrado

Cada una de las 16 rondas de DES incluye los siguientes pasos:

1. **Transformación de la clave:** La clave de 56 bits se divide y se somete a un desplazamiento circular, y después se seleccionan 48 de los 56 bits para formar la subclave de la ronda.
2. **Permutación de expansión:** El RPT se expande de 32 a 48 bits para alinearse con la longitud de la subclave.
3. **Substitución y mezcla de bits (S-Boxes):** La salida de la expansión se combina con la subclave mediante una operación XOR, y el resultado se procesa a través de las S-Boxes que sustituyen bits específicos basados en un conjunto de tablas predefinidas.
4. **Permutación:** Después de la sustitución, los bits se permutan nuevamente antes de fusionarse con el LPT de la ronda anterior para formar el nuevo RPT.

**Permutación Final (FP)**

Después de las 16 rondas, las mitades LPT y RPT se recombinan y se someten a una permutación final que produce el bloque de texto cifrado de 64 bits.

## Diagrama de flujo DESA diagram of a process Description automatically generated

Imagen No.1 Diagrama de flujo algoritmo DES

## Vulnerabilidad ante ataques de fuerza bruta

A pesar de su uso extendido, el DES ha demostrado ser vulnerable frente a ataques de fuerza bruta. Este tipo de ataque implica probar sistemáticamente todas las posibles combinaciones de claves hasta encontrar aquella que descifra correctamente el mensaje cifrado. La clave de 56 bits de DES, que inicialmente ofrecía 256256 combinaciones posibles, parecía suficiente durante la década de 1970. Sin embargo, con los avances tecnológicos y el aumento exponencial en la capacidad de procesamiento de computadoras, el DES comenzó a ser considerado como insuficiente en términos de seguridad.

# Resultados

## Pruebas fáciles

**Texto de prueba:** Hola

**Clave:** 123

### Secuencial

Key: 122

Encrypted text: �lK���&v

Decrypted text: Hola

Time to decrypt: 0.000022 seconds

### Paralelo

Key: 122

Encrypted text: ���6�?

=��=v

Decrypted text: Hola

Time to decrypt: 0.000587 seconds