Análisis Comparativo de Algoritmos de Criptografía Ligera

Kevin Arturo Amaya Osorio

Universidad Nacional de Colombia

kaamayao@unal.edu.co

December 5, 2025

¿Qué es la Criptografía Ligera?

Definición

La **criptografía ligera** (Lightweight Cryptography) es una rama de la criptografía que diseña algoritmos optimizados para dispositivos con recursos limitados.

Características principales:

- Bajo consumo de memoria (RAM y ROM)
- Menor consumo energético
- Implementaciones compactas en hardware
- Adecuada para IoT, RFID, sensores y sistemas embebidos

Cifrado Simétrico y Cifrado de Bloque

Cifrado Simétrico

Un esquema de cifrado simétrico es una tupla $(\mathcal{K}, \mathcal{M}, \mathcal{C}, E, D)$ donde:

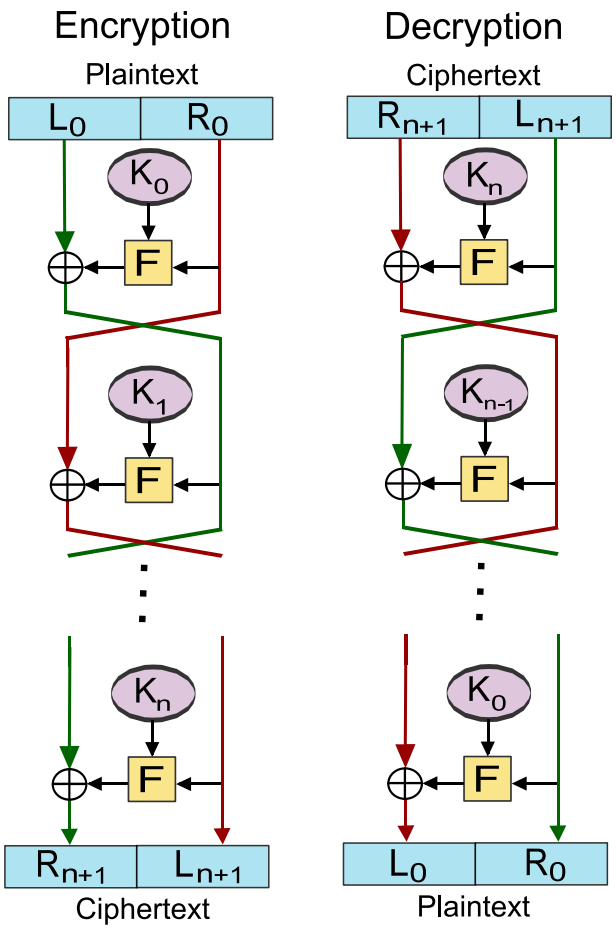
- $\mathcal{K}$ es el espacio de claves, $\mathcal{M}$ el espacio de mensajes, $\mathcal{C}$ el espacio de textos cifrados
- $E : \mathcal{K} \times \mathcal{M} \to \mathcal{C}$ es la función de cifrado
- $D : \mathcal{K} \times \mathcal{C} \to \mathcal{M}$ es la función de descifrado
- $\forall k \in \mathcal{K}, \forall m \in \mathcal{M} : D(k, E(k, m)) = m$

Cifrado de Bloque

Es un cifrado simétrico donde $\mathcal{M} = \mathcal{C} = \{0,1\}^n$ para un tamaño de bloque n fijo.

- $E_k : \{0,1\}^n \to \{0,1\}^n$ es una permutación (biyección)
- Para cada clave k, existe $E_k^{-1} = D_k$
- Tamaños típicos: $n = 64$ (DES, PRESENT) o $n = 128$ (AES)

Estructura: Red de Feistel



Funcionamiento:

- Divide el bloque en dos mitades (L, R)
- Aplica función F con subclave en cada ronda
- Resultado se XOR con la otra mitad
- Las mitades se intercambian

Ventaja clave:

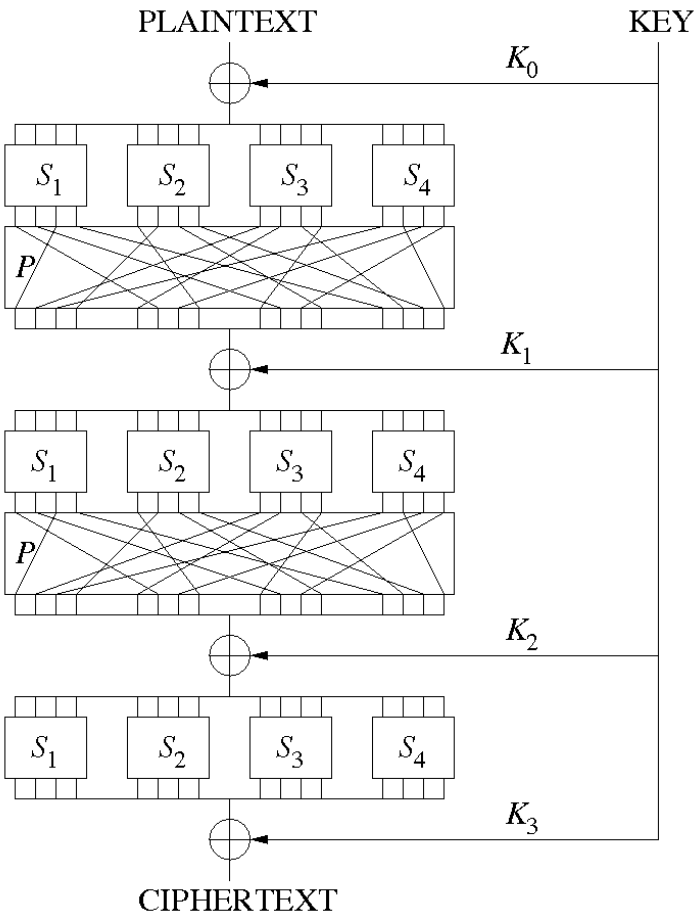
- El mismo circuito sirve para cifrar y descifrar

Usado en: DES, 3DES, Blowfish, Twofish

Seguridad

Teorema de Luby-Rackoff (1988)

Estructura: Red de Sustitución-Permutación (SPN)



Componentes:

- **S-box**: Sustitución no lineal (confusión)
- **P-box**: Permutación de bits (difusión)
- **Key mixing**: XOR con subclave de ronda

Ventaja clave:

- Alta paralelización en hardware
- Mayor velocidad en implementaciones optimizadas

Usado en: AES, PRESENT, SHARK

Seguridad

Wide Trail Strategy (Daemen-Rijmen, 2001)

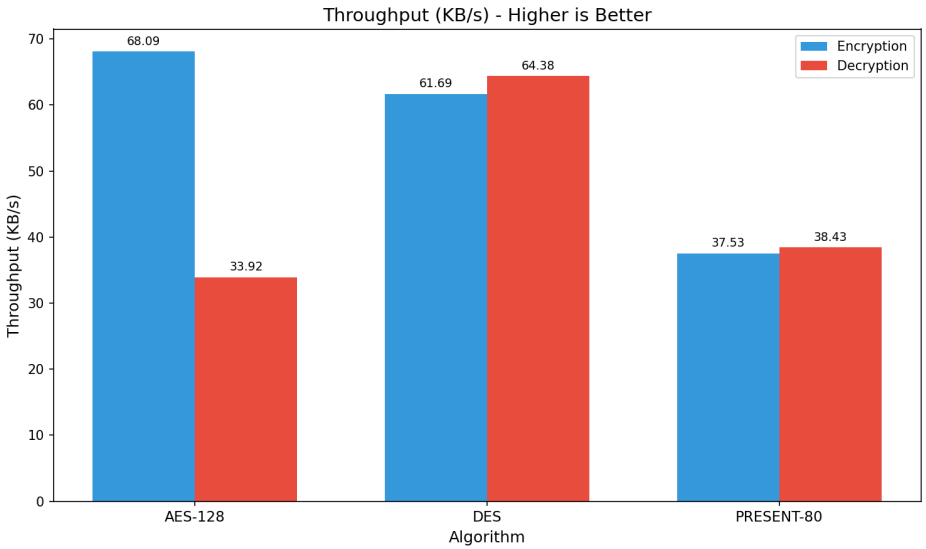
Los Tres Algoritmos Evaluados

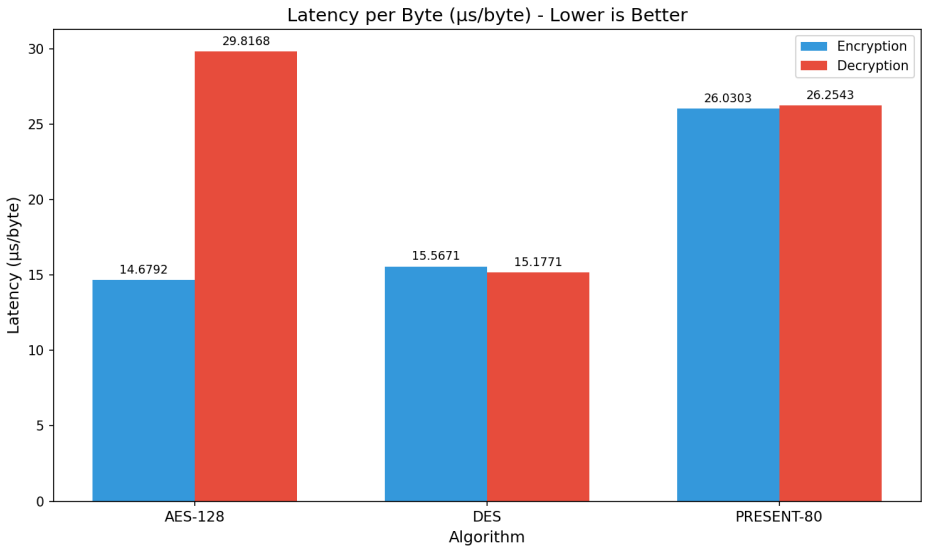
DES (1977)	AES-128 (2001)	PRESENT (2007)
IBM + NSA	Competencia NIST	Orange Labs + Uni
Red de Feistel	Red SPN	Red SPN
Clave: 56 bits	Clave: 128 bits	Clave: 80 bits
Bloque: 64 bits	Bloque: 128 bits	Bloque: 64 bits
16 rondas	10 rondas	31 rondas
Roto en 22h (1999)	Estándar actual	1570 GE (ultra-ligero)

Aplicaciones:

- **DES**: Cajeros ATM legacy, tarjetas EMV antiguas (deprecado)
- **AES**: WiFi, HTTPS, WhatsApp, BitLocker, aceleración AES-NI
- **PRESENT**: ISO/IEC 29192-2, influenció ASCON (NIST 2023)

Resultados: Rendimiento y Latencia

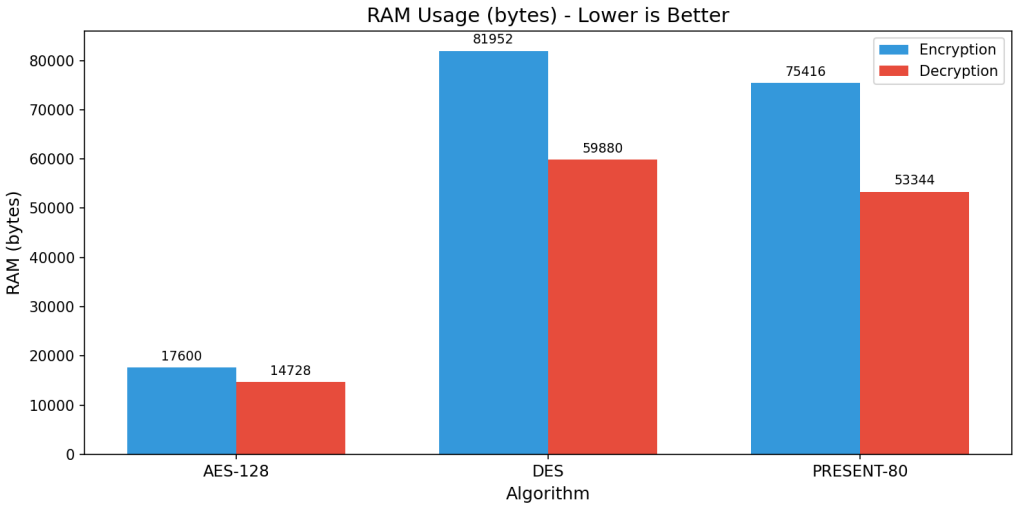


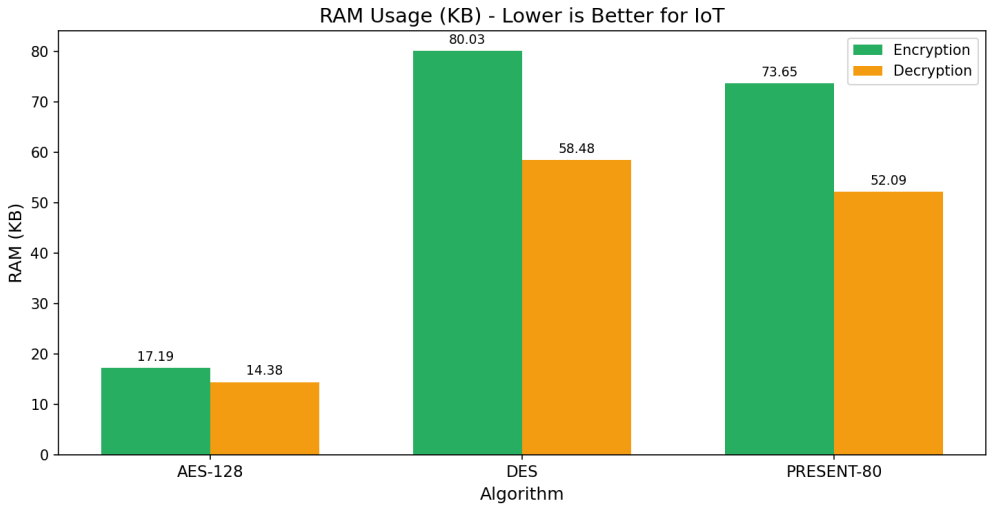


Observaciones:

- **AES-128**: 68 KB/s cifrado — El más rápido en software
- **DES**: 63 KB/s — Balanceado cifrado/descifrado
- **PRESENT**: 38 KB/s — Diseñado para hardware, no software
- En hardware dedicado, PRESENT sería más competitivo

Resultados: Memoria RAM





Memoria pico durante cifrado:

- **AES-128**: 17 KB
- **PRESENT**: 74 KB
- **DES**: 80 KB

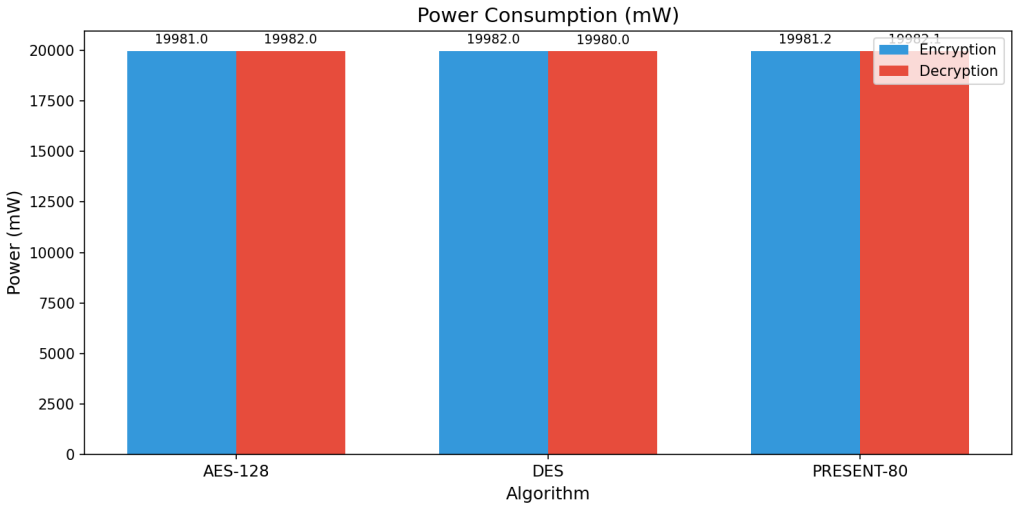
¿Por qué importa?

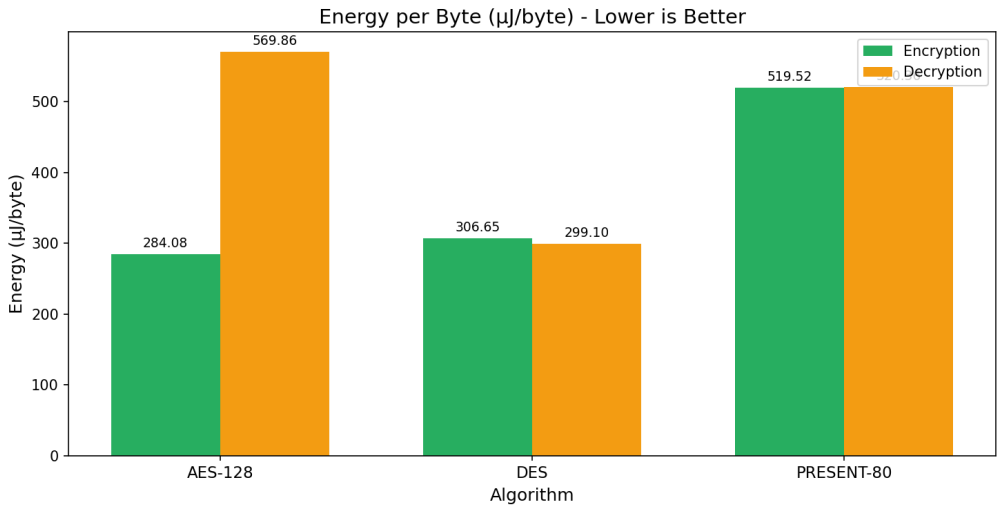
- MSP430: 512 bytes RAM
- ATtiny85: 512 bytes RAM
- ESP8266: 80 KB RAM

Nota

Implementación Python. En C/ASM los valores serían menores.

Resultados: Consumo Energético





Métricas:

- Potencia (mW): similar entre los tres
- Energía por byte (µJ/byte): varía significativamente

Implicaciones para IoT:

- Menor energía/byte = Mayor duración de batería
- Sensores remotos: años sin recargar
- PRESENT optimizado para eficiencia en hardware

Seguridad: Ataques Conocidos

Algoritmo	Mejor Ataque	Complejidad	¿Práctico?
DES	Fuerza bruta	2^{56}	Sí (horas)
AES-128	Biclique	$2^{126.1}$	No
PRESENT-80	Fuerza bruta	2^{80}	No (aún)

Contexto:

- **DES**: EFF lo rompió en 1998 con hardware de $250,000 USD
- **AES-128**: Biclique reduce de 2^{128} a $2^{126.1}$ — aún impracticable
- **PRESENT-80**: 80 bits es adecuado para IoT de corta vida, pero no para datos de largo plazo

Conclusiones: ¿Cuál Elegir?

Algoritmo	Throughput	RAM	Seguridad	Recomendación
DES	63 KB/s	80 KB	Obsoleto	No usar
AES-128	68 KB/s	17 KB	Excelente	Uso general
PRESENT-80	38 KB/s	74 KB	Adecuado	IoT restringido

Recomendaciones

- **DES**: Solo valor histórico/educativo. Deprecado desde 2005.
- **AES-128**: Opción por defecto. Si tienes AES-NI, úsalo.
- **PRESENT-80**: Para RFID, sensores desechables, smart dust.

El Futuro: ASCON

NIST estandarizó **ASCON** en 2023 para criptografía ligera autenticada. Hereda ideas de PRESENT.

Mensaje Final

La criptografía ligera no es simplemente hacer algoritmos más pequeños.

Es el arte de encontrar el **balance óptimo** entre tres factores en tensión:

Seguridad **Rendimiento** **Recursos**

Cada aplicación IoT tiene restricciones diferentes.
Elegir el algoritmo correcto requiere entender tanto las limitaciones del hardware como los requisitos de seguridad.