Algoritmo de cifrado

AES

(Advanced Encryption Standard).
Laboratorio: Demostración en JavaScript

Zharick Lisbeth Alba - Julio Cesar Calderón

compensar | fundación universitaria

AES

Advanced Encryption Standard (AES) es el **cifrado de bloque simétrico** que **cifra texto plano** en **bloques** de 128 bits con **claves estándar de 128, 192 y 256** bits en un **texto cifrado, codificado en base-64**. Al ser un cifrado **simétrico**, la misma clave se utiliza en el proceso de **cifrado y descifrado** de AES.

CRONOLOGÍA AES

1997 — NIST no certifica al DES por su debilidad frente a los ataques de RSA y llama a concurso para sustituirlo.

2000 — NIST proclama vencedor entre 15 participantes al algoritmo Rijndael.

2001 — AES se anuncia como estándar y se hace popular por su seguridad y velocidad.

2010 — AES comienza a usarse masivamente en protocolos seguros como TLS

Características del AES

01 Cifrador de producto (permutación + sustitución) no tipo Feistel

02 Implementado para trabajar en los procesadores de 8 bits usados en tarjetas inteligentes y en CPUs de 32 bits

03 Tamaño de clave variable de 128, 192 y 256 bits, valores estándar, o bien múltiplo de 4 bytes

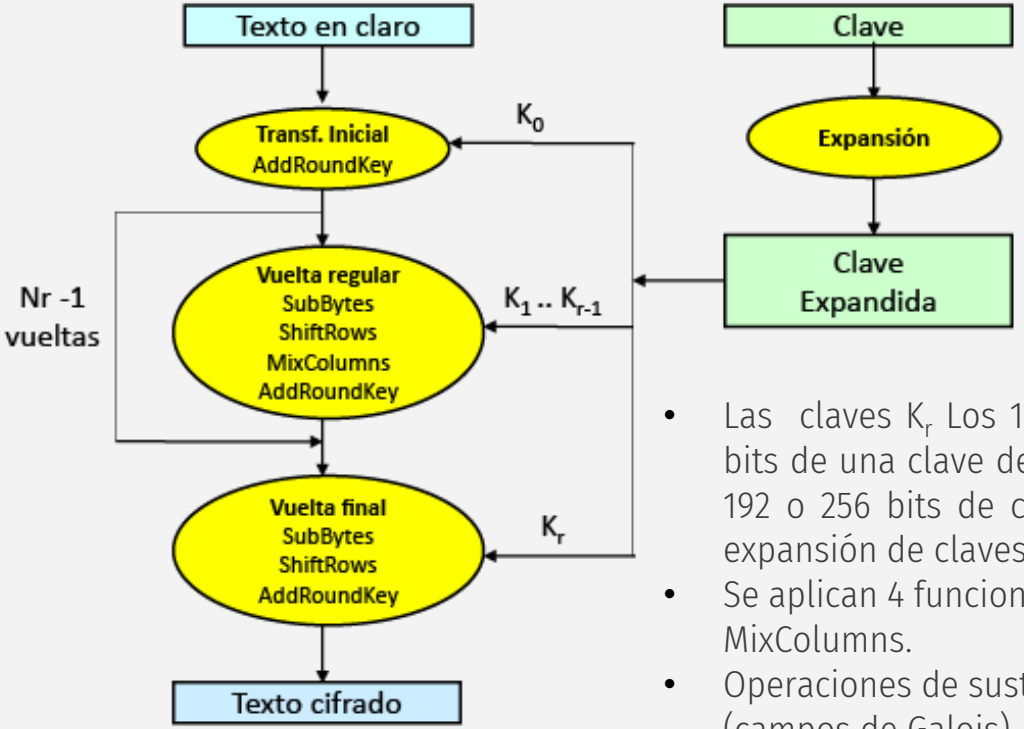
04 Tamaño del bloque de texto de 128 bits o múltiplo de 4 bytes

05 Operaciones modulares a nivel de byte (representación en forma de polinomios) y con palabras de 4 bytes, es decir 32 bits

06 Número de vueltas flexible según las necesidades del usuario

07 Usa 4 funciones invertibles para provocar difusión y confusión

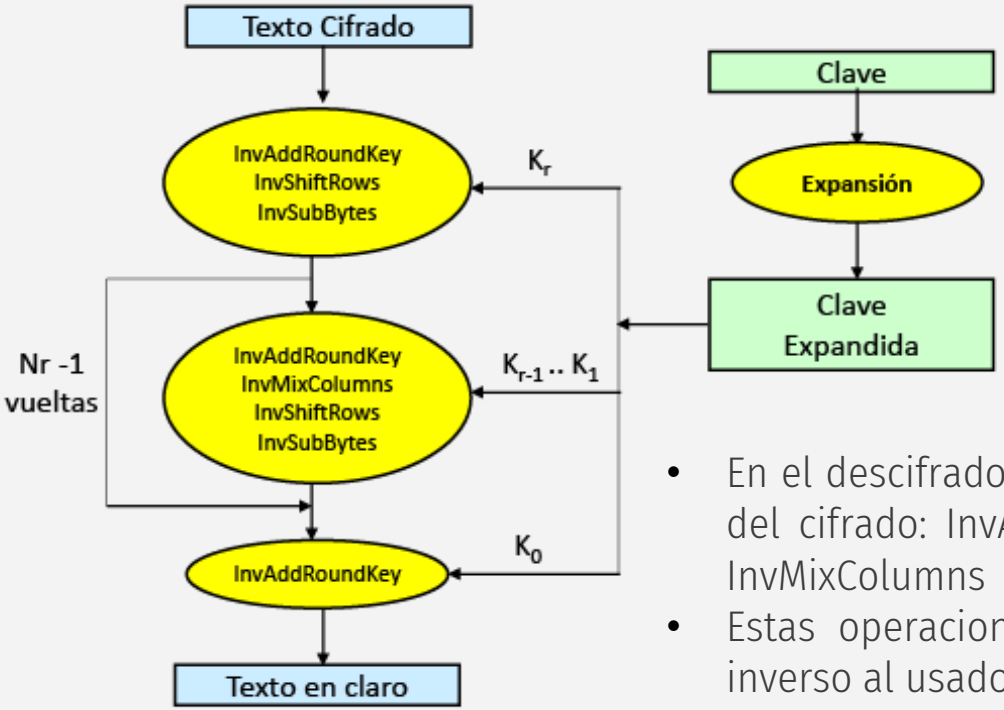
Esquema general AES en el cifrado



- Los 128 bits del texto en claro se mezclan con los bits de una clave de vuelta siempre de 128 bits, sea K igual a 128, 192 o 256 bits.

- Las claves K_r Los 128 bits del texto en claro se mezclan con los bits de una clave de vuelta siempre de 128 bits, sea K igual a 128, 192 o 256 bits de cada vuelta se obtienen con un algoritmo de expansión de claves.
- Se aplican 4 funciones: SubBytes , ShiftRows AddRoundKey , y MixColumns.
- Operaciones de sustitución y permutación con polinomios (campos de Galois)

Esquema general AES en el descifrado



- Las cuatro funciones empleadas AddRoundKey, SubBytes, ShiftRows y MixColumns son fácilmente invertibles.

- En el descifrado se usarán las operaciones inversas a las del cifrado: InvAddRoundKey, InvSubBytes, InvShiftRows, InvMixColumns
- Estas operaciones de descifrado se realizan en orden inverso al usado en el cifrado

AES

Laboratorio practicó en JS

git: https://juliansfreelance.github.io/Algoritmo-AES/

¡Gracias!

Zharick Lisbeth Alba - Julio Cesar Calderón

compensar | fundación universitaria