UVG UNIVERSIDAD DEL VALLE DE GUATEMALA

Cifrados de Bloque II

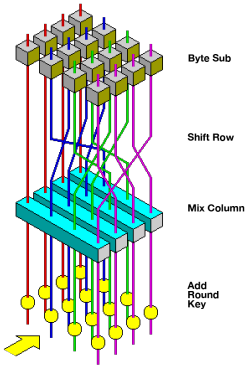
Alan Reyes-Figueroa

Criptografía y Cifrado de Información (Aula 09) 19.agosto.2021

AES

AES (*Advanced Encryption Standard*). También conocido como **Rijndael**. Propuesto por los criptólogos belgas, Joan Daemen y Vincent Rijmen,

- 1997: EL NIST lanza un comunicado para recibir propuesta para su nuevo estándar.
- 1998: 15 propuetas (5 ataques a estas propuestas).
- 1999: NIST elige 5 finalistas.
  Usa $k = 56$ bits, $n = 64$ bits, 16 rondas de bloque.
- 2000: NIST elige a Rijndael para AES. Pasa por un proceso de estandarización de 5 años. Y en 2002 se vuelve el estándar efectivo.

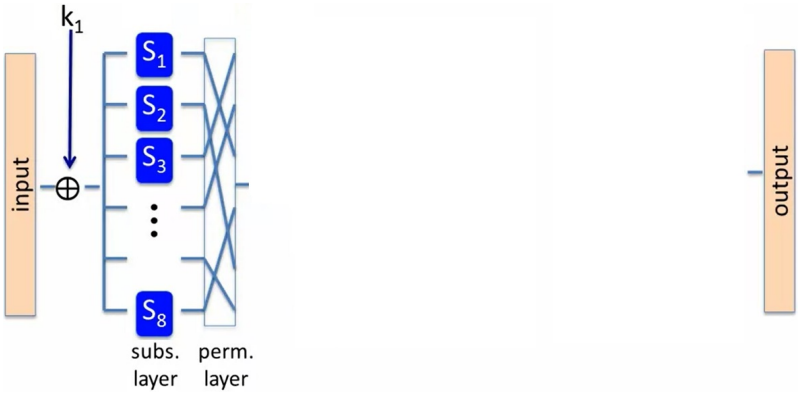


Esquema Rijndael

- Tamaños de clave: 128, 192 ó 256 bits. Tamaño de bloque: 128 bits.

AES

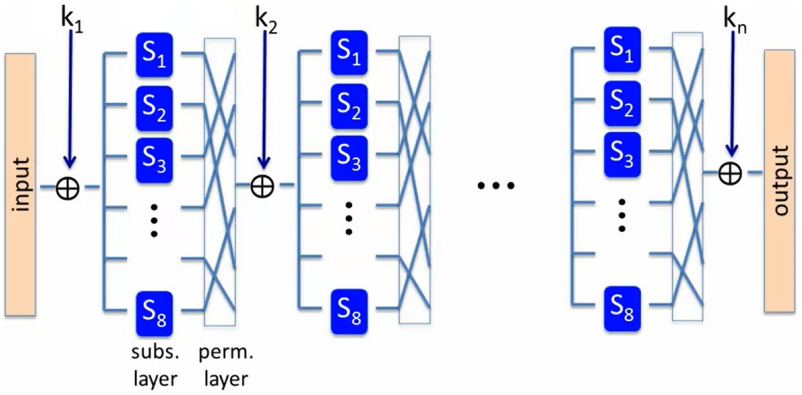
AES se basa en lo que se llama una **red de sustitución-permutación** (diferente a una red de Feistel). De nuevo, este es un esquema donde se aplican varias rondas.



Esquema de rondas en AES.

AES

AES se basa en lo que se llama una **red de sustitución-permutación** (diferente a una red de Feistel). De nuevo, este es un esquema donde se aplican varias rondas.

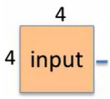


Esquema de rondas en AES.

AES

Esquema de funcionamiento AES:

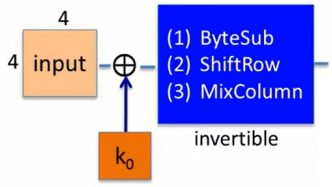
AES opera sobre un bloque de 128 bits (16 bytes). Estos 16 bytes se arreglan en una matriz de 4×4, 1 byte en cada celda.



AES

Esquema de funcionamiento AES:

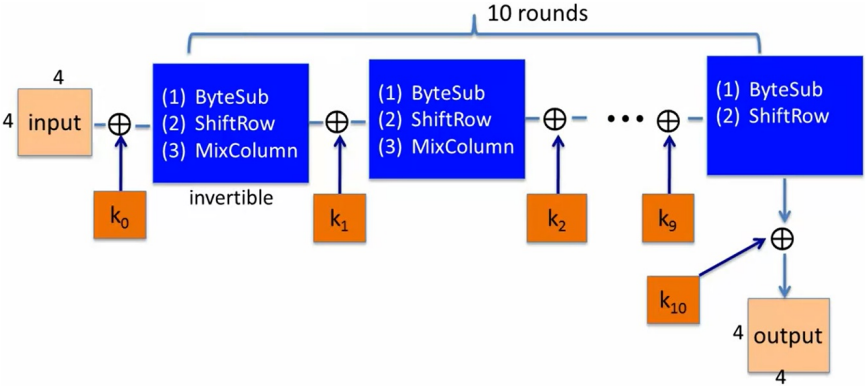
AES opera sobre un bloque de 128 bits (16 bytes). Estos 16 bytes se arreglan en una matriz de 4×4, 1 byte en cada celda.



AES

Esquema de funcionamiento AES:

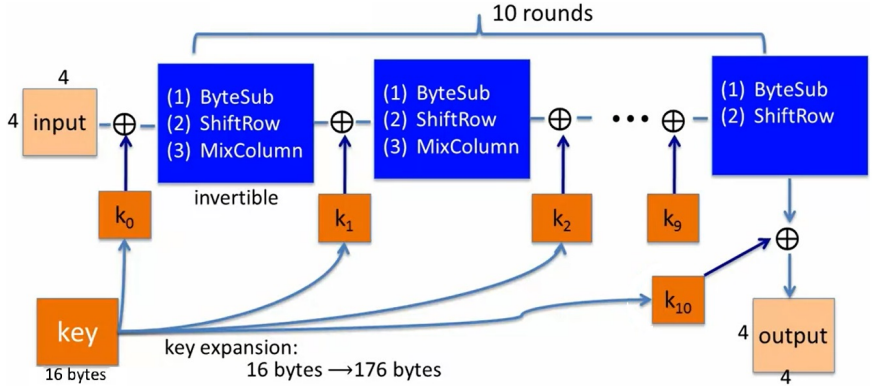
AES opera sobre un bloque de 128 bits (16 bytes). Estos 16 bytes se arreglan en una matriz de 4×4, 1 byte en cada celda.



AES

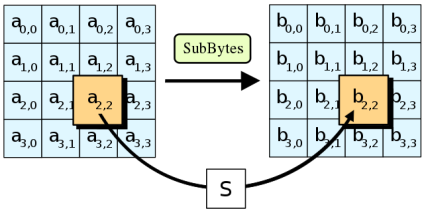
Esquema de funcionamiento AES:

AES opera sobre un bloque de 128 bits (16 bytes). Estos 16 bytes se arreglan en una matriz de 4×4, 1 byte en cada celda.

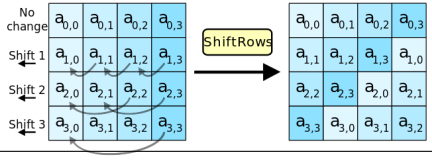


AES

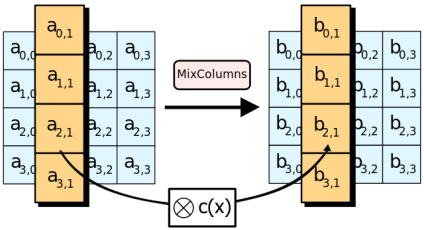
1. ByteSub: Es una tabla *S*-box de 256 bytes, que opera sobre cada byte. Sustituye cada entrada a_{ij} del bloque actual de 4×4, por lo que diga la tabla *S*. Esto es $[a_{ij}] \leftarrow [S(a_{ij})]$



2. ShiftRows: Es una permutación que esencialmente corre las filas a la derecha: la fila 2 se corre 1 posición; la fila 3, 2 posiciones, la fila 4; 3 posiciones.



3. MixColumns: A cada columna del bloque 4×4, sele aplica una transformación lineal específica para producir las nuevas columnas



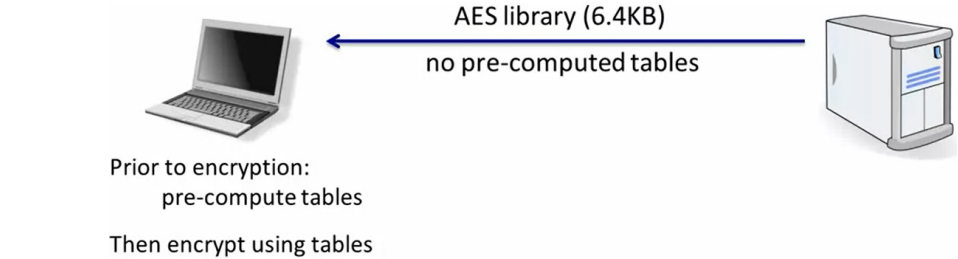
AES

	Code size	Performance
Pre-compute round functions (24KB or 4KB)	largest	fastest: table lookups and xors
Pre-compute S-box only (256 bytes)	smaller	slower
No pre-computation	smallest	slowest

Comparación de desempeño de diferentes implementaciones de AES.

AES

Ejemplo: AES en el browser.



Ver `https://crypto.stanford.edu/sjcl/`.

AES

Ejemplos: AES es hardware.

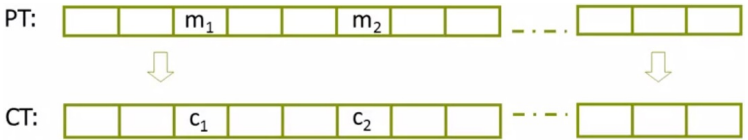
Implementaciones de AES en procesadores Intel Westmere.

- **aesenc**, **aesenclast**: hacen 1 ronda de AES,
  Usan registros de 128 bits: `xxm1 = state`, `xxm2 = round key`,
  aesenc xmm1, xmm2: guarda el resultado en `xmm1`.
- **aeskeygenassist**: ejecuta la expansión de clave.
- $14\times$ más veloz que OpenSSL sobre el mismo hardware.

Implementaciones de AES en procesadores AMD Bulldozer.

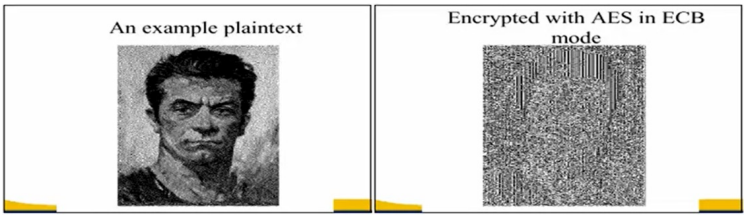
Modos de Operación

Modo ECB: (*Electronic Code Book*).



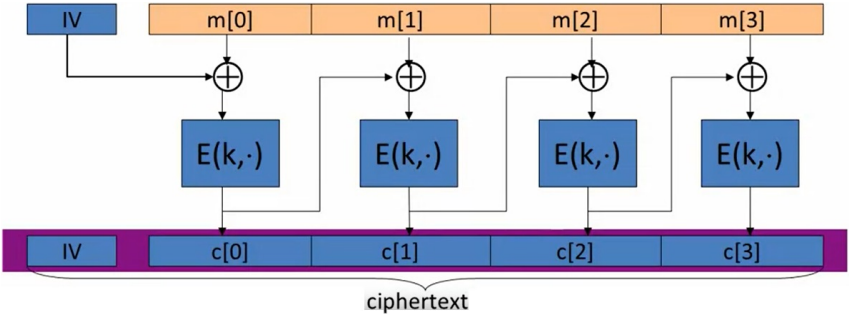
Modo ECB.

Problema: $\mathbf{m_1 = m_2} \Rightarrow \mathbf{c_1 = c_2}$.



Modos de Operación

Modo CBC: (*Cipher Block Chain*) con IV aleatorio.
Sea (E, D) una permutación pseudo-aleatoria PRP. La función de encriptado $E_{CBC}(\mathbf{k}, \mathbf{m})$ toma un IV aleatorio y hace

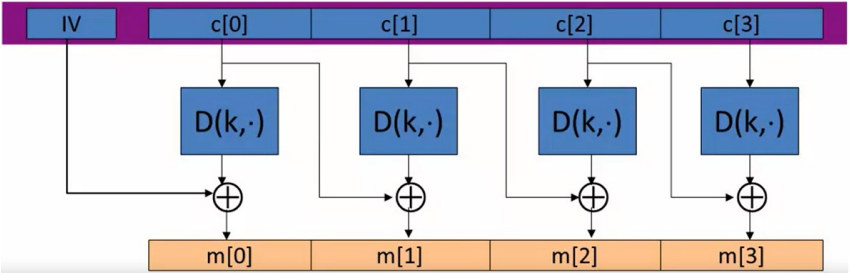


IV = *Initialization Vector*.

Modos de Operación

En este caso si $\mathbf{c}_0 = E(\mathbf{k}, \mathbf{m}_0 \oplus IV)$, entonces $\mathbf{m}_0 = D(\mathbf{k}, \mathbf{c}_0) \oplus IV$.

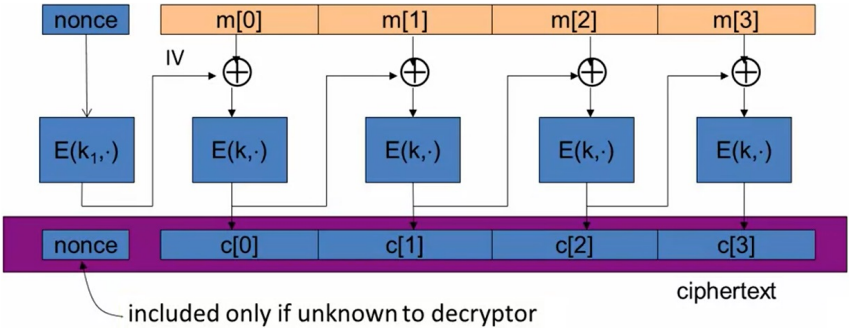
Esta secuencia de decripción se generaliza a todo el CBC:



Esquema de decripción en el modo CBC.

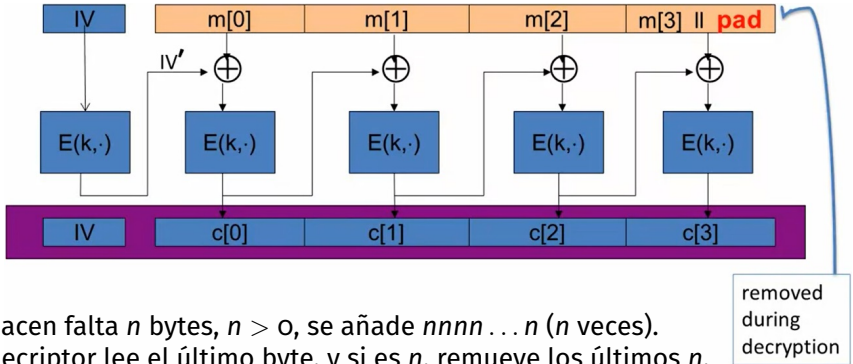
Modos de Operación

Modo CBC: (*Cipher Block Chain*) con Nonce único.
Igual que antes (E, D) una permutación pseudo-aleatoria PRP. Aqui, nonce único significa que el par $(\mathbf{k}, \mathbf{n})$ sólo se usa para un mensaje.



Modos de Operación

Modo CBC: Padding.
Cuando el último bloque no coincide en longitud con el tamaño de los bloques (16 bytes), se añaden bytes extras.

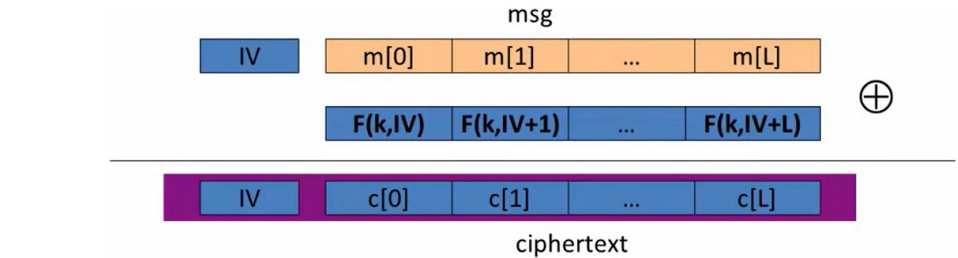


PCKS5:

- Si hacen falta n bytes, $n > 0$, se añade $nnnn \ldots n$ (n veces).
  El decriptor lee el último byte, y si es n, remueve los últimos n.
- Si $n = 0$, entonces se añade un bloque *dummy* de $n = 16$ bytes: $nnnn \ldots n$.

Modos de Operación

Modo CTR: (*Randomized Counter Mode*).
Sea F una PRF, función pseudo-aleatoria segura, digamos $F : \mathcal{K} \times \{0,1\}^n \to \{0,1\}^n$.



- El IV se elige de forma aleatoria en cada mensaje.
- Es paralelizable (el CBC no).