AES-NI

ADVANCED ENCRYPTION STANDARD NEW INSTRUCTIONS

AES-NI

Conjunto de instrucciones del Advanced Encryption Standard

- 2008: Intel anuncia AES-NI
- 2010: primeros Intel Core con instrucciones AES-NI.
- Instrucciones para arquitecturas x86-64 para implementar el uso de AES.
- Todos los nuevos procesadores Intel, AMD y ARM son compatibles con AES-NI.

AES-NI

Conjunto de instrucciones del Advanced Encryption Standard

- **Objetivo:** acelerar la ejecución de AES → rendimiento 3-10 veces superior a implementaciones software en CPUs.
- **Implementación:** un conjunto de 6 instrucciones sirve para ejecutar las etapas más complejas y computacionalmente costosas de AES gracias a la implementación vectorial en HW.
- **Valor añadido:** mejora de la resistencia a los ataques de canal lateral puesto que el cifrado/descifrado se realiza completamente en hardware.

AES-NI

- Conjunto de 6 instrucciones (por defecto AES-128):
  - **4 instrucciones para cifrado/descifrado**:
    - **AESENC:** instrucción para ejecutar una ronda de cifrado.
    - **AESENCLAST:** instrucción para ejecutar la última ronda de cifrado.
    - **AESDEC:** instrucción para ejecutar una ronda de descifrado.
    - **AESDECLAST:** instrucción para ejecutar la última ronda de descifrado.

AES-NI

- Conjunto de 6 instrucciones (por defecto AES-128):
  - **2 instrucciones para la generación de claves**:
    - **AESKEYGENASSIST:** instrucción para generar claves para las rondas de cifrado.
    - **AESIMC:** instrucción para generar claves para las rondas de descifrado.

AES-NI

[1] https://www.redeszone.net/tutoriales/servidores/aceleracion-cifrado-hardware-aes-ni-servidores-nas/

[2] https://www.intel.com/content/www/us/en/developer/articles/technical/advanced-encryption-standard-instructions-aes-ni.html