AES-NI

ADVANCED ENCRYPTION STANDARD NEW INSTRUCTIONS

AES-NI

Advanced Encryption Standard instrukzio multzoa

- 2008: Intelek AES-NI iragartzen du
- 2010: lehen Intel Core prozesaodreak AES-NI prozesdorearekin.
- x86-64 arkitekturetako instrukzioa AES inplementatzeko.
- Intel, AMD eta ARM prozesadore berri guztiak AES-NI-rekin bateragarriak dira.

AES-NI

Advanced Encryption Standard instrukzio multzoa

- **Helburua:** acelerar la ejecución de AES → rendimiento 3-10 veces superior a implementaciones software en CPUs.
- **Inplementazioa:** 6 instrukzioko multzo baten bitartez AES-ren kalkulu konplexu eta motelak azkartu daitezke HW inplementazio bektorialari esker.
- **Balio gehigarria:** alboko kanal erasoak ekiditzeko gomendagarria, zifraketa eta deszifraketa guztiz HW bitartez egiten baita.

AES-NI

- 6 instruzioko multzoa (AES-128 lehenetsia):
  - **zifratze/deszifratzeko 4 instrukzio**:
    - **AESENC:** zifratzeko erronda funtzio baten exekuziorako instrukzioa.
    - **AESENCLAST:** zifratzeko azken erronda funtzioaren exekuziorako instrukzioa.
    - **AESDEC:** deszifratzeko erronda funtzio baten exekuziorako instrukzioa.
    - **AESDECLAST:** deszifratzeko azken erronda funtzioaren exekuziorako instrukzioa.

AES-NI

- 6 instruzioko multzoa (AES-128 lehenetsia):
  - **2 instrukzio gakoen sorrerarago**:
    - **AESKEYGENASSIST:** zifraketarako azpigakoak kalkulatzeko instrukzioa.
    - **AESIMC:** deszifraketarako azpigakoak kalkulatzeko instrukzioa.

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