37. Расширения процессора. AES. Назначение, классификация команд.

Расширение **AES** (*Intel Advanced Encryption Standard New Instructions; AES-NI, 2008*)

- Реализует алгоритмы шифрования AES (Advanced Encryption Standard) и Galois/Counter Mode (GCM) для ускорения шифрования и расшифрования данных.
- Реализует алгоритмы хэширования SHA-1 и SHA-256 для ускорения вычисления хэш-функций.

и т.п.

Классификация команд

- раунда шифрования
- раунда расшифрования
- раунда генерации ключа