**CONTROLLER DECRIPTOGRAFIA**

O AES‑128 (Advanced Encryption Standard) é um algoritmo de criptografia simétrica que usa chaves de 128 bits.

* Criptografia: pega um texto legível (palavra) e transforma em cifra (ininteligível).
* Decriptação: faz o caminho inverso — pega a cifra e recupera o texto original (palavra) usando a mesma chave secreta.

Estrutura da decriptação AES‑128

* Entrada:
  + Cifra (128 bits).
  + Key (128 bits).
* Saída:
  + Palavra (128 bits).
* Subchaves:
  + A chave inicial é expandida em 11 chaves de 128 bits (uma para cada rodada).
* Etapas:
  + Rodada inicial: AddRoundKey com a última chave.
  + 9 rodadas intermediárias: InvShiftRows → InvSubBytes → AddRoundKey → InvMixColumns.
  + Rodada final: InvShiftRows → InvSubBytes → AddRoundKey (sem MixColumns).

Visão Geral dos blocos do AES‑128 decriptação

* Blocos básicos usados:
  + AddRoundKey: XOR entre estado e chave da rodada.
  + InvShiftRows: Desfaz a rotação das linhas.
  + InvSubBytes: Aplica a InvSBox (substituição inversa).
  + InvMixColumns: Mistura colunas inversa (só nas rodadas intermediárias).
  + KeyExpansion: Gera 11 chaves de 128 bits (rodadas 0 → 10).
* Número de rodadas:

AES‑128 tem 10 rodadas.

* + Rodada inicial: AddRoundKey com a chave da última rodada.
  + Rodadas intermediárias (9x): InvShiftRows → InvSubBytes → AddRoundKey → InvMixColumns.
  + Rodada final (sem MixColumns): InvShiftRows → InvSubBytes → AddRoundKey (chave 0).

Porque cada transformação tem uma função inversa bem definida:

* InvSubBytes é a inversa da substituição da S‑Box.
* InvShiftRows desfaz a rotação feita no ShiftRows.
* InvMixColumns desfaz a mistura das colunas.
* AddRoundKey é auto inverso (XOR com a mesma chave desfaz a operação).

Assim, é possível voltar exatamente ao estado original.