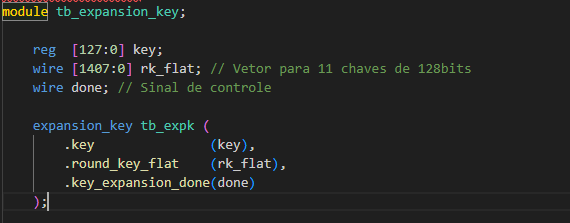
# 1. Objetivo do Testbench

Este testbench tem como finalidade validar o funcionamento do módulo de expansão de chave AES-128, comparando os resultados obtidos com os valores oficiais fornecidos pelo padrão FIPS-197 (Apêndice A). São utilizadas diversas chaves de teste para garantir a conformidade funcional e detectar possíveis erros de expansão.

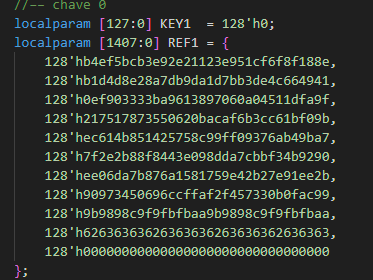
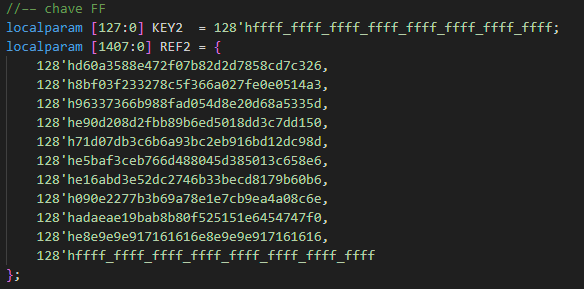
# 2. Estrutura do Testbench

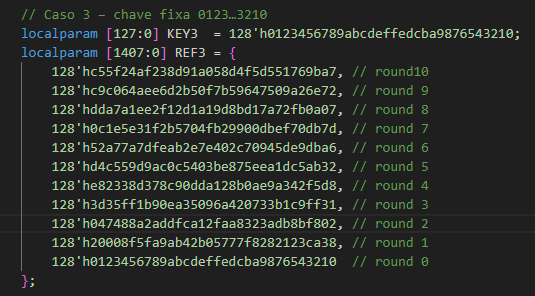
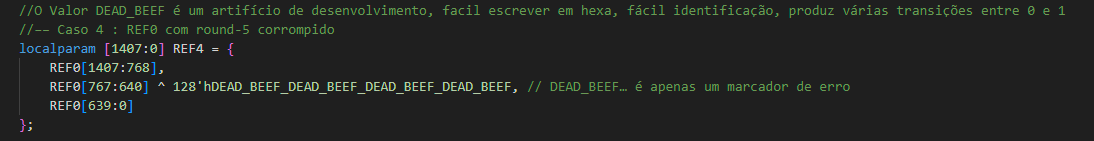
O módulo `tb\_expansion\_key` instancia o DUT (Device Under Test) `expansion\_key`, conectando três sinais principais:  
- `key`: chave original de 128 bits  
- `rk\_flat`: vetor concatenado com 11 chaves de 128 bits (1408 bits no total)  
- `done`: sinal que indica finalização da expansão



# 3. Vetores de Referência

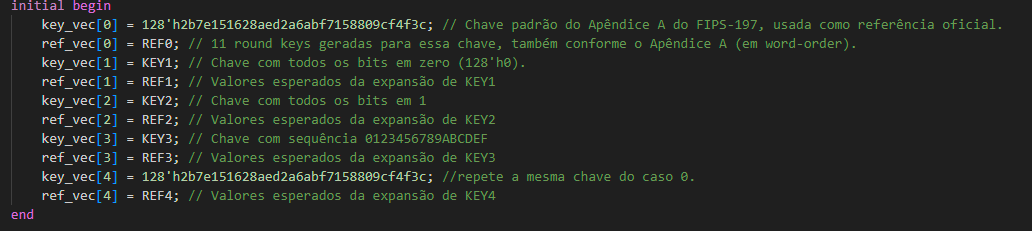
Foram definidos cinco vetores de entrada e seus respectivos vetores de referência:  
- REF0: Chave padrão oficial do Apêndice A  
- REF1: Chave com todos os bits em 0  
- REF2: Chave com todos os bits em 1  
- REF3: Chave incremental 0123…3210  
- REF4: Mesma chave do caso 0, porém com round 5 corrompido (injeção de erro proposital com DEAD\_BEEF)

# 4. Lógica de Validação

O testbench realiza um laço `for` de 5 iterações, uma para cada caso de teste. Em cada iteração:  
- Atribui a chave de teste ao DUT  
- Aguarda 50 ns (considerando 40 ciclos internos #1 + margem)  
- Compara bit a bit o vetor gerado com a referência  
- Em caso de falha, identifica e exibe as rodadas específicas que divergiram

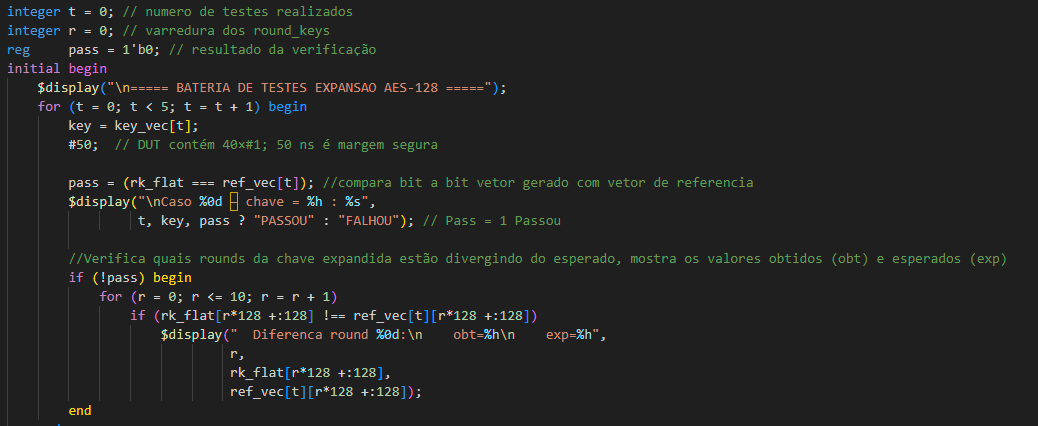


# 5. Motivos da Escolha dos Valores

Os valores foram selecionados para cobrir casos clássicos de validação:  
- Valor oficial (conformidade normativa)  
- Zeros e FFs (testes de borda)  
- Sequência linear (comportamento incremental)  
- Injeção de erro (verificação da sensibilidade do testbench)

# 6. Resultados Esperados

O testbench deve exibir "PASSOU" para os casos 0 a 3, e "FALHOU" para o caso 4, com detalhes das divergências no round corrompido.



# 7. Conclusão

Este testbench é uma ferramenta robusta e didática para verificar a implementação de expansão de chave AES-128. Ele utiliza padrões reconhecidos, cobre casos especiais e insere falhas propositais para validar a integridade da lógica de verificação.

