3. (0,5) Considerando o algoritmo SHA-256, se você fosse responsável por propor uma melhora de sua segurança, com foco em dificultar a decodificação mediante força bruta, o que você faria? Em qual parte do algoritmo você aplicaria a alteração? Justifique sua resposta.

Para dificultar a decodificação por força bruta no algoritmo SHA-256, uma proposta de melhoria seria aumentar a complexidade computacional do processo de hash, de forma que cada tentativa de ataque por força bruta demande mais tempo e recursos computacionais.

O SHA-256 atualmente realiza 64 rounds (iterações) com funções de mistura e compressão internas. Uma forma eficaz de aumentar a segurança contra ataques de força bruta é aumentar esse número, por exemplo, para 128 ou mais rounds, tornando cada tentativa de cálculo do hash mais lenta.