AES Encryption & Decryption Verilog Project - File Explanation

addRoundKey.v

Performs XOR between the AES state and round key.

addRoundKey_tb.v

Testbench for verifying the AddRoundKey module.

AES.v

Top-level module for the AES core integration.

AES_Decrypt.v

Controls the AES decryption flow using inverse transformations.

AES_Decrypt_tb.v

Testbench for verifying the AES decryption controller.

AES_Encrypt.v

Controls the AES encryption flow using core transformations.

AES_Encrypt_tb.v

Testbench for verifying the AES encryption controller.

AES_tb.v

Testbench for the full AES encryption and decryption process.

decryptRound.v

Handles one full AES decryption round (except final round).

encryptRound.v

Handles one full AES encryption round (except final round).

inverseMixColumns.v

Performs inverse MixColumns operation for decryption.

inverseMixColumns_tb.v

Testbench for verifying the inverse MixColumns module.

inverseSbox.v

Implements the inverse S-box lookup for decryption.

inverseShiftRows.v

Reverses the row shifting for AES decryption.

inverseShiftRows_tb.v

Testbench for verifying the inverse ShiftRows module.

inverseSubBytes.v

Implements the inverse SubBytes transformation.

inverseSubBytes_tb.v

Testbench for verifying inverse SubBytes module.

keyExpansion.v

Generates all round keys from the original AES key.

keyExpansion_tb.v

Testbench for verifying the key expansion logic.

mixColumns.v

Mixes each column of the state matrix (encryption).

mixColumns_tb.v

Testbench for verifying the MixColumns module.

sbox.v

Implements the AES S-box (SubBytes) as a ROM.

shiftRows.v

Performs row shifts in AES encryption.

shiftRows_tb.v

Testbench for verifying the ShiftRows module.

subBytes.v

Applies the SubBytes transformation using the S-box.

subBytes_tb.v

Testbench for verifying SubBytes transformation.