AES-128 Encryption and Decryption Code Summary

Objective

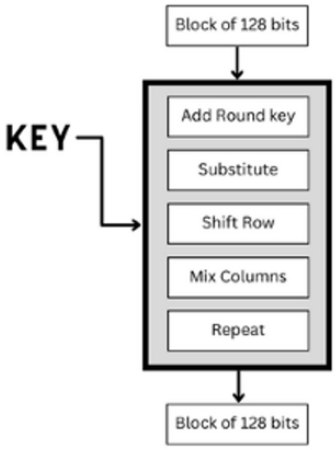
The task was to develop a Python program capable of encrypting and decrypting a 128-bit plaintext using the AES algorithm with a 128-bit key across 10 encryption rounds.

Overview

The code is structured into various functional blocks, including initialization, utility functions, key expansion, encryption, and decryption routines.

Detailed Breakdown

1. **Initialization and S-Boxes:**
    - The program initializes with a 128-bit key and loads two substitution boxes:
        - **S-box** for encryption byte substitution.
        - **Inverse S-box** for decryption byte substitution.
2. **Utility Functions:**
    - **sub_word** and **inv_sub_word**: Apply byte substitution using S-box and inverse S-box.
    - **rot_word** and **inv_rot_word**: Rotate bytes of a word for key expansion.
    - **xtime** and **mul_gf**: Perform multiplication in the Galois field, crucial for the MixColumns and InvMixColumns steps.
3. **Key Expansion:**
    - The keyExpansion method generates round keys from the initial key using byte substitution, rotation, and XOR operations with round constants.
4. **Encryption Process:**



- **Initial Round:**
  - **AddRoundKey**: XORs the plaintext with the initial round key.
- **Main Rounds (1 to 9):**
  - **SubBytes**: Each byte is replaced according to the S-box.
  - **ShiftRows**: Rows of the state are cyclically shifted.
  - **MixColumns**: Combines bytes within each column.
  - **AddRoundKey**: XORs state with the round key.
- **Final Round (10th Round):**
  - Includes SubBytes, ShiftRows, and AddRoundKey, omitting MixColumns.

5. **Decryption Process:**
   - Similar to encryption but in reverse order, using inverse operations and round keys in reverse sequence.
   - **Initial Round**: Encrypted data (ciphertext) is XORed with the last round key generated during the key expansion process
   - **First round**: Includes AddRoundKey, InvShiftRows, InvSubBytes, and omitting MixColumns.
   - Main Rounds (2 to 9):
     - **AddRoundKey**: XORs state with the round key.
     - **InvMixColumns**: Performs inverse mixing on each column.
     - **InvShiftRows**: Rows are cyclically shifted in reverse.
     - **InvSubBytes**: Each byte is replaced using the Inverse S-box.
   - **Final Round** (Decryption Round 10, Corresponds to First Encryption Round:
   - AddRoundKey (XORs state with the initial round key.
6. **Testing and Verification:**
   - Includes debugging outputs of intermediate states in hexadecimal format.
   - Validates encryption by decrypting and comparing with the original plaintext.
   - Checks the equivalence of the output of the 1st encryption round with the 9th decryption round and vice versa, ensuring round inversion integrity.
7. **Test Cases:**

Test Case1

```
Plaintext: [50, 67, 246, 168, 136, 90, 48, 141, 49, 49, 152, 162, 224, 55, 7, 52] <=====> Decrypted: [50, 67, 246, 168, 136, 90, 48, 141, 49, 49, 152, 162, 224, 55, 7, 52]

Round 1 Encryption: [164, 156, 127, 242, 104, 159, 53, 43, 107, 91, 234, 67, 2, 106, 80, 73] <=====> Round 9 Decryption: [164, 156, 127, 242, 104, 159, 53, 43, 107, 91, 234, 67, 2, 106, 80, 73] <====> Matched
Round 2 Encryption: [170, 143, 95, 3, 97, 221, 227, 239, 130, 210, 74, 210, 104, 50, 70, 154] <=====> Round 8 Decryption: [170, 143, 95, 3, 97, 221, 227, 239, 130, 210, 74, 210, 104, 50, 70, 154] <====> Matched
Round 3 Encryption: [72, 108, 78, 238, 103, 29, 157, 13, 77, 227, 177, 56, 214, 95, 88, 231] <=====> Round 7 Decryption: [72, 108, 78, 238, 103, 29, 157, 13, 77, 227, 177, 56, 214, 95, 88, 231] <====> Matched
Round 4 Encryption: [224, 146, 127, 232, 200, 99, 99, 192, 217, 177, 53, 80, 133, 184, 190, 1] <=====> Round 6 Decryption: [224, 146, 127, 232, 200, 99, 99, 192, 217, 177, 53, 80, 133, 184, 190, 1] <====> Matched
Round 5 Encryption: [241, 0, 111, 85, 193, 146, 76, 239, 124, 200, 139, 50, 93, 101, 213, 12] <=====> Round 5 Decryption: [241, 0, 111, 85, 193, 146, 76, 239, 124, 200, 139, 50, 93, 101, 213, 12] <====> Matched
Round 6 Encryption: [38, 14, 46, 23, 61, 65, 183, 125, 232, 100, 114, 169, 253, 210, 139, 37] <=====> Round 4 Decryption: [38, 14, 46, 23, 61, 65, 183, 125, 232, 100, 114, 169, 253, 210, 139, 37] <====> Matched
Round 7 Encryption: [90, 65, 66, 177, 25, 73, 220, 31, 163, 224, 25, 101, 122, 140, 4, 12] <=====> Round 3 Decryption: [90, 65, 66, 177, 25, 73, 220, 31, 163, 224, 25, 101, 122, 140, 4, 12] <====> Matched
Round 8 Encryption: [234, 131, 92, 240, 4, 69, 51, 45, 101, 93, 152, 173, 133, 150, 176, 197] <=====> Round 2 Decryption: [234, 131, 92, 240, 4, 69, 51, 45, 101, 93, 152, 173, 133, 150, 176, 197] <====> Matched
Round 9 Encryption: [235, 64, 242, 30, 89, 46, 56, 132, 139, 161, 19, 231, 27, 195, 66, 210] <=====> Round 1 Decryption: [235, 64, 242, 30, 89, 46, 56, 132, 139, 161, 19, 231, 27, 195, 66, 210] <====> Matched
Round 10 Encryption: [57, 37, 132, 29, 2, 220, 9, 251, 220, 17, 133, 151, 25, 106, 11, 50] <=====> Round 0 Decryption: [57, 37, 132, 29, 2, 220, 9, 251, 220, 17, 133, 151, 25, 106, 11, 50] <====> Matched
```

Test Case 2

```
Plaintext: [17, 34, 51, 68, 85, 102, 119, 136, 153, 170, 187, 204, 221, 238, 255, 0] <======> Decrypted: [17, 34, 51, 68, 85, 102, 119, 136, 153, 170, 187, 204, 221, 238, 255, 0]

Round 1 Encryption: [151, 109, 99, 77, 94, 1, 74, 0, 191, 82, 65, 52, 121, 161, 85, 167] <=====> Round 9 Decryption: [151, 109, 99, 77, 94, 1, 74, 0, 191, 82, 65, 52, 121, 161, 85, 167] <====> Matched
Round 2 Encryption: [162, 112, 152, 54, 213, 50, 60, 138, 135, 44, 242, 109, 142, 238, 227, 100] <=====> Round 8 Decryption: [162, 112, 152, 54, 213, 50, 60, 138, 135, 44, 242, 109, 142, 238, 227, 100] <====> Matched
Round 3 Encryption: [230, 63, 146, 31, 198, 193, 161, 81, 112, 208, 79, 239, 123, 219, 73, 210] <=====> Round 7 Decryption: [230, 63, 146, 31, 198, 193, 161, 81, 112, 208, 79, 239, 123, 219, 73, 210] <====> Matched
Round 4 Encryption: [81, 24, 132, 69, 176, 139, 178, 104, 90, 73, 59, 135, 235, 73, 231, 129] <=====> Round 6 Decryption: [81, 24, 132, 69, 176, 139, 178, 104, 90, 73, 59, 135, 235, 73, 231, 129] <====> Matched
Round 5 Encryption: [196, 75, 225, 87, 30, 219, 192, 198, 250, 158, 76, 139, 20, 31, 6, 40] <=====> Round 5 Decryption: [196, 75, 225, 87, 30, 219, 192, 198, 250, 158, 76, 139, 20, 31, 6, 40] <====> Matched
Round 6 Encryption: [152, 178, 8, 166, 220, 133, 116, 185, 150, 232, 71, 125, 108, 111, 242, 155] <=====> Round 4 Decryption: [152, 178, 8, 166, 220, 133, 116, 185, 150, 232, 71, 125, 108, 111, 242, 155] <====> Matched
Round 7 Encryption: [212, 200, 65, 219, 83, 80, 177, 56, 58, 123, 237, 45, 218, 202, 158, 255] <=====> Round 3 Decryption: [212, 200, 65, 219, 83, 80, 177, 56, 58, 123, 237, 45, 218, 202, 158, 255] <====> Matched
Round 8 Encryption: [204, 213, 248, 211, 165, 134, 176, 189, 50, 218, 21, 2, 226, 138, 110, 93] <=====> Round 2 Decryption: [204, 213, 248, 211, 165, 134, 176, 189, 50, 218, 21, 2, 226, 138, 110, 93] <====> Matched
Round 9 Encryption: [227, 19, 15, 171, 21, 142, 2, 47, 215, 183, 120, 239, 233, 135, 215, 215] <=====> Round 1 Decryption: [227, 19, 15, 171, 21, 142, 2, 47, 215, 183, 120, 239, 233, 135, 215, 215] <====> Matched
Round 10 Encryption: [193, 13, 69, 166, 144, 71, 43, 235, 239, 40, 122, 221, 168, 30, 123, 121] <=====> Round 0 Decryption: [193, 13, 69, 166, 144, 71, 43, 235, 239, 40, 122, 221, 168, 30, 123, 121] <====> Matched
```

Test Case 3

```
Plaintext: [222, 173, 190, 239, 202, 254, 186, 190, 0, 17, 34, 51, 68, 85, 102, 119] <======> Decrypted: [222, 173, 190, 239, 202, 254, 186, 190, 0, 17, 34, 51, 68, 85, 102, 119]

Round 1 Encryption: [171, 188, 170, 146, 22, 166, 219, 0, 251, 161, 203, 4, 242, 102, 92, 215] <=====> Round 9 Decryption: [171, 188, 170, 146, 22, 166, 219, 0, 251, 161, 203, 4, 242, 102, 92, 215] <====> Matched
Round 2 Encryption: [75, 199, 255, 115, 167, 36, 137, 108, 221, 208, 90, 50, 158, 56, 126, 220] <=====> Round 8 Decryption: [75, 199, 255, 115, 167, 36, 137, 108, 221, 208, 90, 50, 158, 56, 126, 220] <====> Matched
Round 3 Encryption: [34, 0, 52, 44, 19, 43, 165, 92, 200, 134, 100, 173, 174, 55, 117, 1] <=====> Round 7 Decryption: [34, 0, 52, 44, 19, 43, 165, 92, 200, 134, 100, 173, 174, 55, 117, 1] <====> Matched
Round 4 Encryption: [229, 151, 197, 165, 114, 106, 208, 195, 154, 212, 185, 14, 62, 182, 130, 99] <=====> Round 6 Decryption: [229, 151, 197, 165, 114, 106, 208, 195, 154, 212, 185, 14, 62, 182, 130, 99] <====> Matched
Round 5 Encryption: [214, 13, 167, 49, 49, 96, 185, 16, 251, 9, 107, 219, 54, 123, 41, 196] <=====> Round 5 Decryption: [214, 13, 167, 49, 49, 96, 185, 16, 251, 9, 107, 219, 54, 123, 41, 196] <====> Matched
Round 6 Encryption: [146, 88, 95, 236, 229, 253, 251, 158, 48, 154, 85, 162, 77, 243, 61, 26] <=====> Round 4 Decryption: [146, 88, 95, 236, 229, 253, 251, 158, 48, 154, 85, 162, 77, 243, 61, 26] <====> Matched
Round 7 Encryption: [114, 14, 242, 40, 204, 74, 175, 155, 95, 249, 222, 106, 24, 186, 5, 96] <=====> Round 3 Decryption: [114, 14, 242, 40, 204, 74, 175, 155, 95, 249, 222, 106, 24, 186, 5, 96] <====> Matched
Round 8 Encryption: [198, 210, 180, 145, 204, 102, 226, 149, 46, 131, 251, 127, 163, 228, 219, 21] <=====> Round 2 Decryption: [198, 210, 180, 145, 204, 102, 226, 149, 46, 131, 251, 127, 163, 228, 219, 21] <====> Matched
Round 9 Encryption: [220, 237, 20, 186, 152, 35, 138, 176, 86, 148, 14, 162, 205, 70, 249, 226] <=====> Round 1 Decryption: [220, 237, 20, 186, 152, 35, 138, 176, 86, 148, 14, 162, 205, 70, 249, 226] <====> Matched
Round 10 Encryption: [86, 50, 82, 48, 143, 204, 188, 125, 80, 101, 246, 47, 11, 54, 114, 156] <=====> Round 0 Decryption: [86, 50, 82, 48, 143, 204, 188, 125, 80, 101, 246, 47, 11, 54, 114, 156] <====> Matched
```

This summary encapsulates the key components and functionality of the AES-128 implementation, highlighting the systematic approach to both encrypting and decrypting data in alignment with AES standards.