For the demonstration of the working of the code

```
Enter the message to be encrypted:
Two One Nine Two
Enter the key:
ABCDabcd12344321
Round  1 :  [['3C', 'E6', '92', '17'], ['53', 'B1', '7A', 'AF'], ['53', 'F6', '4C', '3C'], ['B5', 'BA', 'A3', '68']]
Round  2 :  [['14', '58', 'CB', 'BF'], ['B1', '3E', 'B8', '22'], ['1D', 'B9', '60', 'F1'], ['85', 'F9', '4A', '71']]
Round  3 :  [['3D', '2E', '12', '4C'], ['9A', 'E6', 'AA', '96'], ['D6', '62', '60', '74'], ['55', 'C9', '4C', '83']]
Round  4 :  [['8D', 'ED', 'B8', '2C'], ['C6', '79', '92', '0B'], ['D1', 'CE', 'AE', 'A0'], ['50', 'A5', 'DF', 'D1']]
Round  5 :  [['50', '37', 'D3', '50'], ['29', 'F3', '92', '73'], ['11', '2C', '55', '10'], ['5C', '48', '4B', '87']]
Round  6 :  [['72', 'A9', '0F', '69'], ['A4', 'BE', 'F5', '12'], ['11', '09', 'E9', '52'], ['6F', '5F', '1E', '4D']]
Round  7 :  [['F8', '9F', 'C3', '9A'], ['E7', '38', '60', 'E7'], ['FB', '4C', '99', 'DF'], ['71', 'E4', '6E', '97']]
Round  8 :  [['55', 'F8', 'BC', '80'], ['C0', 'C0', '12', 'E5'], ['E4', 'AE', '10', '30'], ['44', '27', '43', '18']]
Round  9 :  [['8C', '03', 'E0', 'AF'], ['EA', 'F4', 'E7', '59'], ['2E', 'DA', '59', '06'], ['66', '32', 'EE', '07']]
Round  10 :  [['79', 'B8', 'DD', '40'], ['4A', '4A', '49', 'D3'], ['3D', 'EE', 'C8', '22'], ['E6', '1A', '78', '52']]
794A3DE6B84AEE1ADD49C87840D32252
Received message :  [['79', 'B8', 'DD', '40'], ['4A', '4A', '49', 'D3'], ['3D', 'EE', 'C8', '22'], ['E6', '1A', '78', '52']]
Round  1 :  [['8C', '03', 'E0', 'AF'], ['EA', 'F4', 'E7', '59'], ['2E', 'DA', '59', '06'], ['66', '32', 'EE', '07']]
Round  2 :  [['55', 'F8', 'BC', '80'], ['C0', 'C0', '12', 'E5'], ['E4', 'AE', '10', '30'], ['44', '27', '43', '18']]
Round  3 :  [['F8', '9F', 'C3', '9A'], ['E7', '38', '60', 'E7'], ['FB', '4C', '99', 'DF'], ['71', 'E4', '6E', '97']]
Round  4 :  [['72', 'A9', '0F', '69'], ['A4', 'BE', 'F5', '12'], ['11', '09', 'E9', '52'], ['6F', '5F', '1E', '4D']]
Round  5 :  [['50', '37', 'D3', '50'], ['29', 'F3', '92', '73'], ['11', '2C', '55', '10'], ['5C', '48', '4B', '87']]
Round  6 :  [['8D', 'ED', 'B8', '2C'], ['C6', '79', '92', '0B'], ['D1', 'CE', 'AE', 'A0'], ['50', 'A5', 'DF', 'D1']]
Round  7 :  [['3D', '2E', '12', '4C'], ['9A', 'E6', 'AA', '96'], ['D6', '62', '60', '74'], ['55', 'C9', '4C', '83']]
Round  8 :  [['14', '58', 'CB', 'BF'], ['B1', '3E', 'B8', '22'], ['1D', 'B9', '60', 'F1'], ['85', 'F9', '4A', '71']]
Round  9 :  [['3C', 'E6', '92', '17'], ['53', 'B1', '7A', 'AF'], ['53', 'F6', '4C', '3C'], ['B5', 'BA', 'A3', '68']]
Round  10 :  [['15', '2E', '7F', '14'], ['35', '0C', '5B', '67'], ['2C', '06', '5D', '45'], ['64', '44', '51', '5E']]
Two One Nine Two
PS C:\Users\om>
```

As you can clearly see that:

a. Verify that the ciphertext, when decrypted text will yield the original plaintext
(15 marks)
Ans: I am able to verify this without any issues.

b. Verify that the output of 1st encryption round is the same as the output of the 9th decryption round (5 marks)
Output at end of the 1st encryption round: Round 1 : [['3C', 'E6', '92', '17'], ['53', 'B1', '7A', 'AF'], ['53', 'F6', '4C', '3C'], ['B5', 'BA', 'A3', '68']]
Output at the end of the 9th decryption round: Round 9 : [['3C', 'E6', '92', '17'], ['53', 'B1', '7A', 'AF'], ['53', 'F6', '4C', '3C'], ['B5', 'BA', 'A3', '68']]

c. Verify that the output of the 9th encryption round is the same as that of the 1st decryption round (5 marks)
Output at end of the 9th encryption round :Round 9 : [['8C', '03', 'E0', 'AF'], ['EA', 'F4', 'E7', '59'], ['2E', 'DA', '59', '06'], ['66', '32', 'EE', '07']]
Output at the end of the 1st decryption round: Round 1 : [['8C', '03', 'E0', 'AF'], ['EA', 'F4', 'E7', '59'], ['2E', 'DA', '59', '06'], ['66', '32', 'EE', '07']]

For the implementation of AES I have looked at the following sources:

Official Documnetation of the AES method
https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.197.pdf

Lecture Notes on “Computer and Network Security” by Avi Kak (kak@purdue.edu) March 8, 2023 12:59 Noon ©2023 Avinash Kak, Purdue University
https://engineering.purdue.edu/kak/compsec/NewLectures/Lecture8.pdf

AES Components:
S-Box (Substitution Box) and Inverse S-Box: These are used for the SubBytes step in both encryption and decryption. The S-Box substitutes each byte of the state with another byte, and the Inverse S-Box is used for the reverse process during decryption.

Rcon: A round constant used during the key expansion phase.

MixColumns and Inverse MixColumns: These are used for mixing up bytes within each column of the state.

Key Expansion: This process involves taking the initial cipher key and deriving a set of RoundKeys from it. These RoundKeys are used in each round of the AES encryption and decryption process.

Usage:
Run the main function.
Enter the message to be encrypted.
Enter the encryption key.
The encrypted message (ciphertext) will be displayed.
The decrypted message (original plaintext) will also be displayed, showing the accuracy and functionality of the AES implementation.