The project contains three files namely server.py, client.py, aes.py and an output pdf containing screenshot of the output. The code is written in python language and is implemented in PyCharm editor.

Steps for running the code:

Step 1: Open server.py file on any python editor. Click on Run Server.

Step 2: Open client.py file on the same python editor and click on Run Client.

Step 3: The output console of the client.py will ask user to input 16-bit plaintext and 16-bit key.

Step 4: On giving input values to the output console, the client will encrypt the plain text and will print the cipher text and other parameters used in the encryption process. The client will send the ciphertext and the key to the server for decryption process.

Step 5: Click on the server.py file console, and the user can see the output of the decryption process and the plain text the user has entered.

Description and working of aes.py algorithm:

The aes.py file contains the code for implementing AES variant given in the assignment. The code consists of various functions whose explanation are given below:

1. KeyExp(key):

In this function, the key entered by the user is being passed as the parameter. It is used for generating three rounds of keys. The 16 bit key is being split into two 8 bit words w[0] and w[1].

To get the value of w[0] we Performed & bitwise operation with 1111111100000000 (0xff00) which will result into first 8 bits and the succeeding 0's will get eliminated with right shift operation.

Similar operation is used to calculate w[1] as well, the key was multiplied with 0000000011111111 (0x00ff) to get the desired result.

To get value of w[2], XOR'ed operation is performed with w[0], Round Constant and SubNib(RotNib(w[1]))

SubNib(b): This function will swap each nibble and will substitute with SBox.

For example: w[1] is 11110101. It will pass as parameter to SubNib() function.

return (SBox[11110101 >> 4] + (SBox[11110101 & 0x0f] << 4)

return (SBox[00001111] + (SBox[00000101] << 4)

return (00010111)

The value of w[3], w[4] and w[5] will be calculated in same way.

2. int_to_state(): The plain text is converted to four states in the form of vector.

3. state_to_int(): This function performs the reverse operation and converts the four states into 16 bit integer.

4. SubNibble(): This function is used for Substituting nibble from SBox.

5. ShiftRows(): In this function, Swapping of 2nd and 4th nibble takes place.

6. MixColumns(): This function is used for matrix multiplication with a constant vector. Inside the function gfmult() is called.

7. gfmult(): This function performs galois multiplication. It takes two numbers as input and performs GF multiplication i.e, it uses XOR operation for the purpose of addition.

8. enrypt(): The encrypt function is used for the encryption process. A plaintext is provided as parameter to the function and it returns the ciphertext.

9. decrypt(): The decryption is used for decryption process. A ciphertext is provided as parameter to the function and it returns the plaintext.

Description and working of client.py

In this file a client socket is created and is connected to the localhost of the server with port number 9999.

This file is basically used for the encryption process. All the functions required for the encryption process are taken from aes.py file.

The input plaintext and key are taken from the user that needs to be encrypted. The encrypt function is called with plaintext as the parameter and key expansion function is called with key as the parameter.

The encrypt function returns a ciphertext which is send to the server along with the key.

Description and working of server.py

In the server.py file, firstly a server socket is created for accepting the data from the client. The server is then bind to the localhost with port number 9999.

The server than accepts the client requests for connection and receives the ciphertext and the key that is send by the client to the server. The received ciphertext is then passed as the parameter to the decrypt function and a plaintext is returned and displayed as output.

- The screenshot of the output is given in output.pdf file inside the folder.