Report

The files for the operations are stored in data directory:

a. “/data/plaintext.txt”
b. “/data/subkey.txt”
c. “/data/result.txt”

To compile, simply clone the repository and navigate to the the src directory:

cd src

And then to execute the AESEncryption, run the following command:

python3 main.py

The following helper functions are used and they perform the following functionalities

a. **Plaintext_convert**: converts plaintext to state matrix.

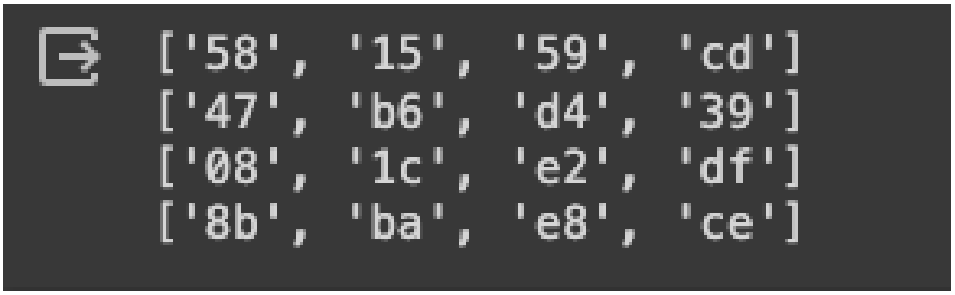
b. **Hex_to_matrix**: converts subkeys to 4 by 4 matrix

c. **Xor_with_original**: performs AddKey operation

d. **Shift_rows**: performs shiftrows operation in AES encryption

e. **Mix_columns:** performs mixcolumns operation.

The following is the screenshot at the end of round 1 of AES encryption:



```
['58', '15', '59', 'cd']
['47', 'b6', 'd4', '39']
['08', '1c', 'e2', 'df']
['8b', 'ba', 'e8', 'ce']
```