CS 5153/6053 Network Security, Spring 2023
Project 1: Advanced Encryption Standard

Margi Amin M15219371

Software: Python 3.6.3 is required to run this if you're using Windows 10.

Program Location: ..\aes_m15219371\build

Files and structure:

Build

-main.py

Data

-plaintext.txt

-subkey_example.txt

Description:

-Read the message from "../data/plaintext.txt and convert each char into ASCII(should be 128) and obtain the initial state.

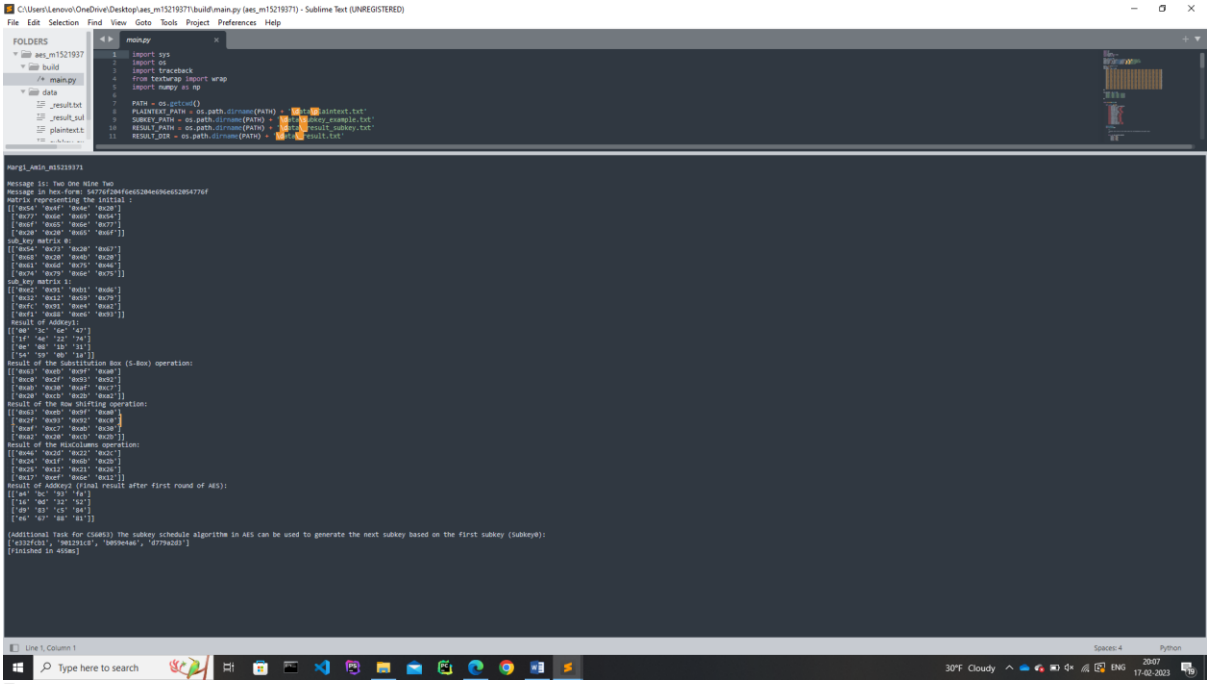
-Read the two subkeys from "../data/subkey example.txt and calculate one AddKey before Round 1 with subkey0.

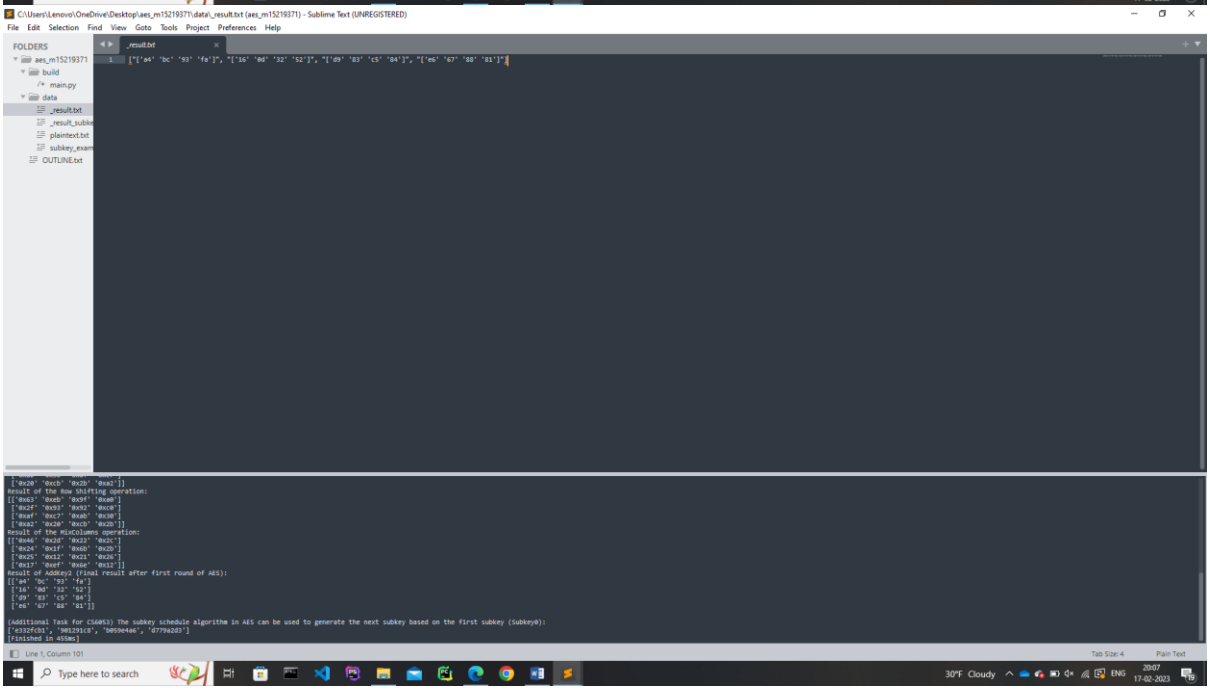
-Compute all the operations for Round 1 (SubBytes, ShiftRows, MixColumns, and one AddKey with subkey1).

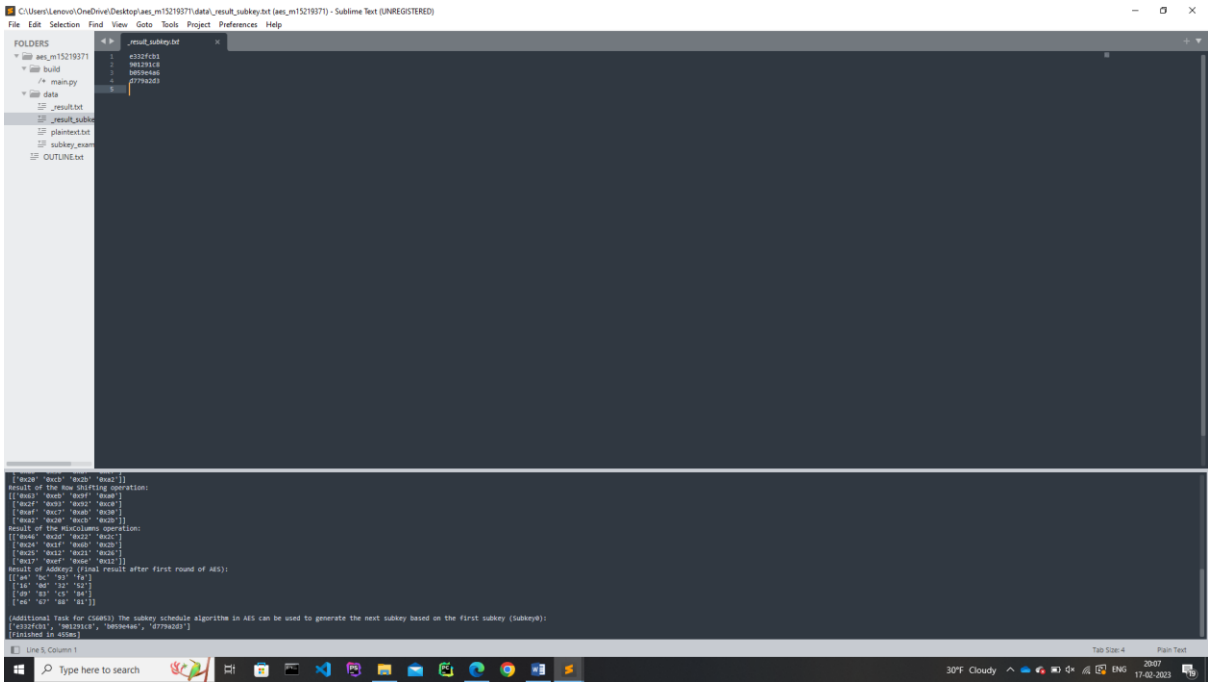
-Screenshot the output and include below.

-Read the first subkey from file "../data/subkey example.txt", generate the next subkey using subkey schedule algorithm in AES. Print the next subkey in terminal and write the result to a file

"../data/result subkey.txt". The result needs to be printed and written in hexadecimal.


C:\Users\Lenovo\OneDrive\Desktop\aes_m15219371\build\main.py (aes_m15219371) - Sublime Text (UNREGISTERED)
File Edit Selection Find View Goto Tools Project Preferences Help
FOLDERS
aes_m15219371
build
main.py
data
_result.txt
_result_sul
plaintext.t
main.py
import sys
import os
import traceback
from textwrap import wrap
import numpy as np
PATH = os.getcwd()
PLAINTEXT_PATH = os.path.dirname(PATH) + '\\data\\plaintext.txt'
SUBKEY_PATH = os.path.dirname(PATH) + '\\data\\subkey_example.txt'
RESULT_PATH = os.path.dirname(PATH) + '\\data_result_subkey.txt'
RESULT_DIR = os.path.dirname(PATH) + '\\data_result.txt'
Margi_Amin_m15219371
Message is: Two One Nine Two
Message in hex-form: 54776f204f6e65204e696e6520547 6f
Matrix representing the initial :
[['0x54' '0x4f' '0x4e' '0x20']
['0x77' '0x6e' '0x69' '0x54']
['0x6f' '0x65' '0x6e' '0x77']
['0x20' '0x20' '0x65' '0x6f']]
sub_key matrix 0:
[['0x54' '0x73' '0x20' '0x67']
['0x68' '0x20' '0x6b' '0x20']
['0x61' '0x6d' '0x75' '0x46']
['0x74' '0x79' '0x6e' '0x75']]
sub_key matrix 1:
[['0xe2' '0x91' '0xb1' '0xd6']
['0x32' '0x12' '0x59' '0x79']
['0xfc' '0x91' '0xe4' '0xa2']
['0xf1' '0xb8' '0xe6' '0x93']]
Result of AddKey1:
[['00' '3c' '6e' '47']
['1f' '4e' '22' '74']
['0e' '08' '1b' '31']
['54' '59' '0b' '1a']]
Result of the Substitution Box (S-Box) operation:
[['0x63' '0xeb' '0x9f' '0xa0']
['0xc0' '0x2f' '0x93' '0x92']
['0xab' '0x30' '0xaf' '0xc7']
['0x20' '0xcb' '0x2b' '0xa2']]
Result of the Row Shifting operation:
[['0x63' '0xeb' '0x9f' '0xa0']
['0x2f' '0x93' '0x92' '0xc0']
['0xaf' '0xc7' '0xab' '0x30']
['0xa2' '0x20' '0xcb' '0x2b']]
Result of the MixColumns operation:
[['0x46' '0x2d' '0x22' '0x2c']
['0x24' '0x1f' '0x6b' '0x2b']
['0x25' '0x12' '0x21' '0x26']
['0x17' '0xef' '0x6e' '0x12']]
Result of AddKey2 (final result after first round of AES):
[['a4' 'bc' '93' 'fa']
['16' '0d' '32' '52']
['d9' '83' 'c5' '04']
['e6' '67' '88' '01']]
(Additional Task for CS6053) The subkey schedule algorithm in AES can be used to generate the next subkey based on the first subkey (Subkey0):
['e332fcb1', '981291c8', 'b059e4a6', 'd779a2d3']
[Finished in 455ms]
Line 1, Column 1
Spaces:4
Python
Type here to search
30°F Cloudy
ENG
20:07
17-02-2023


C:\Users\Lenovo\OneDrive\Desktop\aes_m15219371\data_result.txt (aes_m15219371) - Sublime Text (UNREGISTERED)
File Edit Selection Find View Goto Tools Project Preferences Help
FOLDERS
aes_m15219371
build
main.py
data
_result.txt
_result_subke
plaintext.txt
subkey_exam
OUTLINE.txt
_result.txt
[["['a4' 'bc' '93' 'fa']", "['16' '0d' '32' '52']", "['d9' '83' 'c5' '04']", "['e6' '67' '88' '01']"]
['0x20' '0xcb' '0x2b' '0xa2']]
Result of the Row Shifting operation:
[['0x63' '0xeb' '0x9f' '0xa0']
['0x2f' '0x93' '0x92' '0xc0']
['0xaf' '0xc7' '0xab' '0x30']
['0xa2' '0x20' '0xcb' '0x2b']]
Result of the MixColumns operation:
[['0x46' '0x2d' '0x22' '0x2c']
['0x24' '0x1f' '0x6b' '0x2b']
['0x25' '0x12' '0x21' '0x26']
['0x17' '0xef' '0x6e' '0x12']]
Result of AddKey2 (final result after first round of AES):
[['a4' 'bc' '93' 'fa']
['16' '0d' '32' '52']
['d9' '83' 'c5' '04']
['e6' '67' '88' '01']]
(Additional Task for CS6053) The subkey schedule algorithm in AES can be used to generate the next subkey based on the first subkey (Subkey0):
['e332fcb1', '981291c8', 'b059e4a6', 'd779a2d3']
[Finished in 455ms]
Line 1, Column 101
Tab Size:4
Plain Text
Type here to search
30°F Cloudy
ENG
20:07
17-02-2023


C:\Users\Lenovo\OneDrive\Desktop\aes_m15219371\data_result_subkey.txt (aes_m15219371) - Sublime Text (UNREGISTERED)
File Edit Selection Find View Goto Tools Project Preferences Help
FOLDERS
aes_m15219371
build
main.py
data
_result.txt
_result_subkey.txt
plaintext.txt
subkey_exam
OUTLINE.txt
_result_subkey.txt
e332fcb1
981291c8
b059e4a6
d779a2d3
['0x20' '0xcb' '0x2b' '0xa2']]
Result of the Row Shifting operation:
[['0x63' '0xeb' '0x9f' '0xa0']
['0x2f' '0x93' '0x92' '0xc0']
['0xaf' '0xc7' '0xab' '0x30']
['0xa2' '0x20' '0xcb' '0x2b']]
Result of the MixColumns operation:
[['0x46' '0x22' '0x22' '0x7c']
['0x24' '0x1f' '0x6b' '0x2b']
['0x25' '0x12' '0x21' '0x34']
['0x17' '0xef' '0x6e' '0x12']]
Result of AddKey2 (final result after first round of AES):
[['a4' 'bc' '93' 'fa']
['16' '0d' '32' '62']
['d9' '83' 'c5' '04']
['e6' '62' '88' '01']]
(Additional Task for CS6053) The subkey schedule algorithm in AES can be used to generate the next subkey based on the first subkey (Subkey0):
['e332fcb1', '981291c8', 'b059e4a6', 'd779a2d3']
[Finished in 455ms]
Line 5, Column 1
Tab Size: 4
Plain Text
Type here to search
30°F Cloudy
ENG
20:07
17-02-2023