Network Security Project 1 Report Aiden Frank

This project was written on the **Windows** operating system in **Python 3.13.2** using **Visual Studio Code**.

You can find the repository of the project here:

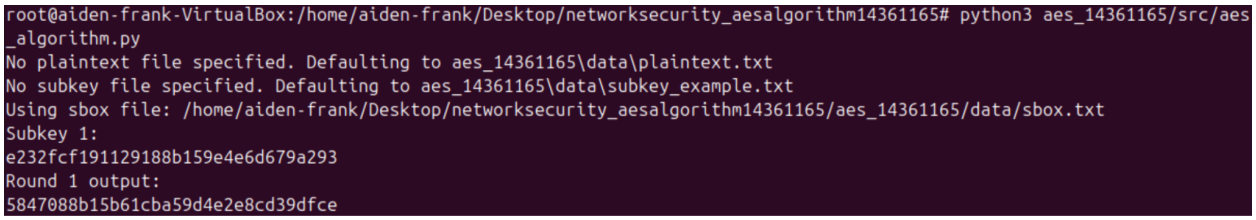
https://github.com/AidenFrank/networksecurity_aesalgorithm14361165

How to use:

In order to use this project, you must have python downloaded. On your computer, navigate to https://www.python.org/ and download the latest version of Python, or version 3.13.2.

Linux:

Copy the networksecurity_aesalgorithm14361165 folder over to your linux machine. Within the networksecurity_aesalgorithm14361165 folder, run the command "python3 aes_14361165/src/aes_algorithm.py".

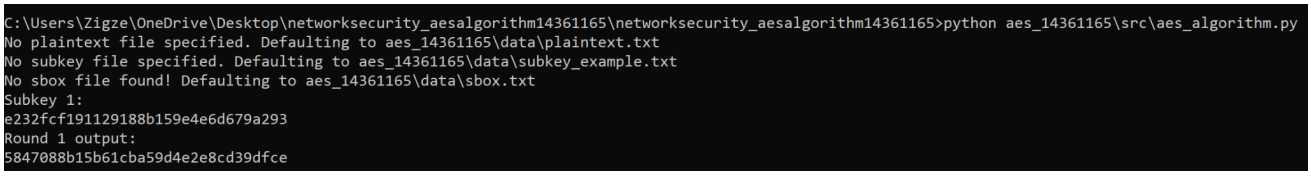


You should get similar output to the screenshot above.

You can find the output written to a file under "\aes_14361165\data\result.txt" and "\aes_14361165\data\result_subkey.txt".

Windows:

Copy the networksecurity_aesalgorithm14361165 folder over to your Windows machine. Within the networksecurity_aesalgorithm14361165 folder, run the command "python aes_14361165/src/aes_algorithm.py".

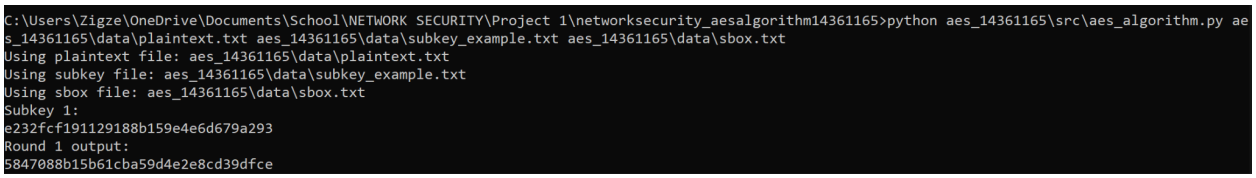


You should get similar output to the screenshot above.

You can find the output written to a file under "\aes_14361165\data\result.txt" and "\aes_14361165\data\result_subkey.txt".

Important Note:

In the event that the command can't find a data file, you can specify the path to a file in the arguments of the command. See this example:



After "python aes_14361165/src/aes_algorithm.py", specify the file path of the plaintext, subkey, and sbox in that order.

How the Project was Completed:

This project was written in Visual Studio Code in Python. I began by creating functions for each part of the AES process and then systematically went through each step of AES checking to make sure my output matched what was in the AES lectures. I also wrote comments to explain my logic for each function and its steps. The main confusion through the project came from performing XORs and other arithmetic with integers, and then converting the data to hex values to check my work. The hardest function to write was the MixColumns function. After writing up the logic for the AES round, I wrote the code for the subkey schedule. Once this was complete, I formatted the data correctly and made some adjustments to how files were read and written to.