Homework Number: 5
Name: Dylan Huynh
ECN login: huynh38
Due Date: 2/21/2023

For this code, my AES program from last week worked, so I just imported the code for encryption, and left out the steps that were required for decryption.

For X931 random number generating, the code calls a function with a seed for the start value and a date and time value. The program encrypts the date and time with AES, and does a looping structure based on the amount of numbers required to be generated. To generate a random number, it takes the seed value which was either the starting argument or the one calculated in the previous round of the loop, and XORs the encrypted date and time with the seed, and then the encryption of the product of the XOR is the random number. The generated random number is XORed with the encrypted date and time, and the encrypted output of that XOR becomes the seed of the next step. All of the random numbers are held in an array and returned.

For AES_image using CTR, it first reads in the 3 lines of the ppm file and directly inserts them into the output file, because they are the parameters of the generated image and should not be encrypted. After that, the file is read 16 bytes at a time into a ‘byte’ class, which is used to construct a bitvector. This bit vector is XORed with the encrypted output of the initialization vector. The initialization vector’s value is then added to by one, and this is done for every block until the file has no more bytes to read.

This version of encrypting which will make a vastly different output of the block, even if the block is the same as the previous block. This is because the output of AES encryption produces a large difference based on 1 change in the plaintext, which the counter does by adding 1 to the initialization vector everytime. The difference is palpable in the difference between the AES encryption from this homework and the DES encryption from homework 2. In homework 2, the encryption of the whitespace makes it very clear that the encryption is a helicopter, because all of the white pixels are encrypted to make the same output. The DES encryption is using ECB, which has a weakness in repetitive structures because the same input of DES will produce the same output. Because the AES encryption uses counter mode, it will make a different output even if the input block is the same because it does not apply AES on the input block, instead it applies AES on a separate vector. This makes it so that there is no discernable pattern within the output, despite the amount of whitespace blocks contained in the image.