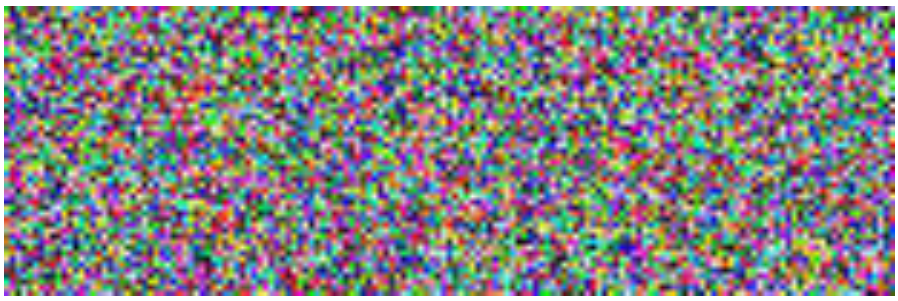
Homework Number: 5
Name: Dulani Wijayarathne
ECN Login: dwijayar
Due Date: 2/21/2023

Problem 1

I simply followed the PRNG function from the lecture diagram. First the date/ time bit vector is encrypted with my AES encrypt function with the key given. A for loop is run for totalNum times it is needed. The seed bit vector is then xored with the encrypted date/time. This becomes the generated random number, and it is appended to a list. Random number is xored with encrypted date/time and is encrypted. This encrypted output is used as the new seed.

Problem 2

I used similar code to DES image where each 128-bit chunks were read in a while after extracting the header from the image file. Inside the while loop is a simple code where a bit vector is produced by incrementing the initialization vector in each round. The incremented initialization vector is encrypted using the implemented AES function. The encrypted initialization vector is xored with the bitvector of the plaintext from the image. This becomes the ciphertext and is written to the output file in each round of the while loop.



Encrypted Image

When using DES the encryption the traces of the original image was still visible. I could still see outline of the original image. But when AES encryption is used in Counter Mode, the original image cannot be traced. The original image is fully blurred out.