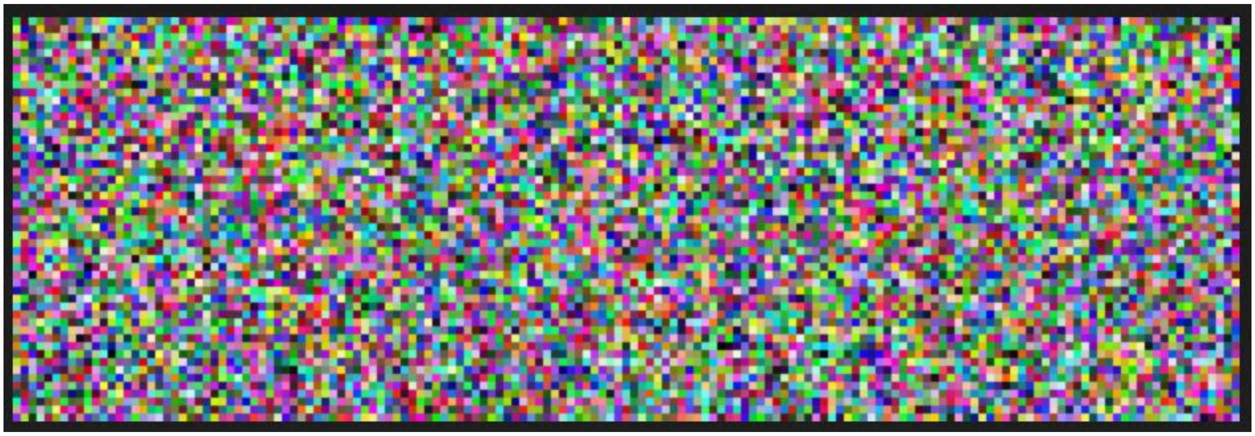
HW05: PRNG and CTR Mode

Homework Number: 04
Name: Jack Gardner
ECN Login: gardne97
Due Date: 2/21/23

CTR Explanation: This AES CTR mode implementation takes in an initialization vector, an input file, output file, and encryption key. The first three lines of the input file are written to the output file without any encryption, representing the images ppm header. The initialization vector is encrypted using 256 bit key AES and then xored with the plaintext. After each 128 bit section of the initialization vector is encrypted, then a numerical value of one is added to the initialization vector and after it is encrypted it is xored with the next section of the plaintext. This is repeated for the entirety of the plaintext, yielding the ciphertext.

PRNG Explanation: x391 PRNG works by taking in an initialization vector, the date and time, and an encryption key. To generate a random number, the Date and time is encrypted using 256 bit key AES and xored with the initialization vector. This output is encrypted once again, yielding the first random number. To get the next initialization vector, the encrypted date and time is xored with the last generated random number. This result is encrypted once again, yielding the initialization vector. This process is repeated as many times as random numbers are needed. This implementation uses a constant date and time inputted by the user but could easily be modified to pull the current date and time from the computer.

Encrypted image:



How this image differs from HW2: The encrypted image in homework 2 still has an image of the helicopter visible, even if the colors are different. This is because each group of background pixel undergoes the same encryption process in regular DES mode, resulting in those pixels having the same color pattern, which reveals the background of the image. When you encrypt the same image using AES CTR mode, the position of the pixel affects the encryption process due to the presence of the counter vector. This masks the background and renders the helicopter inviable in the encrypted image.