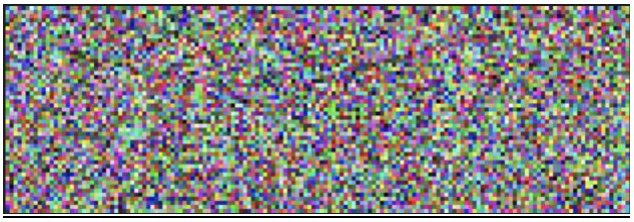
Chan Ng Cashin
ECE 404
HW 05

Problem 1:

Description

In my ctr_aes_img function I encrypted the image using the parts of the encrypt function I had already built in HW04. Using this I encrypted the iv variable using the key then XORed that with the plaintext bitvector of the current block. I kept iterating like so until the enc_image file was fully encrypted.

enc_image.ppm



Problem 2:

Description

To develop my random numbers, I followed the block diagram given in lecture 10. Iterating in the range of the total number given in the function call I first encrypted dt using a previously built encrypt function. Next, I XOR this encrypted dt with the v0 variable getting passed into the function. Next, I encrypted this XORed value. I added this number to the list holding the random numbers and then encrypted this random number XORed with the encrypted dt and stored it as the new v0 value.

random_numbers.txt

331374527193731622526773163027689011175
262633037080229609278739248627548891 87
621388110439928640615094882415799550 8
317525806849049200816126045738729418009
240080400546264647934751409092776671804