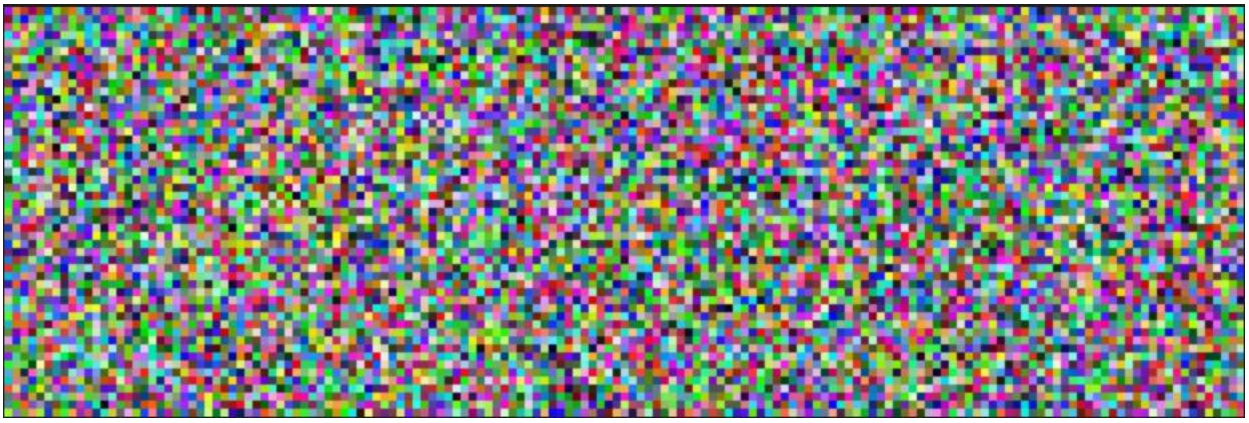
Luke Canfield ECN Login: lcanfiel Due Date: 2/10/2024

HW05 ECE 40400

Encrypted Image for Problem 1



Brief Explanation of Code for Problem 1

I modified my encrypt function from HW4 so that the inputs to the function are now the IV vector, the key_words, and the subBytesTable instead of the plaintext and ciphertext files. I also removed all of the file handling from the encrypt function and also returned the state_array instead of the function being void. For the ctr_aes_image function I initialized the key_words and subBytesTable variables and then initialized a bitvector as the input file so I could read the header from the image.ppm file and write it to the enc_image.ppm file before reading bits from the bitvector I created. Then I implemented through the steps as shown in the diagram from lecture 9 and encrypted the IV in my modified encrypt function. Then I created a bitvector of the returned state array and Xored it with the plaintext and set that as cipher_block. Then I increased the IV vector by 1 and wrote the cipher text to the enc_image.ppm file. This process repeats until there are no more bits to read from the file.

5 Pseudo-Random Numbers for Problem 2

331374527193731622526773163027689011175

262633037080229609278739248627548891 87

621388110439928640615094882415799550 8

317525806849049200816126045738729418009

240080400546264647934751409092776671804

Brief Explanation of Code for Problem 2

For the x931 function I just went off the diagram shown in lecture 10 and implemented each part of the process switching out EDE for AES as instructed. I created a while loop which creates the number amount specified from the command line. Before the while loop, I encrypted ‘dt’ and created a new bitvector variable equal to the state array so I could use it for the Xor operations within the while loop. I originally had this in the while loop but realized it only needed to be calculated once. In the while loop I opened the outfile and then calculated the random number as a bitvector for each iteration of the process (as well as the next v0) and set it to an output variable which was then written to the outfile.