Homework Number: 5

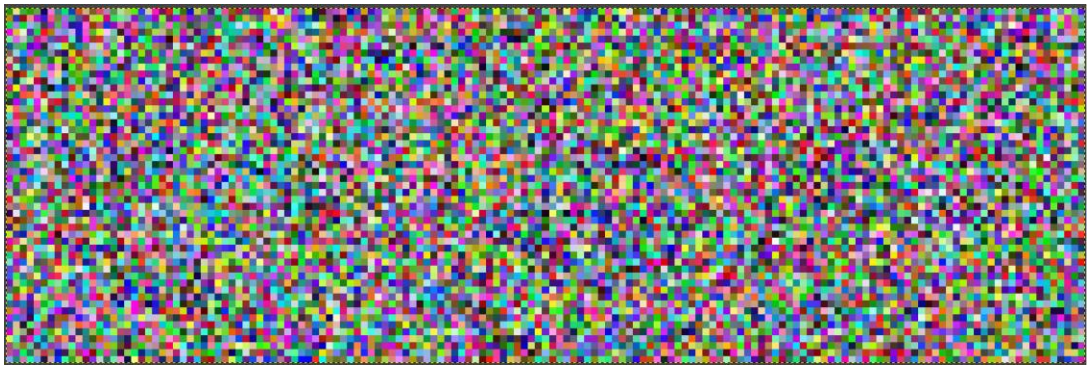
Name: Andrew Wu

ECN Login: wu1795

Due Date: 2/20/24

For my code, I first altered my AES encryption to take in only a bitvector variable and return a bitvector variable. This is due to the way I programmed by ctr_aes_image and x931 functions. Furthermore, I also removed the while loop, moved the key gen to the init part of the file, and made the encrypt function encrypt once, instead of running through the entire inputted bitvector, and moved the while loop to the other two functions. For ctr_aes_image, I opened the image file and read through the first three header lines, then created a while loop that encrypts the initialization vector, read the input image file 16 bits at a time, XOR the encrypted initialization vector and the 16 bits as the cipher text, wrote it to the output, and incremented the initialization vector. The while loop stops when the number of bits read is equal to zero. For the x931 function, I encrypted the date and time bitvector and created a set containing the v0 value. I then created a for loop that loops totalNum times, and follows the x931 encryption chart in the notes. I obtain the Vj value based on totalNum, I XOR the date and time with the Vj value and encrypt it. I then write it to the output file and use the output from the encryption and XOR it again with the encrypted date and time. From there I once more encrypt the XOR and append that value to the set containing v0, creating Vj+1.

Encrypted Image:



5 pseudo-random numbers:

331374527193731622526773163027689011175

262633037080229609278739248627548891 87

621388110439928640615094882415799550 8

317525806849049200816126045738729418009

240080400546264647934751409092776671804