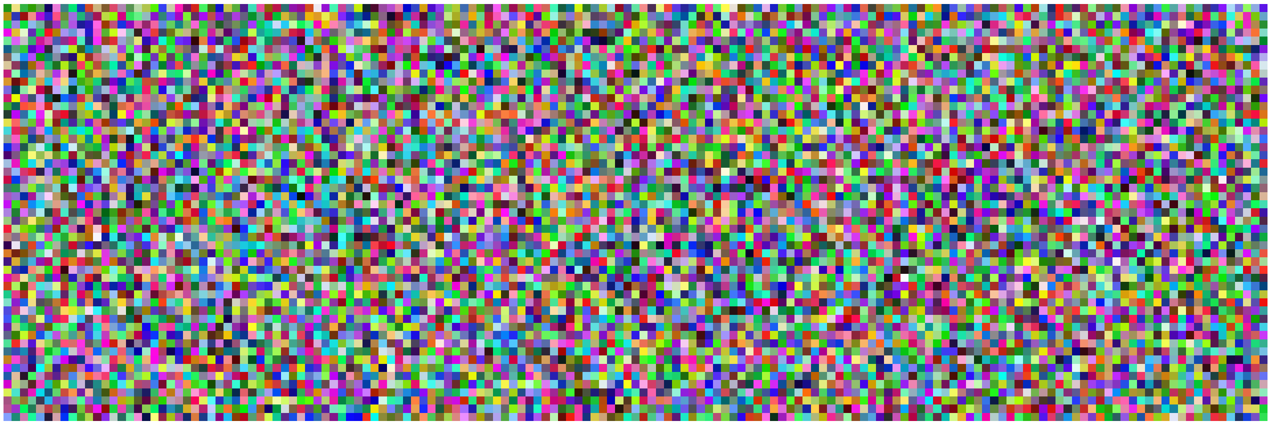
Anish Laddha
Professor Avinash Kak
ECE404
February 19 2024

Homework 5

Problem 1 Encrypted Image:



Problem 2 Random Numbers:

33137452719373162252677316302768901175
26263303708022960927873924862754889187
62138811043992864061509488241579955508
31752580684904920081612604573872941800 9

Code Explanation:

For problem 1, we encrypt an image using AES in counter encryption mode.
To do this, we first load the image’s bits into a bitvector, then we pad it so that The bitvector can be iterated through in chunks of size 128. Then, using the previous split headers function from HW2, we split it into a header and the actual “plaintext” data. We write the header into the encrypted img file as that should stay the same. We then iterate through 128-bit chunks of the plain bitvector. We run AES on the provided initial vector (using our HW4 algorithm), XOR the result with our plaintext block, and then write that into our encrypted image. At every iteration, we increase the value of the initial vector by 1.

For the second, we are generating pseudo random numbers using AES with ANSI X9.31. We first set i_bv equal to the datetime run through AES encryption (AES encryption will use the algorithm from the last HW). We set v to the provided initial value v0. Then we iterate once for every number we want to generate (5 in this case). Our random number is the AES encryption of i_bv XORed with v, which we write to our file. We update v to be equal to the AES encryption of our random number XORed with i_bv.