

Homework Number: HW05

Name: Raghava Vivekananda Panchagnula

ECN Login: rpanchag

Due Date: 2/20/2024

Output for Problem 1:



Output for Problem 2:

331374527193731622526773163027689011175

26263303708022960927873924862754889187

6213881104399286406150948824157995508

317525806849049200816126045738729418009

240080400546264647934751409092776671804

Code Explanation:

- `block_encrypt`
 - I made a new function called `block_encrypt` that only performs the 14 rounds of the AES encryption algorithm and returns the resultant bitvector as an output. It works the same way that my function from homework 4 works, so for further detail please refer to that.
- `ctr_aes_image`
 - This function reads the first 3 lines of the input image and writes it to the output as is.
 - It then reads the whole file again as a bv, discards the first 112 bits which is what the length of the header was, and then begins the encryption process.
 - In this process, first, it takes the initial value and encrypts it with the roundkeys. It then xors it with the 128 bits from the image. It then increments the iv by 1 and adds the result from the xor to the file and moves on to the next 128 bits.
- `x931`
 - This function takes the `dt` value to create an “encoder” variable that I will use for subsequent operations. I then, for each of the numbers we have to create and output, I take the encoder variable I made, xor it with the seed, and then generate the random

number by inputting it into my `block_encrypt` function. I then generate a new seed by xoring the encoder value with the previously created random number and then putting it through the `block_encrypt` function again. I then write the generated random values to a new file.