

Ethan James
33378430
Epjames

HW05

Problem 1:

In problem one I was tasked with using AES to encrypt the image given to us. I first write the header to the output file. Then I read in a block of bits from the image file. I pad it. Then send the initialization factor to my modified encryption function to be encrypted. It does all the encryption on that and then it is returned to me. Then using what is returned, I xor it with a block from the image. Then I increment the initialization vector by one and we do the same process.

IMAGE:



Problem 2:

Problem two essentially uses EDE to create random numbers. I do this with a series of encryption functions calls and xoring given the amount of numbers I want with a given seed. I then output this to an output file.

Numbers:

331374527193731622526773163027689011175
26263303708022960927873924862754889187
6213881104399286406150948824157995508
317525806849049200816126045738729418009
240080400546264647934751409092776671804