Homework Number: 05
Name: Samitha Ranasinghe
ECN Login: sranasi
Due Date: 02/21/2023

Problem 1

I referred to the Figure 4 in Lecture 10 to implement the general ANSI X9.31 PRNG algorithm where the date time is first encrypted and then a loop is initiated. Inside the loop, a round key is generated by encrypting the XORed value of the encrypted date time value and a random number generated by encrypting the XORed value of the previous random number and encrypted date time value. For the first round, the random number would be a seed value provided for the function. The loop is repeated until the needed number of random numbers are generated.

For encryption, AES is used rather than EDE which is done using the implementation from the previous homework. The changes made are:

- The round keys are generated once and sent when AES is called rather than generating every time.
- Since the generated random number and the values used for producing it are all 128 bits, the AES algorithm encrypts only 1 block and doesn't iterate over several blocks.
- The functions used for decryption are removed and the code that produces the table for Inverse Byte substitution is removed.

Problem 2

A similar strategy for encryption of the image in Homework 2 was used. The changes made were the implementation of AES from Homework 4 rather than DES for encryption and the encryption of a counter rather than the actual plain text and then XORed with the plain text to produce the cypher text as Counter Mode was used. The counter was initialized with the provided initialization vector and then incremented by 1 in every loop and then the modulus with 2^{128} taken so that it doesn't go above 128 bits. The changes in AES are the removal of all functionalities needed for decryption as it is not needed for the problem.

Encrypted PPM Image:

When using DES, the outline of the helicopter in the picture to be encrypted still remains in the encrypted image and the object can be figured out because the Electronic Code Book Mode was used. The blocks are encrypted independently and therefor since most of the blocks are the same due to the same color in the area, the output is also the same for most areas except the outline. Using Counter Mode has solved the problem of visual recognition as can be seen where no trace of the helicopter is left. This is because a counter is used and incremented with every block so that even though two plaintext blocks are the same, the produced encrypted blocks would be different.