**Homework Number:** 02

**Name:** Samitha Ranasinghe

**ECN Login:** sranasi

**Due Date:** 01/26/2023

**Problem 1**

**Plaintext message:**

In the unforgiving world of Formula One, Lewis Hamilton abides at the top. He's the man to beat, the top earner, the most important voice, the most prominent figure - a Black man alone at the summit of motorsports' highest echelon. England's knight in Mercedes armor. Over the past 15 years, the 36-year-old Briton has won seven world championships, tying the record set by Ferrari's Michael Schumacher - the German F1 driver who was regarded as the greatest of all time until Hamilton broadsided him from that perch. At Sunday's Russian Grand Prix, Hamilton rallied through a late rain shower to claim the checkered flag on the way to becoming the first driver in the sport's history with 100 career victories. And that's besides his 100 career pole positions. As achievements go in racing, this is beyond otherworldly.

**Key:** zoomzoom

**Encrypted message:**



**Decrypted message:**

In the unforgiving world of Formula One, Lewis Hamilton abides at the top. He's the man to beat, the top earner, the most important voice, the most prominent figure - a Black man alone at the summit of motorsports' highest echelon. England's knight in Mercedes armor. Over the past 15 years, the 36-year-old Briton has won seven world championships, tying the record set by Ferrari's Michael Schumacher - the German F1 driver who was regarded as the greatest of all time until Hamilton broadsided him from that perch. At Sunday's Russian Grand Prix, Hamilton rallied through a late rain shower to claim the checkered flag on the way to becoming the first driver in the sport's history with 100 career victories. And that's besides his 100 career pole positions. As achievements go in racing, this is beyond otherworldly.

**Brief Explanation:**

Contains code for encrypting and decrypting a message using DES with a specified key.

The encrypt function uses functions provided in lecture notes to obtain the encryption key after first permutation and then a list of round keys. A bitvector file object is created with the file containing the message to be encrypted and then blocks are grabbed at 64-bit sizes to be encrypted. The block is padded with null bits if a block is less than 64 (usually needed for the last block) and normal Feistel function is run on the right half of the block. Expansion permutation, xoring with the round key, a function called for substitution with s-boxes and p-box permutation is done before xoring with left half of the block and repeated where result from Feistel function gets sent to right half and previous right half sent to left half. This process is done 16 times and resulting string written into output file as a hex string.

The decrypt function is similar to encrypt function except the string is read as a hex string into the bitvector and a for loop used to grab 64-bit blocks and the round key order is reversed. The decrypted strings are written into the output file each time a block is decrypted

**Problem 2**

**Input image:**



**Key:** zoomzoom

**Encrypted Image:**



**Brief Explanation:**

The code is very similar to the previous problem with the difference being only a changed encrypt function exists which is adjusted to read data from a ppm file, encrypt the data and write the encrypted data to another ppm file. The first three lines are written straight from the input file to the output file as this is the header of the ppm file and cannot be encrypted. The rest of the data is read and loaded into a bitvector as raw bytes and the DES encryption applied as described in the previous problem before being written into the output file.