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:

36d2e582921b6b4a4729ec8a60a4915ba76f3fec1c010014c13444b4afbefb124743582e779a
57cf992d871fcd7e178fe0c5b2c8ccc1a78fcae1aab4c09dd92388d20af1deaf36212e9fad48d6
cf32d8299cf7bfe82e8faa32b3383d1877fb86eb489571936cdcda5d32f1bc9a359bd63f41130
5859fec912107c147cb77b2f459f944561933e2ca54416929a35c2ce30438568de299dac4a33
811a43d6b1e6ec75f86e0768b8ff5eea71a6bb8907125a17a19997c153b4665123bf24bfe084f
129a72292fe22fadf0ab59a06babc93f9aecc82545e35920fa68a6eea18322458bf5a0fe9e506
95326cb0ff211484b883a677b20a3318584f058b818fa594e9bb2744c67a5ba2ad2d65e39d45
22476efa8770e1bf5547cc90f12f73ec93102586e55c8a8e6bdeb8e16205040647bbcb8be20b
29d589da8c3fa2a9ec2f00dc056046c299bbb1532ef8c38b24c021558175055c4a95a1b193de
ec41112afa5db015fbac30c6c95c83e3cb07f9b28c849b0330d4b4e84abf996f91ae58a499a44
b87340c11ca00748b00072d7bf22bb383f3f2e2aa185921e974e23fc695bab5c2ddd27d5fa0e
6e6de2af262f2608fa8cbc25bfbdc4f5f8f0f785a1b4d4c63fa94f0c16601d8cff74856ca0a1ca8e
1167db0a5a55e7dbb246202ae59835c16e90c1e0c5b2c8ccc1a78f726e8963d971baba5db79
b6739f3fa4329acdfef24b1b13d361832c5bd814d7acf7059e1b251f74e604116ecb90755cc43
a12639c01917653cd945c9065737efa9401947fb9557568b567bdf059a474f95217f55ba63b3
ed666854c2dda688b6acf0722076e3fd18d59b9109d4639c5a10dcc9dd17a3e78fe956fb9687
276ad8aefbfa2764ab669e7444e751fc396940fee2446b2e40d29f277a46ab9781445b25725c
d74215a01694f2566b33456851c5966303a2053f6a22d41581fa810f1668eb7761db9206b46
6a8a65e50171f030c680a971cffd17e583060cd6e32ec5bd4ba1f9bda5976a883327bada1169
74b7e8220290949d5315cd4d308e297b7789bcf7466c433e6effef150ea4a44df492f44950904
4104c47b32351b272672fc599ea6926482920a08dd08cfdfdd19ae50585efebe84f51afbd7487
e04b5e127457e37e615da2b55fafc317fecebf59a

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:

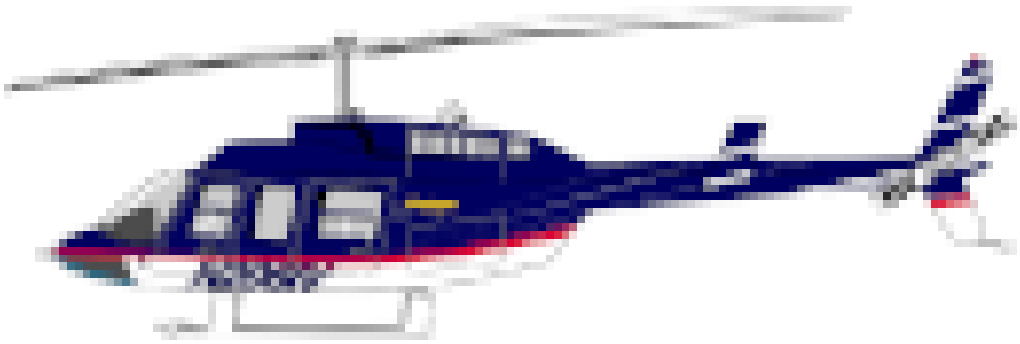
Contains code for encrypting and decrypting a message using DES with a specified key.

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

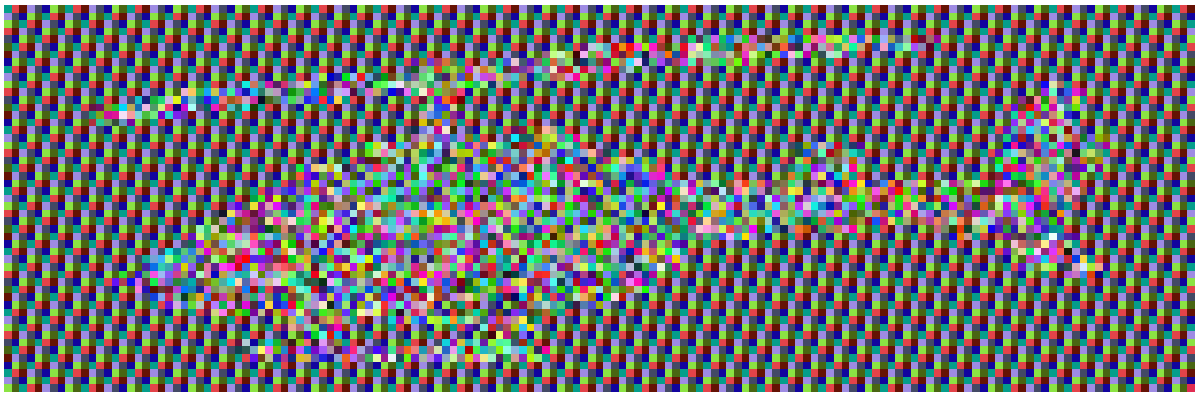
Problem 2

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.