ECE 404 HW2

1. For the first problem, I first added the lists required to permutate the blocks, which were the substitution blocks, the key permutation to make round keys and to permute the key, and the pbox permutation data. I also added the shift data to make the round keys. The encryption and decryption functions both start off using the get_cipher_key function and the generate_round_key function. The get_cipher_key function reads the given file which contains an 8 character key, and permutes it using the key permutation 1 variable, which is the used to call generate_round_key which makes 16 round keys by looping through each index of the left and right halves of the key, and shifting and permuting to get the round key. Next it takes the plaintext and breaks it into blocks of 64, which is then split into a left and right half, the right half is then changed from 32 to 48 bits by permuting with the expansion matrix. Then the expanded half is XORed with the round key depending on the round of encryption, from 0-15. Then the block is substituted by taking the 16 new bits and using them to substitute them by assigning a row and column to substitute. Then that substitution made half is purmuted using the p-box permution which moves the indexes based on what the table says its new index should be. All of this code was taken from the source code of the lecture notes and meshed together. I also made the rounds iterate 16 times in order to get a full Feistel structure of encryption, which at the end of the round the left half and right half need to be swapped again. What I added that was new was adding a null byte if the bit that was read was not a multiple of 64. For decryption, everything was the same except I took the ciphertext file as a string and used that to construct the bitvector to undergo decryption. I also reversed the round_keys variable to make it so that the round go in reverse so that LD[0] = RE[16].

ciphertext:
36d2e582921b6b4a4729ec8a60a4915ba76f3fec1c010014c13444b4afbefb124743582e779a57c
f992d871fcd7e178fe0c5b2c8ccc1a78fcae1aab4c09dd92388d20af1deaf36212e9fad48d6cf32d8
299cf7bfe82e8faa32b3383d1877fb86eb489571936cdcda5d32f1bc9a359bd63f411305859fec91
2107c147cb77b2f459f944561933e2ca54416929a35c2ce30438568de299dac4a33811a43d6b1e
6ec75f86e0768b8ff5eea71a6bb8907125a17a19997c153b4665123bf24bfe084f129a72292fe22f
adf0ab59a06babc93f9aecc82545e35920fa68a6eea18322458bf5a0fe9e50695326cb0ff211484b
883a677b20a3318584f058b818fa594e9bb2744c67a5ba2ad2d65e39d4522476efa8770e1bf554
7cc90f12f73ec93102586e55c8a8e6bdeb8e16205040647bbcb8be20b29d589da8c3fa2a9ec2f00
dc056046c299bbb1532ef8c38b24c021558175055c4a95a1b193deec41112afa5db015fbac30c6c
95c83e3cb07f9b28c849b0330d4b4e84abf996f91ae58a499a44b87340c11ca00748b00072d7bf2
2bb383f3f2e2aa185921e974e23fc695bab5c2ddd27d5fa0e6e6de2af262f2608fa8cbc25bfbdc4f5f
8f0f785a1b4d4c63fa94f0c16601d8cff74856ca0a1ca8e1167db0a5a55e7dbb246202ae59835c16
e90c1e0c5b2c8ccc1a78f726e8963d971baba5db79b6739f3fa4329acdfef24b1b13d361832c5bd
814d7acf7059e1b251f74e604116ecb90755cc43a12639c01917653cd945c9065737efa9401947f
b9557568b567bdf059a474f95217f55ba63b3ed666854c2dda688b6acf0722076e3fd18d59b9109
d4639c5a10dcc9dd17a3e78fe956fb9687276ad8aefbfa2764ab669e7444e751fc396940fee2446
b2e40d29f277a46ab9781445b25725cd74215a01694f2566b33456851c5966303a2053f6a22d41
581fa810f1668eb7761db9206b466a8a65e50171f030c680a971cffd17e583060cd6e32ec5bd4ba
1f9bda5976a883327bada116974b7e8220290949d5315cd4d308e297b7789bcf7466c433e6effef

150ea4a44df492f449509044104c47b32351b272672fc599ea6926482920a08dd08cfdfdd19ae50585efebe84f51afbd7487e04b5e127457e37e615da2b55fafc317fecebf59a
Decrypted plaintext:
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. (There are 2 null bytes at the end)

2. For the second problem, the steps within the rounds was the same as encryption, the only difference was reading the inputs in as a binary file instead of text, which I re-used the first 3 lines to make same header for the ppm files. I also changed the way the output was written as a binary file, and instead of writing the output of the encryption as a hexstring, I wrote them into the ppm file as bits. As the bits were taken in blocks of 64, the helicopter is very noticable as shown below.