ECE 404 Homework 2

Problem 1

Key: zoomzoom

Encrypted Text:

36d2e582921b6b4a4729ec8a60a4915ba76f3fec1c010014c13444b4afbefb124743582e779a57cf9
92d871fcd7e178fe0c5b2c8ccc1a78fcae1aab4c09dd92388d20af1deaf36212e9fad48d6cf32d8299
cf7bfe82e8faa32b3383d1877fb86eb489571936cdcda5d32f1bc9a359bd63f411305859fec912107
c147cb77b2f459f944561933e2ca54416929a35c2ce30438568de299dac4a33811a43d6b1e6ec75f
86e0768b8ff5eea71a6bb8907125a17a19997c153b4665123bf24bfe084f129a72292fe22fadf0ab59
a06babc93f9aecc82545e35920fa68a6eea18322458bf5a0fe9e50695326cb0ff211484b883a677b20
a3318584f058b818fa594e9bb2744c67a5ba2ad2d65e39d4522476efa8770e1bf5547cc90f12f73ec
93102586e55c8a8e6bdeb8e16205040647bbcb8be20b29d589da8c3fa2a9ec2f00dc056046c299bb
b1532ef8c38b24c021558175055c4a95a1b193deec41112afa5db015fbac30c6c95c83e3cb07f9b28
c849b0330d4b4e84abf996f91ae58a499a44b87340c11ca00748b00072d7bf22bb383f3f2e2aa1859
21e974e23fc695bab5c2ddd27d5fa0e6e6de2af262f2608fa8cbc25bfbdc4f5f8f0f785a1b4d4c63fa9
4f0c16601d8cff74856ca0a1ca8e1167db0a5a55e7dbb246202ae59835c16e90c1e0c5b2c8ccc1a78
f726e8963d971baba5db79b6739f3fa4329acdfef24b1b13d361832c5bd814d7acf7059e1b251f74e
604116ecb90755cc43a12639c01917653cd945c9065737efa9401947fb9557568b567bdf059a474f
95217f55ba63b3ed666854c2dda688b6acf0722076e3fd18d59b9109d4639c5a10dcc9dd17a3e78f
e956fb9687276ad8aefbfa2764ab669e7444e751fc396940fee2446b2e40d29f277a46ab9781445b2
5725cd74215a01694f2566b33456851c5966303a2053f6a22d41581fa810f1668eb7761db9206b46
6a8a65e50171f030c680a971cffd17e583060cd6e32ec5bd4ba1f9bda5976a883327bada116974b7e
8220290949d5315cd4d308e297b7789bcf7466c433e6effef150ea4a44df492f449509044104c47b3
2351b272672fc599ea6926482920a08dd08cfdfdd19ae50585efebe84f51afbd7487e04b5e127457e
37e615da2b55fafc317fecebf59a

Decrypted Text:

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.

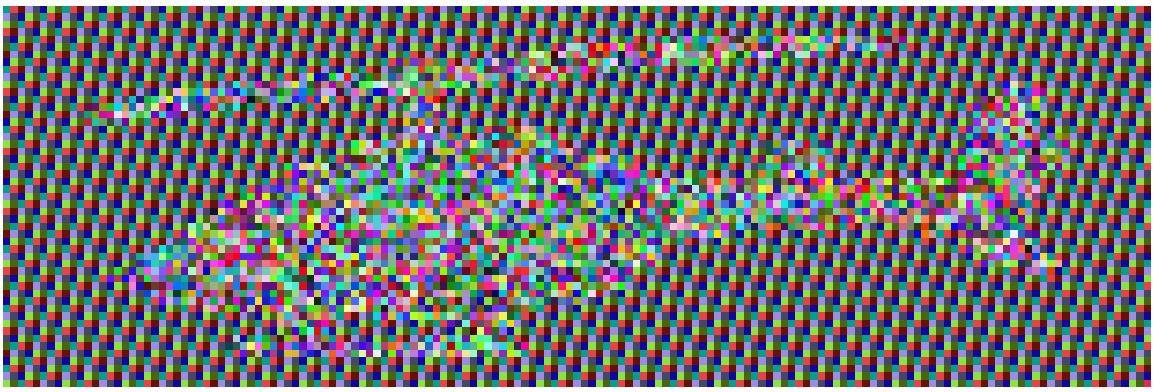
Brief Explanation of Code: The code is an adaptation of the code provided in the lecture slides. It follows the DES algorithm. The block cipher design includes both confusion and diffusion. I first began by retrieving the encryption key provided. The ‘get encryption key’ function opens the key text file and converts the key into a bit vector and ensures it is more than 64 bits, if not we use the padding function to pad it. After performing a key permutation, we return the key to

the encryption function. Next, we need the round keys to perform the DES algorithm. We then initialize a bit vector and store the message to be encrypted as a bit vector. Next, we read each bit from the file and divide the vector into two halves. Now we implement the Feistel function. We run a for loop for 16 rounds to perform the DES. First, we perform the expansion permutation converting the right half (32 bits) into 48 bits. We then xor the 48 bits with the round key for round 1. Then using the substitution boxes we convert the 48 bits back into 32 bits and then perform the P-box permutation. Finally, we xor these 32 bits with the unchanged left half. Lastly, we switch the left and right half and concatenate the encrypted text. This is done for 16 rounds with a different round key for each round. We use the 'get hex string from bit vector' and convert the string into a hex string and write it to an output file.

The decrypt function has a very similar implementation with the difference of reversing the list of the round keys and performing the same Feistel function.

Problem 2

Picture of encrypted PPM image:



Brief Explanation of Code: The encryption for the image is similar to that of a text. Initially since we do not want to encrypt the header of the PPM file we need to move the file pointer to the end of the header. Soon after we do this, we write the contents of the header directly to the output file as required. Now we begin the encryption by reading the image.ppm file as a binary file and then converting it into a bit vector. Using a for loop, I then iteration from 0 to the number of bytes in the file. Now I can extract a bit vector for every 64 bits of the file. We essentially need blocks of 64 to implement the Feistel function. We perform a permutation with the right half of the bit vector (32 bits) and then xor the new right half with the round key. Next, we use the substitution boxes to convert the 48 bits into 32 bits. Next, we perform the next permutation using the P boxes. Finally, the left half is xor'ed with the output of the permutation, and swapped with the right half. Each time 64 bits are encrypted they are concatenated and written to the file as text. We can clearly see that the encrypted image file is a helicopter which greatly reduces the idea of encryption in the first place. Therefore, we do not use block ciphers and DES encryption anymore.