HW04 ECE 40400

Problem 1 Output

encrypted.txt:

Problem 1 Decrypted Output

Scuderia Ferrari is the racing division of luxury Italian auto manufacturer Ferrari and the racing team that competes in Formula One racing. The team is also known by the nickname "The Prancing Horse", in reference to their logo. It is the oldest surviving and most successful Formula One team, having competed in every world championship since the 1950 Formula One season. The team was founded by Enzo Ferrari, initially to race cars produced by Alfa Romeo. By 1947 Ferrari had begun building its own cars. Among its important achievements outside Formula One are winning the World Sportscar Championship, 24 Hours of Le Mans, 24 Hours of Spa, 24 Hours of Daytona, 12 Hours of Sebring, Bathurst 12 Hour, races for Grand tourer cars and racing on road courses of the Targa Florio, the Mille Miglia and the Carrera Panamericana. The team is also known for its passionate support base, known as the tifosi. The Italian Grand Prix at Monza is regarded as the team's home race.

Brief Explanation of Problem 1 Code

All of my code besides the encrypt, decrypt, and main functions were adapted from the professor’s lecture 3 code that was shown in lecture or given to us in the HW02 zip folder. My main function controls whether the encrypt or decrypt function is called within the DES class based off the first argument given in the command line. If “-e” is the first argument the encrypt function is called which continually iterates through the Feistel structure implementing each step (ex. Expansion permutation, substitution with the s-boxes, permutation with the p-box) until there are no more bits to read in the BitVector. It then converts the bits into a hex string and writes it to the encryption file. If “-d” is the first argument in the command line the decrypt function is called which iterates through the Feistel structure in the same way as the encrypt function except the round keys are reversed so that they decrypt the message. This file also converts the input encryption file from hex to binary so it can iterate through the steps of the Feistel structure. The output is written to the decrypted file and then the encryption file is written over with original hex input.

Encrypted PPM Image

Was never able to successfully display ppm image :(

Brief Explanation of Code Problem 2

I’m pretty sure my code doesn’t work but there’s a slim chance it does. I wasn’t able to view the file we’re initially given in GIMP or online PPM image viewers so I truly don’t know if my code is correct (I know it resembles helicopter). That being said my new function encrypt\_image is very similar to the encrypt function. I read the first three lines of the input file and set that as a variable named header which is a byte string. I then open the output file and write the header to it before encrypting the image data. I used the Feistel structure as before to encrypt the data and then write it to the output file afterwards. My code would run for about 45sec but like I said I was never able to view the image. I’m assuming I messed up somewhere but it could be correct so rather be safe than sorry.