Homework Number: 2

Name: Andrew Wu

ECN Login: wu1795

Due Date: 1/25/24

Problem 1:

For the encrypt part, I turned the message file into a bitvector and then generated the round keys by calling get\_encryption\_key and generate\_round\_keys. I then read the bitvector by 64 bits, adding an if loop that exits the loop if there is no more to read. I then padded the bitvector to ensure that the file is of proper size. I then divide the bitvector into two, and then for each of the 16 round keys, I coded up the DEA process. I used expansion\_permutation to expand the right half of the bitvector from 32 bits to 48 bits, xor’d the expanded right half of the bitvector with the round key of that round and used the substitute function to substitute the output with the s boxes. I then used the output to permutate with the p box, and then xor’d that output with the left half of the input to form the new right half, with the new left half being the original right half of the bitvector. After all the rounds were done, I combined the right and left halves of the output and wrote the final output in hex to the outfile, creating the cipher text below.

For the decrypt part, I first opened the encrypted file and converted it from hex into a bitvector. I then generated the round keys and reversed them, since decryption happens in the reverse order of encryption. I then created blocks of 64 bits from the bitvector and then repeated the same process that I did for encryption. I start with adding an if loop to exit once there was no more to read, and then ran through the DEA process after the loop. After all the rounds of DEA, I wrote the output in ASCII to the outfile, which created the decrypted text below.

Cipher text:



Decrypted text:

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.

Problem 2:

For problem 2, I followed the same method that I used for the encryption problem in problem 1. However, since the first three lines of the image were used as a header, I first created a for loop that read the first three lines and wrote them directly to the output. I then followed the same method I used for encryption above and obtained the image of a helicopter as my output.

A pixelated image of a television screen

Description automatically generated