Aubrey Gatewood

Init: I put the P-box, key, permutation 1 and 2, expansion permutation, and s-boxes as attributes of the DES class. These I pulled from the lecture 3 starter code. I also based my solution for encrypt, decrypt, and image encrypt heavily on the sample code from the lecture notes.

Problem 1 encrypt: A computer screen shot of a program

Description automatically generated

This is most of my encrypt function. I make the bitkey based on the text input file, then permute it with permutation 1. Then I make the round keys based off of that. I make a bitvector off of the file with the message in it, and read from that vector in chunks of 64 bits. Then I divide it into 2 outside of the round key for loop so that it doesn’t split each time it loops. Then inside the for loop, I do the expansion permutation on the right side, xor with the round key, do the substitution, then do permutation with the p box. I xor the output from the p-box and the left side and make that result the new right side. Then I make the left side the old right side, and update the right side. Outside the for loop, I concatenate the left and right sides together, and add it to a bitvector in hex. Outside of the while loop (when the reading is done, I write that result to the output file.

Here is my encrypted output: 

Decrypt function:

A computer screen shot of code

Description automatically generated

This is the beginning of my decrypt function. Little is different from encrypt. I make a new file because that is the only way I could figure out to manipulate the bitvector so that it could be fed exactly into the encryption code with only the round key order reversed. I read from the file, make a bitvector with the hex string input, and write that to a temporary file. Then I’m able to read directly from the temp file for the desired bitvector. The only other change is that I reverse the order of the round keys.

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.

Problem 2:

For the image encoding I took the text encoding function and copied it over almost verbatim. The only difference was that at the beginning I wrote the first 3 lines (the header) of the image file to the output file, then proceed with encryption.

Output image: A screen shot of a television screen

Description automatically generated