**HW02: Data Encryption Standard**

Homework Number: 02

Name: Jack Gardner

ECN Login: gardne97

Due Date: 1/26/23

**Problem 1:**

**Summary**: The code borrows parts of the lecture 3 code for the extraction of round keys, permutations, and substitutions. For encryption, the code is read from the file in 64-bit chunks. If the code is less than 64 bits, zeros are padded on the right. Each chunk is split in two, the Feistel function is applied to one side using the round key, and then both sides are xored and swapped. This process is repeated 16 times to create the ciphertext, which is written to the output file in hexstring format.

For decryption, the process is essentially the same. The two most notable differences are the fact that each chunk of the cipher text must be split in two and swapped before decryption begins, and that the round keys are applied in reverse order. Another difference between encryption and decryption is the output file for the decryption is in text form rather than binary or hexstring form.

**Recovered 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.

**Encrypted text:** 

**Problem 2:**

**Brief Explanation:** This program is very similar to the DES text encryption, with a few minor differences. Primarily, the three lines at the start of the file are instantly read and written into the output file, as those lines remain unchanged after encryption. The rest of the file is read and encrypted, and is written to the output file after the header. Another notable difference is that I had to change to read byte and write byte mode, as I was having an error reading the first few lines of the file in regular mode. This resulted in passing raw bytes into the BitVector function instead of a hex string.

**Encrypted Image:**

A picture containing fabric

Description automatically generated