**HW04: Advanced Encryption Standard**

Homework Number: 04

Name: Jack Gardner

ECN Login: gardne97

Due Date: 2/14/23

**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:** As a constructor in Formula One, Ferari has a record 16 Constructors' Championships. Their most recent Constructors' Championships was won in 2008. The Team also holds the record for the most Drivers' Championships with 15, won by nine different drivers: Alberto Ascari, Juan Manuel Fangio, Mike Hawthorn, Phil Hill, John Surtees, Niki Lauda, Jody Scheckter, Michael Sschumacher and Kimi Raikkonen. Raikkonen's title in 2007 is the most recent for the team. The 2020 Tuscan Grand Prix marked Ferrari's 1000th Grand Prix in Formula One.

**Encrypted text:** 