**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 8 code for the generation of the key schedule and the byte substitution table. The 256 bit key and plaintext are read from the file, and the key schedule is generated. In encryption, at the very beginning, the first 128 bit chunk of plaintext is xored with the first four words of the key schedule. Then each 128 bit section is substituted using the generated table, then the chunk is turned into a state array, the row shifting step is applied, the columns are mixed , the state array is decomposed, and the corresponding key words are xored with the 128 bit section. These steps are repeated another 13 times, with the exception that on the last time, the mix columns step is excluded. Then the bitvector is converted to a hex string and written to the output file.

In decryption, the overall process is similar, although the steps are slightly altered and performed in a different order. The ciphertext is read from the input file and once again the key schedule and inverse sub bytes table is generated. The initial adding to the key happens again, although this time the end of the key schedule is used. Firstly, the rows are shifted again, although this time to the right instead of the left. The inverse substitution table is used for the inverse substitution step that follows. Then, the key is adding, working backwards down the key schedule. Finally, the inverse mix columns step works up the columns instead of down the columns. This is once again skipped on the last iteration. These 4 steps are repeated another thirteen times and the output plaintext is written to the output file.

**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:** 

Diagram

Description automatically generated