**Homework Number:** 04

**Name:** Samitha Ranasinghe

**ECN Login:** sranasi

**Due Date:** 02/14/2023

**Problem 1**

**Plaintext message:**

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.

**Key:** scuderiaferraritheprancinghorse!

**Encrypted message:**



**Decrypted message:**

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.

**Brief Explanation:**

Contains code for encrypting and decrypting a message using AES with a specified key.

The main function first runs the genTables function which produces the S-Boxes for encryption and decryption. For the encryption lookup table, a for loop finds the multiplicative inverse for each integer in from 0 to 255 in GF(28) and XOR that with several circular rotated versions of it and a constant. We do the same thing for the decryption lookup array, except that we first do the XORing and then we compute the multiplicative inverse. For the decryption lookup table, the same thing is done except the XORing is done first.

The encrypt function first uses functions provided in lecture notes to obtain the set of round keys. The get\_round\_keys function is called which first obtains the key from the file and then calls code from lecture to produce 15 round keys from 60 key words. A bitvector file object is created with the file containing the message to be encrypted and then blocks are grabbed at 128-bit sizes to be encrypted. The block is padded with null bits if a block is less than 128 (usually needed for the last block) and the first-round key is XORed with the block. The 4 steps in AES are then executed using different functions. The byte substitution is done by obtaining 8 bits at a time and then grabbing the element from the S-Box which the index is the integer equivalent of the 8 bits. The padded element is then substituted with the 8 bits. The row shifting is done by first producing a 4x4 matrix of the 128-bit block with a byte in each element. The shifting is done manually by swapping the elements and then converting the matrix back to a Bitvector string. The column mixing is then done by again converting into a matrix and then using a matrix multiplying function tweaked to multiply in GF(28) and then the resulting matrix is converted back to a Bitvector string. At last, the round key for the respective round is then XORed and the steps are repeated in the next round. 14 rounds are executed with the same steps except in step 14 where the column mixing is omitted

The decrypt function is similar to encrypt function except the round keys are reversed, the order of the steps is different where first the inverse row shifting, then inverse byte substitution, then round key XORing and then inverse column mixing is done. The inverse column mixing is omitted in the last round. The inverse row shifting is different in that the cycle direction is opposite to the row shifting in encryption. The inverse byte substitution is different in using a different S-Box. The inverse column mixing is different in the ratios that each element is multiplied in each column.